



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

4.26.9

NOVEMBER 12, 2019

EFFECTIVE DATE

(11-12-2019)

PURPOSE

- (1) This transmits revised text for IRM 4.26.9, *Bank Secrecy Act, Examination Techniques for Bank Secrecy Act Industries*.

MATERIAL CHANGES

- (1) This revision updates CTR, SAR and other BSA document titles and form numbers:
 - *Currency Transaction Report* (CTR) updated from FinCEN Form 104 to FinCEN Form 112
 - *Suspicious Activity Report* (SAR) updated from TD 90-22.47 to FinCEN Form 111
 - *Foreign Bank Account Report* (FBAR) updated from TD F90-22.1 to FinCEN Form 114
 - *Designation of Exempt Person* updated from TD F.90-22.53 to FinCEN Form 110
 - *Registration for Money Services Business* updated from TD 90.22.55 to FinCEN Form 107
- (2) Terms and acronyms were revised to reflect current usage:
 - CBRS updated to FCQ (FinCEN Query)
 - Workload Selection updated to Examination Case Selection (ECS)
- (3) This revision updates amendments to casino BSA regulations as per 72 FR 35008 June 26, 2007 "Financial Crimes Enforcement Network; Amendments to the Bank Secrecy Act Regulations Regarding Casino Recordkeeping and Reporting Requirements".
- (4) This revision updates amendments to the BSA regulations as per 75 FR 65806 October 26, 2010 "Transfer and Reorganization of Bank Secrecy Act Regulations". The change renumbered and reorganized the regulations from 31 CFR Part 103 to now 31 CFR Chapter X.
- (5) This revision includes edits that adapt to changes in the casino industry.
- (6) This revision removes the routine use of a Computer Audit Specialist (CAS) for examination of casinos with computerized systems since most ADP systems data from casinos can now be obtained in a Microsoft Excel or Access format instead of previous files formats not easily used by examiners.
- (7) 4.26.9.10, *Precious Metals, Precious Stones, or Jewels (PMSJ) Overview*, was added to provide guidance on the examination of dealers of precious metals, precious stones, or jewels.
- (8) 4.26.9.11, *Insurance*, was added to provide guidance on the examination of insurance companies.
- (9) 4.26.9.12, *Prepaid Access*, was added to incorporate Interim Guidance Memo SBSE-04-0819-0038, *Guidance on addressing Prepaid Access Issues in Bank Secrecy Act Examination Cases*.
- (10) 4.26.9.13, *Virtual Currency*, was added to provide guidance on the examination of virtual currency businesses.
- (11) All exhibits have been deleted.

EFFECT ON OTHER DOCUMENTS

This supersedes IRM 4.26.9 dated June 1, 2006 and Interim Guidance Memo SBSE-04-0819-0038, *Guidance on addressing Prepaid Access Issues in Bank Secrecy Act Examination Cases*.

AUDIENCE

Intended audience is employees of the Bank Secrecy Act Program in the Small Business/Self Employed (SB/SE) division, and can be referenced by all field compliance personnel, especially in Examination and Collection.

Daniel R. Lauer
Director, Specialty Examination Policy
Small Business/Self-Employed

4.26.9

Examination Techniques For Bank Secrecy Act Industries

Table of Contents

4.26.9.1 Program Scope and Objectives

4.26.9.1.1 Authority

4.26.9.1.2 Roles and Responsibilities

4.26.9.1.3 Acronyms

4.26.9.1.4 Terms

4.26.9.1.5 Related Resources

4.26.9.2 Overview

4.26.9.3 Casino and Card Clubs Overview

4.26.9.3.1 Terminology

4.26.9.3.2 Organization

4.26.9.3.3 Law

4.26.9.3.3.1 Reporting Requirements

4.26.9.3.3.2 Recordkeeping Requirements

4.26.9.3.3.3 AML Program Requirements

4.26.9.3.4 Records Commonly Found

4.26.9.3.4.1 Casino Marketing System

4.26.9.3.4.2 Credit Management System

4.26.9.3.4.3 Customer Master File

4.26.9.3.4.3.1 Multiple Transaction Logs

4.26.9.3.5 Pre-Audit, Interview and Tours

4.26.9.3.6 Systems Analysis

4.26.9.3.7 Review of Records

4.26.9.3.7.1 Special Issues

4.26.9.3.8 Evidence

4.26.9.3.9 Casino's Position

4.26.9.3.10 Money Laundering Trends

4.26.9.3.10.1 Examination Techniques

4.26.9.4 Check Cashier Overview

4.26.9.4.1 Organization

4.26.9.4.2 Law

4.26.9.4.2.1 Reporting Requirements

4.26.9.4.2.2 Registration Requirements

4.26.9.4.2.3 Recordkeeping Requirements

4.26.9.4.2.4 AML Program Requirements

4.26.9.4.3 Records Commonly Found

-
- 4.26.9.4.4 Interview
 - 4.26.9.4.5 Review of the Records
 - 4.26.9.4.6 Supporting Documentation
 - 4.26.9.4.7 Closing the Examination
 - 4.26.9.4.8 Money Laundering Trends
 - 4.26.9.4.8.1 Examination Techniques
 - 4.26.9.5 Credit Unions Overview
 - 4.26.9.5.1 Terminology
 - 4.26.9.5.2 Organization
 - 4.26.9.5.3 Law
 - 4.26.9.5.3.1 Reporting Requirements
 - 4.26.9.5.3.2 Recordkeeping Requirements
 - 4.26.9.5.3.3 AML Program Requirements
 - 4.26.9.5.4 Records Commonly Found
 - 4.26.9.5.4.1 Cash Control System
 - 4.26.9.5.5 Interview
 - 4.26.9.5.6 Review of the Records
 - 4.26.9.5.6.1 Review of Exempt Customers
 - 4.26.9.5.6.2 Review of Customer Identification Program
 - 4.26.9.5.7 Supporting Documentation
 - 4.26.9.5.8 Closing the Examination
 - 4.26.9.5.9 Money Laundering Trends
 - 4.26.9.5.9.1 Examination Techniques
 - 4.26.9.6 Dealers in Foreign Exchange
 - 4.26.9.6.1 Law
 - 4.26.9.6.1.1 Reporting Requirements
 - 4.26.9.6.1.2 Registration Requirements
 - 4.26.9.6.1.3 Recordkeeping Requirements
 - 4.26.9.6.1.4 AML Program Requirements
 - 4.26.9.6.2 Records Commonly Found
 - 4.26.9.6.3 Interview
 - 4.26.9.6.4 Review of the Records
 - 4.26.9.6.5 Supporting Documentation
 - 4.26.9.6.6 Closing the Examination
 - 4.26.9.6.7 Money Laundering Trends
 - 4.26.9.6.7.1 Examination Techniques
 - 4.26.9.7 Money Orders Overview
 - 4.26.9.7.1 Nationwide Money Orders
 - 4.26.9.7.1.1 Private Money Orders

-
- 4.26.9.7.2 Law
 - 4.26.9.7.2.1 Reporting Requirements
 - 4.26.9.7.2.2 Registration Requirements
 - 4.26.9.7.2.3 Recordkeeping Requirements
 - 4.26.9.7.2.4 AML Program Requirements
 - 4.26.9.7.3 Records Commonly Found
 - 4.26.9.7.4 Interview
 - 4.26.9.7.5 Review of the Records
 - 4.26.9.7.6 Supporting Documentation
 - 4.26.9.7.7 Closing the Examination
 - 4.26.9.7.8 Money Laundering Trends
 - 4.26.9.7.8.1 Examination Techniques
 - 4.26.9.8 Money Transmitter Overview
 - 4.26.9.8.1 Terminology
 - 4.26.9.8.2 Law
 - 4.26.9.8.2.1 Reporting Requirements
 - 4.26.9.8.2.2 Registration Requirements
 - 4.26.9.8.2.3 Recordkeeping Requirements
 - 4.26.9.8.2.4 AML Program Requirements
 - 4.26.9.8.3 Records Commonly Found
 - 4.26.9.8.4 Interview
 - 4.26.9.8.5 Review of the Records
 - 4.26.9.8.6 Supporting Documentation
 - 4.26.9.8.7 Closing the Examination
 - 4.26.9.8.8 Money Laundering Trends
 - 4.26.9.8.8.1 Examination Techniques
 - 4.26.9.9 Traveler's Checks Overview
 - 4.26.9.9.1 Nationwide Traveler's Checks
 - 4.26.9.9.2 Law
 - 4.26.9.9.2.1 Reporting Requirements
 - 4.26.9.9.2.2 Registration Requirements
 - 4.26.9.9.2.3 Recordkeeping Requirements
 - 4.26.9.9.2.4 AML Program Requirements
 - 4.26.9.9.3 Records Commonly Found
 - 4.26.9.9.4 Interview
 - 4.26.9.9.5 Review of the Records
 - 4.26.9.9.6 Supporting Documentation
 - 4.26.9.9.7 Closing the Examination
 - 4.26.9.9.8 Money Laundering Trends

- 4.26.9.9.8.1 Examination Techniques
- 4.26.9.10 Precious Metals, Precious Stones, or Jewels (PMSJ) Overview
 - 4.26.9.10.1 Terminology
 - 4.26.9.10.2 Definition of a Dealer
 - 4.26.9.10.2.1 Retailer Exception
 - 4.26.9.10.2.2 Pawnbrokers
 - 4.26.9.10.3 Covered Goods
 - 4.26.9.10.4 Law
 - 4.26.9.10.4.1 Form 8300 Filing Requirement
 - 4.26.9.10.4.2 AML Program
 - 4.26.9.10.4.2.1 Policies, Procedures, and Internal Controls
 - 4.26.9.10.4.2.2 Compliance Officer
 - 4.26.9.10.4.2.3 Training
 - 4.26.9.10.4.2.4 Independent Testing
 - 4.26.9.10.4.2.5 AML Program for Foreign Dealers
 - 4.26.9.10.5 Risk Assessment
 - 4.26.9.10.5.1 Product Risk
 - 4.26.9.10.5.2 Customer and Counterparty Risk
 - 4.26.9.10.5.3 Geographic Risk
 - 4.26.9.10.5.4 Operational Risk
 - 4.26.9.10.5.5 Monitoring Risk
 - 4.26.9.10.6 Records Commonly Found
 - 4.26.9.10.7 Title 31 or Title 26 Exam
 - 4.26.9.10.8 Title 31 Examination Procedures
 - 4.26.9.10.8.1 Pre-Plan
 - 4.26.9.10.8.2 Determining Exam Period
 - 4.26.9.10.8.3 Initial Contact
 - 4.26.9.10.8.4 Exam Scope Depth
 - 4.26.9.10.8.5 Interview
 - 4.26.9.10.8.6 Examining the AML Program
 - 4.26.9.10.8.7 Examining for Reportable Transactions
 - 4.26.9.10.8.8 Transaction Testing
 - 4.26.9.10.8.9 Red Flags
 - 4.26.9.10.9 Finalizing the Title 31 Exam
 - 4.26.9.10.10 Closing
 - 4.26.9.10.10.1 Closing a Non-Dealer Case Examined Under Title 31
 - 4.26.9.10.10.2 Closing a Dealer Case Examined Under Title 31
- 4.26.9.11 Insurance Companies Overview
 - 4.26.9.11.1 Terminology

-
- 4.26.9.11.2 Definition of Insurance Company and Covered Products
 - 4.26.9.11.3 BSA Law
 - 4.26.9.11.3.1 AML Program
 - 4.26.9.11.3.1.1 Policies, Procedures, and Internal Controls
 - 4.26.9.11.3.1.2 Compliance Officer
 - 4.26.9.11.3.1.3 Training
 - 4.26.9.11.3.1.4 Independent Review
 - 4.26.9.11.3.2 Reporting Suspicious Activity
 - 4.26.9.11.3.2.1 Timing of a SAR Filing
 - 4.26.9.11.3.3 Form 8300 Filing Requirement
 - 4.26.9.11.3.4 Record Retention
 - 4.26.9.11.4 Risk Assessment
 - 4.26.9.11.4.1 Customer Risk
 - 4.26.9.11.4.2 Product Risk
 - 4.26.9.11.4.3 Geographic Risk
 - 4.26.9.11.4.4 Distribution Channel Risk
 - 4.26.9.11.4.5 Operational Risk
 - 4.26.9.11.5 Records Commonly Found
 - 4.26.9.11.6 Title 31 or Title 26 Exam
 - 4.26.9.11.7 Title 31 Examination Procedures
 - 4.26.9.11.7.1 Pre-Plan
 - 4.26.9.11.7.2 Initial Contact
 - 4.26.9.11.7.3 Exam Scope and Depth
 - 4.26.9.11.7.4 Interview
 - 4.26.9.11.7.5 Assessing Risk
 - 4.26.9.11.7.6 Examining the AML Program
 - 4.26.9.11.7.7 Examining for Suspicious Activity Monitoring and Reporting
 - 4.26.9.11.7.8 Examining for Reportable Form 8300 Transactions
 - 4.26.9.11.7.9 Transaction Testing
 - 4.26.9.11.7.10 Verifying Agent Monitoring
 - 4.26.9.11.7.11 Red Flags
 - 4.26.9.11.7.12 Examining Recordkeeping Compliance
 - 4.26.9.11.7.13 Finalizing the Title 31 Exam
 - 4.26.9.11.8 Closing a Case Examined Under Title 31
 - 4.26.9.12 Prepaid Access Overview
 - 4.26.9.12.1 Prepaid Access Defined
 - 4.26.9.12.2 Prepaid Access Terminology
 - 4.26.9.12.3 Prepaid Access Program
 - 4.26.9.12.3.1 Prepaid Access Program Inclusions

-
- 4.26.9.12.3.2 Prepaid Program Exclusions
 - 4.26.9.12.3.2.1 Closed Loop Prepaid Access Exclusions
 - 4.26.9.12.3.2.2 Open Loop Prepaid Access Exclusions
 - 4.26.9.12.3.2.3 Employment-Related Limited Exclusions
 - 4.26.9.12.4 Prepaid Access Provider
 - 4.26.9.12.5 Prepaid Access Seller Defined
 - 4.26.9.12.6 Prepaid Access Provider Regulatory Requirements
 - 4.26.9.12.6.1 Provider Requirement to Register with FinCEN
 - 4.26.9.12.6.1.1 Who Is Not Required to Register
 - 4.26.9.12.6.2 Agent Listing
 - 4.26.9.12.6.3 Prepaid Access Provider and Program Participant Requirements
 - 4.26.9.12.6.3.1 AML Program
 - 4.26.9.12.6.3.2 Customer Identification Requirements
 - 4.26.9.12.6.3.3 Suspicious Activity Reports
 - 4.26.9.12.6.3.4 Recordkeeping Requirements
 - 4.26.9.12.6.3.4.1 Records Commonly Found
 - 4.26.9.12.6.3.5 Additional Prepaid Access Requirements
 - 4.26.9.12.7 Risk Factors
 - 4.26.9.12.7.1 Knowledge about Customers
 - 4.26.9.12.7.2 Intended Users
 - 4.26.9.12.7.3 Number of Prepaid Cards per Person
 - 4.26.9.12.7.4 Card Expiration
 - 4.26.9.12.7.5 Geographic Area
 - 4.26.9.12.7.6 Load and Reload Frequency
 - 4.26.9.12.7.7 Source of Funding
 - 4.26.9.12.7.8 Funding by Value Transfer
 - 4.26.9.12.7.9 Value Limits
 - 4.26.9.12.7.10 Cash Withdrawal via Automated Teller Machine (ATM)/Cash Redemption
 - 4.26.9.12.7.11 Intended Scope of Card Use
 - 4.26.9.12.7.12 Third-Party Relationships
 - 4.26.9.12.8 Risk Mitigation
 - 4.26.9.12.9 Examination Procedures
 - 4.26.9.12.9.1 Pre-Plan
 - 4.26.9.12.9.2 Initial Contact
 - 4.26.9.12.9.3 Scope and Depth
 - 4.26.9.12.9.4 Interviews
 - 4.26.9.12.9.5 The AML Compliance Program
 - 4.26.9.12.9.5.1 Examining the AML Compliance Program
 - 4.26.9.12.9.5.2 Examination Techniques

-
- 4.26.9.12.9.5.3 Examining for Suspicious Activity Monitoring and Reporting
 - 4.26.9.12.9.5.3.1 Transaction Testing
 - 4.26.9.12.9.5.3.2 Red Flags
 - 4.26.9.12.10 Pre-Paid Access and Tax Refund Fraud
 - 4.26.9.12.10.1 Prepaid Access Red Flags for Tax Refund Fraud
 - 4.26.9.12.10.2 Detecting and Stopping Fraudulent Tax Refunds
 - 4.26.9.12.11 Verifying Seller Monitoring
 - 4.26.9.12.12 Finalizing the Exam
 - 4.26.9.12.13 Closing a Case
 - 4.26.9.13 Virtual Currency Overview
 - 4.26.9.13.1 Virtual Currency Terminology
 - 4.26.9.13.2 Virtual Currency Defined
 - 4.26.9.13.3 Virtual Currency Participants
 - 4.26.9.13.4 Law
 - 4.26.9.13.5 Regulatory Requirements
 - 4.26.9.13.5.1 Registration Requirements
 - 4.26.9.13.5.2 Anti-Money Laundering Program Requirements
 - 4.26.9.13.5.2.1 AML Policies and Procedures
 - 4.26.9.13.5.2.2 Compliance Officer
 - 4.26.9.13.5.2.3 Education and Training
 - 4.26.9.13.5.2.4 Independent Testing
 - 4.26.9.13.6 Recordkeeping and Retention
 - 4.26.9.13.7 Reporting Requirements
 - 4.26.9.13.7.1 Currency Transaction Reports
 - 4.26.9.13.7.2 Suspicious Activity Reports
 - 4.26.9.13.7.3 Other Required BSA Reports if Warranted
 - 4.26.9.13.8 Other BSA Requirements

4.26.9.1
(11-12-2019)
Program Scope and Objectives

- (1) **Purpose.** This IRM explains the Bank Secrecy Act (BSA) examiner's responsibilities when conducting risk-based examinations of financial institutions. The material covers the full examination process from the pre-planning stage to closing.
- (2) **Audience.** This IRM is for BSA managers and examiners.
- (3) **Policy Owner.** Director, Specialty Examination Policy – Small Business/Self Employed.
- (4) **Program Owner.** Director, Examination - Specialty Examination owns Bank Secrecy Act.
- (5) **Primary Stakeholders.** SB/SE Specialty Examination BSA, Specialty Examination, Specialty Exam Policy BSA and SB/SE Examination Quality & Technical Support are the primary stakeholders for this IRM.
- (6) To recommend changes or make any other suggestions related to this IRM section, see IRM 1.11.6.6, *Providing Feedback About an IRM Section - Outside of Clearance*.

4.26.9.1.1
(11-12-2019)
Authority

- (1) The Department of the Treasury has primary responsibility for implementing and enforcing the BSA. The Secretary of the Treasury delegated the authority to administer the BSA to the Director, Financial Crimes Enforcement Network (FinCEN). FinCEN re-delegated responsibility for assuring civil compliance with the law to various Federal agencies including the Internal Revenue Service.
- (2) 31 CFR 1010.810(b)(8) delegates authority to the Commissioner of Internal Revenue to examine all financial institutions, except brokers or dealers in securities, mutual funds, futures commission merchants, introducing brokers in commodities, and commodity trading advisors, not currently examined by federal bank supervisory agencies for soundness and safety.
- (3) 31 CFR 1010.810(f), *Enforcement*, allows FinCEN or its delegate, and any agency to which compliance has been delegated to examine any books, papers, records, or other data of domestic financial institutions relevant to the recordkeeping and reporting requirement of the BSA.

4.26.9.1.2
(11-12-2019)
Roles and Responsibilities

- (1) Director, Examination - Specialty Policy is the executive responsible for BSA examination policy and procedures.
- (2) Director, Examination - Specialty Examination is the executive responsible for BSA examination operational compliance.
- (3) Chief, BSA Examination is responsible for ensuring information about basic BSA examiner responsibilities and IRM sections is communicated to and carried out by BSA examiners.
- (4) All examiners must perform their professional responsibilities in a way that supports the IRS Mission. This requires examiners to provide top quality service and to apply the law with integrity and fairness to all.

4.26.9.1.3
(11-12-2019)
Acronyms

(1) The following is a table of commonly used acronyms and their definitions:

Acronym	Definition
ACH	Automated Clearing House
AML	Anti-Money Laundering
ATM	Automated Teller Machine
BSA	Bank Secrecy Act
CAS	Computer Audit Specialist
CFR	Code of Federal Regulations
CI	Criminal Investigation
CMS	Credit Management System
CMIR	Report of International Transportation of Currency or Monetary Instruments
CTR	Currency Transaction Report
CVC	Convertible Virtual Currency
EFT	Electronic Funds Transfer
EIN	Employer Identification Number
ECS	Exam Case Selection
ERCS	Examination Return Control System
FAQ	Frequently Asked Question
FBAR	Report of Foreign Bank and Financial Accounts
FCQ	FinCEN Query
FinCEN	Financial Crimes Enforcement Network
GAGR	Gross Annual Gaming Revenue
GM	Group Manager
GPR	General Purpose Reloadable
IDR	Information Document Request
IDRS	Information Data Retrieval System
IPMI	Information Precious Metals Institute
IT	Information Technology
ITG	Indian Tribal Government
KYC	Know Your Customer
MIL	Monetary Instruments Log
MIS	Management Information System
MMORPG	Massively Multiplayer Online Role-Playing Game

Acronym	Definition
MSB	Money Service Business
MTL	Multiple Transaction Log
NBFI	Non-Bank Financial Institution
NBPCA	Network Branded Prepaid Card Association
NCUA	National Credit Union Administration
NIL	Negotiable Instruments Log
NYCE	New York Currency Exchange
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person
PMSJ	Precious Metals, Precious Stones, or Jewels
POS	Point of Sale
P-to-P	Person to Person
SAA	Survey After Assignment
SAR	Suspicious Activity Report
SRS	Specialist Referral System

4.26.9.1.4
(11-12-2019)
Terms

- (1) The following table lists commonly used terms and associated definitions:

Term	Definition
Activity Record	The term “activity record”, as used throughout this IRM, means Form 9984, <i>Examining Officer’s Activity Record</i> .
CI	The term “CI”, as used throughout this IRM, means IRS Criminal Investigation – the law enforcement arm of the IRS.
Disclosure	The term “Disclosure”, as used throughout this IRM, means IRC 6103, <i>Confidentiality and Disclosure of Returns and Return Information</i> .
ECS	The term “ECS” as used throughout this IRM means BSA Exam Case Selection.
Examiner	The term “examiner”, as used throughout this IRM, means BSA examiner.
Examination	The term “examination”, as used throughout this IRM, means a BSA examination.

Term	Definition
5104 Package	The term “5104 Package”, as used throughout this IRM, means the complete Form 5104, <i>Report of Apparent Violation of Financial Record-keeping and Reporting Regulations</i> , referral package. The package includes the actual Form 5104 narrative and all attachments.
5104 Referral	The term Form “5104 Referral” as used throughout this IRM means the Form 5104.
Financial Institution	The term “financial institution”, as used throughout this IRM, means a financial institution for which IRS has been delegated examination authority and includes casinos, MSBs, and banks/credit unions without a Federal regulator.
Title 31 Database	The term “Title 31 Database”, as used throughout this IRM, means the Title 31 NBFI Database that houses the entire population of Title 31 entities identified as being subject to IRS jurisdiction. The database contains entity information and examination information. The database uses multiple tables in an SQL environment.

4.26.9.1.5
(11-12-2019)

Related Resources

- (1) The following table contains related resources referenced in this IRM.

Resource	Title
https://organization.ds.irsnet.gov/sites/SbseSpec/BSA/SitePages/Home.aspx	BSA Exam SharePoint
https://organization.ds.irsnet.gov/sites/SbseFraudBSA/BkSecAct/SitePages/Home.aspx	BSA Policy SharePoint
https://www.fincen.gov/	FinCEN website

4.26.9.2
(06-01-2006)

Overview

- (1) This section discusses basic information about how each unique financial institution operates, books and records commonly found at each financial institution, and examination and auditing techniques for each financial service offered. Some examination steps will be consistent for all financial institutions, others will be unique to the financial service provided. The information is intended to assist examiners in conducting a Bank Secrecy Act (BSA) examination. All cases are subject to factual development. Examiners should adapt the procedures in this section, as necessary, to each situation.
- (2) The primary goals of any BSA examination are to:
- Determine whether the financial institution has established and implemented an effective anti-money laundering (AML) program,

- b. Determine whether the financial institution is following all recordkeeping and reporting requirements,
- c. Determine if there are weaknesses or violations,
- d. Assist the financial institution to understand the BSA requirements and encourage compliance, and
- e. Refer serious or repeated BSA violations to FinCEN or CI, as appropriate.

4.26.9.3
(11-12-2019)
**Casino and Card Clubs
Overview**

- (1) The BSA defines a casino as a financial institution if:
 - a. It is duly licensed or authorized as a casino or card club in the United States or a class III tribal casino with or without authority to operate as a tribal class II casino and
 - b. has more than \$1,000,000 in Gross Annual Gaming Revenue (GAGR).
- (2) Casinos that meet the definition of a casino financial institution must adhere to the BSA regulations contained in 31 CFR Part 1010, *General Provisions*, and 31 CFR Part 1021, *Rules for casinos and card clubs*. Casinos as defined in 31 CFR 1010.100(t)(5), *Casino*, and 31 CFR 1010.100(t)(6), *Card clubs*, are not required to comply with rules specific to MSBs or other financial institutions. Each casino licensee with more than \$1,000,000 GAGR is a separate and distinct financial institution even if several different casino licensees have common ownership such as a single corporate owner, a common parent corporation or a common tribal ownership.

Example: If one corporation has three casinos each with the same EIN but with three separate casino licenses then each casino is a separate financial institution. Conversely, if two or more casinos share a common casino license and have a combined GAGR greater than \$1,000,000 then they are a single financial institution instead of separate financial institutions.

- (3) Casino and card clubs with GAGR of \$1,000,000 or less but meet the definition of an MSB financial institution must adhere to the BSA regulations contained in 31 CFR Part 1010 and 31 CFR Part 1022, *Rules for money service businesses*. Casinos and card clubs with GAGR of \$1,000,000 or less and do not offer MSB services are not financial institutions, but instead are a non-financial trade or business subject to the requirements of IRC 6050I, *Returns relating to cash received in trade or business*, and BSA 31 CFR 1010.340, *Reports of transportation of currency or monetary instruments*.
- (4) Pursuant to a 1985 memorandum of agreement with the Department of Treasury, certain casinos in Nevada were exempted from direct application of BSA recordkeeping and currency transaction reporting requirements. Instead, these casinos were subject to Nevada Gaming Commission Regulation 6A, if they had GAGR of \$10,000,000 or more and table games statistic win of \$2,000,000 or more. Nevada casinos which had over \$1,000,000 in GAGR were not subject to Nevada Gaming Commission Regulation 6A and are instead were subject to the reporting, recordkeeping and compliance program requirements of the BSA. The 1985 BSA exemption for those certain Nevada casinos remained until June 30th, 2007. After June 30th, 2007, Nevada casinos were no longer exempt from the BSA. Nevada casinos with a GAGR of \$1,000,000 or less were and continue to be subject to the reporting requirements of IRC 6050I and now also BSA 31 CFR 1010.340.

- (5) Whenever the term casino is used in the regulations or in this IRM, the term expressly includes card clubs, and the same requirements therefore apply, unless a different treatment for card clubs is explicitly stated in 31 CFR Part 1021.
- (6) Unlike other financial institutions, which exist solely for conducting financial transactions, casinos primarily function as entertainment and recreational facilities. However, as with other financial institutions, casinos provide a wide range of financial services to their customers including:
 - a. Acceptance of funds for deposit and withdrawals of funds on deposit,
 - b. Issuance of credit and receipts of payments on credit,
 - c. Check cashing services,
 - d. Issuance of checks,
 - e. Wire transfers of funds, and
 - f. Currency exchanges.
- (7) Casinos vary in size and sophistication from small one owner gambling parlors, offering a limited number of games and services, to large corporate luxury mega facilities offering a full range of games, services and entertainment. In addition to a gambling casino, the larger resort type casino complex may include hotel facilities, restaurants, bars and lounges, theaters and showrooms, sports and health facilities, convention space, and various exclusive shops and stores.
- (8) The requirements of the BSA apply only to transactions taking place between the gambling casino and its customers, however, 31 CFR 1021.100(c) defines a “customer” as every person involved in a transaction applicable to 31 CFR 1021 regardless if that person participates or intends to participate in gaming activities. For example, if a person wires funds to a casino to be placed in a front money account but never gambles, they are still considered to be a “customer” of the casino. Another example would be if a person cashes a check at the casino cage but never gambles they would still be considered a customer of the casino. Currency transactions between the hotel and/or other outlets within the casino complex and their customers are subject to the requirements covered under IRC 6050I and 31 CFR 1010.340 .
- (9) The definition of a casino as a financial institution includes any branch office. Even though each separate casino license defines a casino as a financial institution for BSA purposes, some casinos may have branch offices to accept payments for debit and credit accounts. Transactions at these branch offices specific to a casino licensee are considered to have occurred by, through or to the licensee. Occasionally, these offices will accept currency for deposit to a customer’s casino account or in payment of markers. The funds are usually placed on deposit in the branch office’s bank account and wire transferred to the casino. These branch offices may be shared with other related properties and may operate under a different legal name and EIN. Some branches may even be a residence for a junket operator, marketing representative or an independent agent who has been delegated authority by a casino to accept funds for deposit or as credit payments from customers. These branch offices can be authorized to conduct wire transactions for customers which would be considered as conducted by, through or to the casino. Transactions between customers and foreign branch offices are not subject to BSA reporting and recordkeeping requirements. Subsequent transactions between a foreign branch office and a U.S. casino, however, are considered transactions by, through or to the U.S. casino.

- (10) Authority to examine casinos to determine compliance with the BSA reporting, recordkeeping, and compliance program requirements has been delegated by Treasury to the IRS in 31 CFR 1010.810(b)(8).

4.26.9.3.1
(11-12-2019)
Terminology

- (1) After the Fact Aggregation – The process by which a casino reviews and aggregates cash transactions that were otherwise not possible to be known to exceed \$10,000 in real time.
- (2) Backline Betting - A type of betting that occurs when a customer, who is standing behind a seated player, places a bet or wager on the betting circle for a specific hand on which a seated player also is wagering. The extra players that stand behind each seat position are known as “backline betters”. This type of betting is more common at card clubs. Although backline betting makes it difficult to track customer wagers at the gaming table, a card club is required to have a procedure in place to identify such transactions.
- (3) Barred Player List - A list of casino customers barred from future gambling activity such as card markers, other casino cheats, thieves, and card counters. Almost all casinos maintain a barred patron list containing the names of customers who did not provide identification credentials after completing reportable currency transactions.
- (4) Bill Stuffing - A customer placing currency in a slot machine, then cashing out after minimal or no play. The customer then takes the Ticket-In/Ticket-Out (TITO) ticket(s) and redeems them at a kiosk on the gaming floor.
- (5) Bill Validator (Acceptor) - An optical mechanical device attached to an electronic gaming device such as a slot machine or video lottery terminal that accepts U.S. paper currency of various denominations as well as each casino’s TITO tickets and issues gaming credits for use in an electronic gaming device.
- (6) Buy-in – The amount of funds a player uses to purchase casino chips when commencing play. A buy-in can occur in cash, credit, or as a deposit withdrawal.
- (7) Cage - A secure work area within a gaming establishment for cashiers, a storage area for the gaming facility’s bankroll (for example, maintains the inventory of cash, chips, tokens, and credit), and a place where banking services are provided to customers and other casino banks. In this capacity, it is the casino’s in-house bank where customers can open deposit and credit accounts, deposit and withdraw funds, receive and pay off credit (for example, markers), purchase and cash payroll and personal checks, wire transfer funds, purchase and redeem (or exchange) gaming chips, tokens and tickets, and exchange currency. Also, larger casinos may maintain satellite cages in slot areas, high roller areas or in the betting parlors. A card club cage operates, for the most part, as does a casino cage except that it does not offer token sales and redemptions because there are no slot machines.
- (8) Chips (also known as, Checks, Tokens) - A gaming instrument issued in various denominations and used as a substitute for currency at table games in a casino.

- (9) Chip Walk - A casino term for chips that a customer leaves a gaming table with at the end of play.
- (10) Chip Redemption - The exchanging of chips by a customer for cash, casino check, or outgoing wire transfer.
- (11) Complimentary (Comps) - Complimentary items or “comps” typically are goods or services that a casino gives to a customer, at reduced or no cost, based on significant play and can include beverages, coupons, or other representations of money for use in wagering, beverage, food, entertainment, merchandise, lodging, show ticket and ticket to special events, or transportation (for example, airplane ticket, car rental). Also, a “comp” can be in the form of currency.
- (12) Drop – “Drop” in table games, is the total amount of cash or cash equivalents plus paper credits (for example, markers) that a dealer puts in the table drop box which were exchanged for chips or plaques. “Drop” in slot machines or video lottery terminals, is the total amount of customers’ coins and tokens in the drop bucket, and customers’ U.S. paper money (bills) and TITO tickets (vouchers) in the bill storage box in such devices. Also, the drop refers to the removal of the slot machine and table game drop boxes that are transported to the hard and soft count rooms, respectively.
- (13) Front Money (Deposits and Withdrawals) - Money deposited by a customer into a personal casino account at a cage that a customer could later withdraw at a gaming table (in the form of chips to bet or wager with after signing a so-called “front money marker” against the deposited funds), electronic gaming devices (in the form of credits or access cards), or later at a cage (in the form of casino check, currency, money transfer, and other similar items.). This internal account is offered to allow a customer to deposit with a casino funds to be gambled or won.
- (14) Gaming Day - The normal business day of the casino by which it maintains its books and records for business, accounting, and tax purposes. A casino may have only one gaming day common to all its divisions.
- (15) Junket Representative - A person who is responsible for organizing a group of players (a junket) to gamble at a casino. The representative can be a junket operator or an employee of the junket operator. Typically, the representative will send a wire or money transfer of the total funds that the junket players intend to gamble to a casino’s domestic bank or a money transmitter located on the casino’s premises. The funds will be held in a front money deposit account until the junket arrives at a casino. Most U.S. State gambling regulators require that a junket representative provide to the regulator identification information and financial qualifications or rating of gambling performance (such as their theoretical win/loss) for each customer before or upon arrival at a casino. In most jurisdictions junket operators are not casino employees and thus are not subject to the same degree of licensing oversight by State gambling regulators; nonetheless, some background screening is done on junket operators. Also known as, a “Junket Master”, “Junket Operators”, or “Independent Agent”.
- (16) Kiosk Machine - A multifunctional machine, connected to a gateway or kiosk server, that can perform a variety of financial transactions, such as redeeming slot machine/video lottery tickets for currency, exchanging U.S. currency for U.S. currency (for example, breaking bills or paper money), redeeming player slot club points, purchasing slot machine vouchers (for example, tickets), and

initiating electronic transfers of money to or from a wagering account including currency withdrawals from a casino ATM. Such machines are designed to reduce time to pay out slot jackpots to customers and improve productivity. Currently, kiosk machines do not require a customer who has a slot club account card to use it to conduct transactions. Cash kiosk machines and/or ATM machines in casinos are not supplied typically by a casino, but by machine vendors, who are able to place these machines in casinos on two conditions:

- a. A vendor and a casino come to satisfactory business terms, and
 - b. The regulatory authority, and in some jurisdictions the legislature, approves the arrangement.
- (17) Lammer - A button or chip distinguishing the amount of credit being granted to a customer. A lammer is placed on the table while the chips are given to the customer.
- (18) Marker (also known as Counter Check) - A blank check provided to an established customer and drawn against his/her casino line of credit account, in exchange for chips, tokens, or currency, and is intended for use in gambling. A customer would have to sign a marker before a casino will extend credit, which insures that a marker is treated as a personal check. Also, a marker resembles a personal check, which can be deposited into the casino's commercial bank for processing through the Federal Reserve System or commercial clearing-houses and correspondent domestic banks if the check is not redeemed within a specified period.
- (19) Marker Redemption - The redemption or paying off a previously issued marker by a customer. Typically, markers are settled before a customer leaves a casino, but many casinos will allow customers time to repay a marker, depending on each customer's status with that casino, and based upon a gaming regulator's marker repayment schedule.
- (20) Minimal Gaming or Minimal Play - A term that can apply to many different situations in a casino environment. The most common reference is for individuals who:
- a. Exchange a large amount of currency for casino chips or obtain large markers in a gaming day,
 - b. Gamble for a small amount of time,
 - c. Either lose/win a nominal amount of the chips or make small bets in comparison to the buy-in, and
 - d. Then cash out the remaining chips either by the gamblers or their agents. These activities are conducted to make the currency appear as a legitimate source of income.

An effective method to detect this is by reviewing computerized customer records such as player ratings to determine potential suspicious activity.

- (21) Monetary Instruments Log (MIL) (also known as a NIL) – A term used by casinos for the separate record containing a list of each transaction between the casino and its customers involving negotiable instruments having a face value of \$3,000 or more as required by 31 CFR 1021.410(b)(9).

- (22) MTL - Casino documents used for recording and keeping track of customer currency transaction activity above a given dollar threshold.
- (23) Off Track Betting (OTB) - Pari-mutuel wagering that is conducted at a gambling establishment other than the race course (for example, horse and/or dog/greyhound track) where the actual race is being held.
- (24) Pari-Mutuel Wagering - Wagering conducted pursuant to licenses granted in the US by state governmental agencies on various sports, including horse racing, greyhound racing and jai alai that occur at racetracks, racinos, and frontons. The betting can occur at racetracks, OTB facilities, tribal, racinos, frontons, on Internet platforms, and interactive television platforms. Thus, the wagering may be conducted at a location other than the racetrack or fronton where the race or jai alai match, respectively, is held. In a pari-mutuel system of wagering, gambling establishments pool all customer wagers on the outcome of various racing and sporting events. The gambling establishments do not risk any of their own money. Winners divide the total amount bet in the wagering pool in proportion to the sums that customers have wagered individually on each racing event, after the operator deducts its takeout (which constitutes the gross revenue of the pari-mutuel business that is used to pay operating expenses, contributions to purses, taxes, including pari-mutuel taxes, interest, debt service, pension benefits, and any other charge against income). Bettors are essentially betting against each other, which means that the losers pay the winners.
- (25) Player Rating - A monitoring system a casino uses to rate and track the gaming activity of a single player. Casinos use a variety of methods to award complimentary services, or comps to attract and retain their customers. The most common method is based on theoretical win, which is the amount a casino expects to win from a customer. It is calculated using the following four factors:
 - a. Theoretical house advantage of a game (each game has a specified percentage of house advantage),
 - b. Number of expected hands or spins per hour (for example, expected value of play),
 - c. Gambler's average bet, and
 - d. Length of time the gambler plays.

The latter two factors, which are used to compute the "player" rating is monitored, recorded by a casino supervisor typically on a player rating card, and entered by a pit clerk into a computerized tracking system. These four factors, when multiplied together, produce the theoretical win for a casino. Casinos award comps to gamblers based on a percentage of theoretical win.

- (26) Player Rating System - A manual or computerized system of tracking customer gambling activities at various gaming departments (Tables Games, Race and Sports, Keno, Poker, and Bingo) based on physical observations by casino employees. Casino employees manually input the customer's transactions on manual documents or a computerized system. A slot player rating system is a computerized system used to track customer gaming activity at the slot machines using "Slot Club Membership Cards" inserted into the machine.
- (27) Rake - The money a casino charges for each hand of poker. It is usually a percentage or a flat fee that is taken from the pot after each round of betting.

- (28) Rim Credit - An extension of credit, noted on a rim card for faster session play. Upon completion of the session play the balance is settled in the form of a marker.
- (29) Safekeeping (Deposits/Withdrawals) - Funds placed on deposit into an account at a casino cage to be held for security and convenience purposes that a customer could only withdraw by returning to a cage. Safekeeping funds cannot be drawn down at the gaming tables or slot machines/video lottery terminals.
- (30) Shill - A casino employee who actively plays in a table game for the casino, club or the house. Usually seen at a Baccarat table to fill empty seats, until more real players join the game.
- (31) Ticket-In/Ticket-Out (TITO) - Slot machines or video lottery terminals allow customers to play on credits from bills, tickets or coins. The machines only dispense tickets and not coins. The TITO tickets, which can have any stated monetary value, can be inserted in an electronic gaming device that has the TITO function and can be played in such a device or cashed out with a cashier or at a kiosk machine.
- (32) Token - A gaming instrument issued in various denominations and used as a substitute for currency to play slot machines.
- (33) Trip - Any number of continuous days of gaming activity by a customer in which there is not a break in play.
- (34) Trip History Summary Report - A report that summarizes the total funds from a customer's multi-day trip and the most recent trips, usually between three and nine trips. Because a trip includes any number of continuous days of gaming activity in which there is not a break in play, the player trip history is only a limited summarized record that typically does not provide all the information contained on the original player rating cards, such as the specific amounts of the customer's currency transactions conducted for each gaming day.
- (35) Wagering Account - An account set up for the purposes of mobile gaming or on-line gaming.

4.26.9.3.2 (06-01-2006) **Organization**

- (1) Casinos that are duly licensed or authorized to do business are regulated by state, tribal, or local governments. As such, their organizational structure may vary depending upon applicable laws and regulations as well as the needs of management within each individual casino. Generally, however, a typical gambling casino is organized into two separate, yet related, operations: the casino floor and the casino cage. Larger casinos may have more than one casino floor and/or more than one casino cage.
- (2) The casino floor is the area of the casino where all gaming activities occur. It is usually organized into Gaming Pits and Slot Zones and operates under the direction of the Casino Manager.
- (3) A pit is an area of the casino floor enclosed or encircled by gaming tables in which casino personnel administer and supervise the games being played at those tables. Pits may be comprised of tables offering only one type of game or may be made up of tables offering a number of different types of games. Pit personnel may include the following:

- a. Pit Boss - A management employee who has supervisory authority over all gaming activity taking place in the pit.
 - b. Floor person - A management employee who has supervisory authority over all gaming activity taking place at a given number of tables within the pit.
 - c. Dealer - A casino employee who conducts the gaming activity at a single gaming table within the pit.
 - d. Pit Clerk – An employee in a table game pit who documents, fills, and credits player credit instruments (such as markers) and player rating forms.
- (4) A Slot Zone is an area of the casino floor, usually separated from the gaming pits, where slot machines are grouped into rows, circles and banks of machines. A slot zone may also include slot booths and coin redemption stations where coins and tokens can be purchased or redeemed, slot markers can be issued or redeemed, and slot jackpots can be paid. Slot personnel may include slot managers, slot supervisors, and slot attendants.
- (5) Some casinos may also maintain separate rooms or parlors that offer other games such as Keno, Bingo, Poker, Race Betting, Sports Betting, and others. Each room or parlor operates under the direction of a room manager who reports to the shift manager on duty.
- (6) The casino cage houses the cashiers and the cage's inventory, provides banking services for players and other casino banks, and records, tracks and monitors all financial transactions. It is the financial center of the entire casino operation and is the point at which all currency, chips and other funds are ultimately accounted for. In this capacity it is the casino's in-house bank where customers can open deposit and credit accounts, deposit and withdraw funds, receive and pay off credit (such as markers), purchase and cash checks, wire transfer funds, redeem chips, exchange currency and more. Larger casinos may also maintain satellite cages in slot areas, high roller areas or betting parlors. Under the supervision of the Casino Cage Manager, the casino cage operates much like a commercial bank and is generally organized into five components:
- a. Main bank - The area of the casino cage where all currency is stored. It is through the main bank that currency is transferred from the gaming tables, to and from the cashier's windows and to or from the casino's commercial banking institution. The main bank maintains an inventory of coins and chips.
 - b. Chip bank - The area of the casino cage where all of the gaming chips are stored. It is through the chip bank that chips are transferred to and from the gaming tables and to or from the cashiers' windows.
 - c. Marker bank - The area of the casino cage where all marker activity related to credit accounts is recorded, processed and stored.
 - d. Credit management - The area of the casino cage where customer credit accounts are managed.
 - e. Cashier (Teller) windows - The area of the casino cage where financial transactions between the casino cage and its customers occur. The windows are staffed by cashiers who conduct the financial transactions and prepare source documents.
- (7) The casino marketing department is responsible for retaining and bringing new business into the casino. Within the marketing department, casino hosts, who

cater to high roller's needs, may assist players in opening deposit and credit accounts and issuing complimentary gifts and services to customers.

- (8) The casino surveillance department is an important resource in deterring and detecting suspicious or criminal activities. Surveillance employees monitor casino activities using a variety of technologies, including video cameras, monitors, recorders, video printers, switches, selectors and other equipment. Monitored activities that are unusual, suspicious, or potentially criminal in nature are noted in a surveillance log. Videotapes and/or electronic recordings generally will be maintained for a period established by the casino's state, tribal or local regulator.
 - (9) Card rooms offer no house-banked games. Instead, players gamble against each other. Card rooms usually offer games in two broad categories: poker games, and California games. In California games, one player acts as the bank and other players bet against the bank. The banker collects all winning bets and pays all losing bets from his/her bankroll. There are a fixed number of seats at each table, but other players ("backline bettors") can place bets from behind each seat location.
 - (10) The gaming floor of a card room operates much like the gaming floor of a traditional casino, although operational differences exist.
 - a. Generally, poker and California games are in separate rooms.
 - b. As with casinos, individual tables are organized into pits where dealers conduct the games under the supervision of pit bosses or floor persons.
 - c. Card clubs do not rate customer gaming transactions because card club income is based solely on table fee collections and not on player wins and/or losses. Instead, card clubs maintain MTLs for currency transactions in excess of specified amounts, typically \$2,500 or \$3,000. However, a customer's name will be recorded on such logs, only "if known".
 - d. Card clubs do not provide "comps" to customers.
 - e. Dealers typically purchase the inventory of their own chip tray from the card room. Since dealers typically own the inventory of chips and currency in their trays, they often can gamble at the tables during breaks, or even while dealing the game.
 - f. Card clubs employ chip runners who sell and redeem chips directly to the customers.
 - (11) Card clubs can offer the same types of financial services to their customers as traditional casinos (such as deposit accounts, credit accounts, check cashing, wire transfers, and currency exchange services). As with casinos, card rooms maintain cages where cashiers conduct financial transactions. The cage of a card room operates much like the cage of a traditional casino (that is, it is made up of front windows and a cage vault).
-
- (1) Casinos and card clubs in the United States, its territories and possessions, and on Indian lands, with GAGR in excess of \$1,000,000 are defined as financial institutions under 31 CFR 1010.100(t)(5)(i), *Casino*, and 31 CFR 1010.100(t)(6)(i), *Card club*. A separate location is a branch if it is operating under the same casino license or tribal compact. If the additional casino location has a separate and distinct casino license or tribal compact, then it is a separate financial institution.

4.26.9.3.3
(11-12-2019)
Law

- 4.26.9.3.3.1
(11-12-2019)
Reporting Requirements
- (2) For special rules pertaining to casinos including the development of a written compliance program and special terms relating to casinos, refer to 31 CFR 1021.210, *Anti-money laundering program requirements for casinos*.
 - (1) FinCEN Form 112, *Currency Transaction Report*, must be filed by casinos and card clubs (as defined in 31 CFR 1010.100(t), *Financial institutions*) on each transaction in currency involving cash-in or cash-out of more than \$10,000. (31 CFR 1021.300, *General*)
 - (2) Transactions in currency involving cash-in include, but are not limited to:
 - a. Purchases of chips, tokens and other gaming instruments,
 - b. Front money deposits,
 - c. Safekeeping deposits,
 - d. Payments on any form of credit, including markers and counter checks,
 - e. Bets of currency, including money plays,
 - f. Currency received by a casino for transmittal of funds through wire transfer for a customer,
 - g. Purchases of a casino's check, or
 - h. Exchanges of currency for currency, including foreign currency. (31 CFR 1021.311(a), *Transactions in currency involving cash in*)
 - (3) Transactions in currency involving cash-out include, but are not limited to:
 - a. Redemptions of chips, tokens, and other gaming instruments,
 - b. Front money withdrawals,
 - c. Safekeeping withdrawals,
 - d. Advances on any form of credit, including markers and counter checks,
 - e. Payments on bets,
 - f. Payments by a casino to a customer based on receipt of funds through wire transfer for credit to a customer,
 - g. Cashing of checks or other negotiable instruments,
 - h. Exchanges of currency for currency, including foreign currency,
 - i. Travel and complimentary expenses and gaming incentives, or
 - j. Payment for tournament, contest or other promotions. (31 CFR 1021.311(b), *Transactions in currency involving cash out*)
 - (4) Multiple currency transactions shall be treated as a single transaction if the casino has knowledge that they are by or on behalf of any person and result in either cash-in or cash-out totaling more than \$10,000 during any gaming day. (31 CFR 1021.313, *Aggregation*) Transactions in and out do not offset each other for reporting purposes. Transactions in and out are separately aggregated but can be reported on a single CTR form for the same gaming day.
 - (5) Casinos must file a CTR within 15 calendar days following the day the reportable transaction occurs. (31 CFR 1010.306(a)(1), *Filing of reports*)
 - (6) FinCEN Form 111, *Suspicious Activity Report*, must be filed by casinos and card clubs (as defined in 31 CFR 1010.100(t), *Financial institution*) for any suspicious transaction relevant to a possible violation of law or regulation. A transaction requires reporting if it is conducted or attempted by, at, or through a casino, involves or aggregates funds or other assets of at least \$5,000, and the casino knows, suspects, or has reason to suspect that the transaction (or pattern of transactions): involves funds derived from illegal activity, is designed to evade any recordkeeping or reporting requirements of the BSA, serves no

business or apparent lawful purpose and/or the person is trying to use the casino to facilitate criminal activity, including terrorist activity.

- (7) Casinos are required to file a SAR no later than 30 calendar days after the date of the initial detection of facts that constitute a basis for filing a SAR. (31 CFR 1021.320(b)(3), *When to file*) If no suspect is identified at initial detection, an additional 30 days is allowed to identify the subject, but in no case shall reporting be delayed more than 60 calendar days. Additionally, casinos must immediately notify, by telephone, an appropriate law enforcement authority in addition to filing timely a SAR for situations involving violations that require immediate attention, such as, for example, ongoing money laundering schemes. For transactions that may be related to terrorist activity, casinos are encouraged to call FinCEN's Financial Institutions hotline at 1-866-556-3974 in addition to filing timely the suspicious activity report.
- (8) Casinos are generally prohibited from disclosing a SAR or any information that would reveal the existence of a SAR. (31 CFR 1021.320(e), *Confidentiality of SARs*) This applies to all directors, officers, employees, or an agent of any casino. Provided that no person involved in any reported SAR is notified that the transaction has been reported, casinos are not prohibited from disclosing a SAR, or any information that would reveal the existence of a SAR, to FinCEN or any Federal, State, or local law enforcement agency, or any Federal regulatory authority that examines the casino for compliance with the BSA, or any State regulatory authority administering a State law that requires a casino to comply with the BSA or otherwise authorizes the State authority to ensure a casino's compliance with the BSA, or any tribal regulatory authority administering a tribal law that requires a casino to comply with the BSA or otherwise authorizes the tribal regulatory authority to ensure the casino's compliance with the BSA. Casinos are not prohibited from disclosing the underlying facts, transactions, and documents upon which a SAR is based to another financial institution, or any director, officer, employee, or agent of a financial institution, for the preparation of a joint SAR or the sharing of information that would reveal the existence of a SAR within your corporate organizational structure for purposes consistent with the BSA.
- (9) FinCEN Form 105, *Report of International Transportation of Currency or Monetary Instruments (CMIR)*, must be filed by any person who transports, mails, ships, has someone else transport, mail, or ship currency or monetary instruments in excess of \$10,000 into or out of the country or who receives such items into the United States from abroad. (31 CFR 1010.340, *Reports of transportation of currency or monetary instruments*) A CMIR is filed with the Bureau of Customs and Border Protection. The IRS has no delegation authority to examine for CMIR compliance. The United States Customs Service has been delegated authority by the U. S. Treasury Assistant Secretary (Enforcement) to examine for compliance of 31 CFR 1010.340 (31 CFR 1010.810(b)(7)) and investigate criminal violations of 31 CFR 1010.340. (31 CFR 1010.810(c)(1)) If a BSA examiner has knowledge that an entity or a customer has failed to file a CMIR, the examiner should contact the local office of the U.S. Customs Service or call 1-800-BE-ALERT. The BSA examiner will not secure a delinquent CMIR. Interview questions regarding the movement of funds including cash anywhere (including in or out of the U.S.) is an integral part of understanding the casino's overall operations and how they may conduct transactions on behalf of their customers. These questions are not for confirming CMIR compliance but rather understanding the casino's procedures.

If possible CMIR non-compliance is subsequently identified, the examiner should contact the US Customs Service.

- (10) FinCEN Form 114, *Report of Foreign Bank and Financial Accounts (FBAR)*, must be electronically filed for any financial interest in or signature or other authority over a bank, securities, or other financial account which exceeds \$10,000 at any time during the calendar year. (31 CFR 1010.350, *Reports of foreign financial accounts*)
- (11) For foreign financial accounts maintained during calendar years 2015 and earlier, the FBAR must be filed by June 30th of the succeeding year. (31 CFR 1010.306(c), *Reports required to be filed*) The annual due date for filing FBARs required for foreign financial accounts maintained during calendar years 2016 and later, is April 15 of the following year. This date change was mandated by the Surface Transportation and Veterans Health Care Choice Improvement Act of 2015, Public Law 114-41 (the Act). Specifically, section 2006(b)(11) of the Act changes the FBAR due date to April 15. FinCEN will grant filers failing to meet the FBAR annual due date of April 15 an automatic extension to October 15 each year. When the April or October due date falls on a Saturday, Sunday, or legal holiday, the due date is delayed until the next business day.

4.26.9.3.3.2
(11-12-2019)
**Recordkeeping
Requirements**

- (1) For records required of all financial institutions, refer to IRM 4.26.5, *Bank Secrecy Act History and Law*.
- (2) Casinos are required to retain a copy of each CTR filed for five years from the date of the report. (31 CFR 1010.306(a)(2), *Filing of reports*) A casino may electronically save the filing to a computer hard drive, a network drive, or other appropriate storage device.
- (3) Casinos are required to maintain a copy of any SAR filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR. (31 CFR 1021.320(d), *Retention of records*) Casinos must make this available to appropriate regulatory authorities upon request.
- (4) All records created from the AML Program Requirements must be retained by casinos for five years.
- (5) Casinos are required to secure and maintain a record of the name, permanent address, and social security number of each person who deposits funds, opens an account or establishes a line of credit at the time the funds are deposited, the account is opened, or credit is extended. (31 CFR 1021.410(a), *Additional records to be made and retained by casinos*) This record keeping requirement has no dollar threshold criteria, so it applies no matter how small the value of an account. This record may be maintained anywhere in the casino records. It is not required to be a separate record.
- (6) Casinos are required to maintain a record of each receipt (including but not limited to funds for safekeeping or front money) of funds for the account (credit or deposit) of any person. (31 CFR 1021.410(b)(1)) The record must include the name, permanent address and social security number of the person from whom the funds were received, as well as the date and amount of the funds received. If the person from whom the funds were received is a nonresident alien, the person's passport number or a description of some other government document used to verify the person's identity must be obtained and recorded.

- (7) Casinos are required to maintain a record of each bookkeeping entry comprising a debit or credit to a customer's deposit account or credit account with the casino. (31 CFR 1021.410(b)(2))
- (8) Casinos are required to maintain each statement, ledger card or other record of each deposit account or credit account with the casino, showing each transaction (including deposits, receipts, withdrawals, disbursements or transfers) in or with respect to, a customer's deposit account or credit account. (31 CFR 1021.410(b)(3))
- (9) Casinos are required to maintain a record of each extension of credit in excess of \$2,500, the terms and conditions of such extension of credit, and repayments. (31 CFR 1021.410(b)(4)) The record shall include the customer's name, permanent address, social security number, and the date and amount of the transaction (including repayments).
- (10) Casinos are required to maintain a record of each advice, request or instruction received or given by the casino for itself or another person with respect to a transaction in any amount involving a person, account or place outside the United States (including but not limited to communications by wire, letter, or telephone). (31 CFR 1021.410(b)(5)) If the transfer outside the United States is on behalf of a third-party, the record must include the third-party's name, permanent address, social security number, signature, and the date and amount of the transaction. If the transfer is received from outside the United States on behalf of a third-party, the record shall include the third-party's name, permanent address, social security number, signature, and the date and amount of the transaction.
- (11) Casinos are required to maintain records prepared or received in the ordinary course of business which would be needed to reconstruct a person's deposit account or credit account or to trace a check deposited with the casino through the casino's records to the bank of deposit. (31 CFR 1021.410(b)(6)) This regulation does not require the creation of a record. It does require the retention of a record if a record was prepared or received by the casino. For example, if a casino scanned or made copies of checks received from customers but failed to maintain the images of these checks then the casino would be in violation of 31 CFR 1021.410(b)(6).
- (12) Casinos are required to maintain all records, documents or manuals required to be maintained by the casino under state and local laws or regulations, regulations of any governing Indian tribe or tribal government, or terms of (or any regulations issued under) any Tribal-State compacts entered pursuant to the Indian Gaming Regulatory Act. (31 CFR 1021.410(b)(7)) This regulation does not require the creation of a record. It does require the retention of a record if a record was prepared or received by the casino. For example, if a casino created a required state or tribal gaming transaction record but failed to maintain the record then the casino would be in violation of 31 CFR 1021.410(b)(7). Conversely, if the casino violated the state or tribal requirement to create the record then there is no violation of 31 CFR 1021.410(b)(7).
- (13) Casinos are required to maintain all records which are prepared or used by the casino to monitor a customer's gaming activity. (31 CFR 1021.410(b)(8))
- (14) Casinos must retain a separate record containing a list of each transaction between the casino and its customers involving certain types of negotiable in-

struments having a face value of \$3,000 or more. This list must include negotiable instruments issued by the casino to its customers and negotiable instruments received by the casino from its customers. (31 CFR 1021.410(b)(9)) These negotiable instruments include personal checks (excluding personal checks solely used as collateral), business checks (including casino checks), official bank checks, cashier's checks, third-party checks, promissory notes, traveler's checks and money orders. The list must contain the time, date, and amount of the transactions; the name and permanent address of the customer; the type of instruments; the name of the drawee or issuer of the instrument; all reference numbers (for example, casino account number, personal check number, and others); and the name or casino license number of the casino employee who conducted the transaction. Applicable transactions must be placed on the list in the chronological order in which they occur.

- (15) Card clubs must maintain records of all currency transactions by customers, including without limitation, records in the form of currency transaction logs and multiple currency transaction logs, and records of all activity at cages or similar facilities, including, without limitation, cage control logs. (31 CFR 1021.410(b)(11))
- (16) Casinos which input, stored, or retained, in whole or in part, for any period, any BSA required record on computer disk, tape, or other machine-readable media must retain the same on computer disk, tape, or machine-readable media. (31 CFR 1021.410(c)(1))
- (17) Casinos must retain all indexes, books, programs, record layouts, manuals, formats, instructions, file descriptions, and similar materials which would enable a person to readily access and review required records that are input, stored, or retained on computer disk, tape, or other machine-readable media. (CFR 1021.410(c)(2))

4.26.9.3.3.3
(11-12-2019)
**AML Program
Requirements**

- (1) All casinos must establish and implement a written, risk-based AML program reasonably designed to prevent the casino from being used to facilitate money laundering and the financing of terrorism.
- (2) At a minimum, the program shall:
 - a. Incorporate policies, procedures, and internal controls reasonably designed to assure compliance with the BSA and its implementing regulations,
 - b. Designate a compliance officer,
 - c. Provide for education or training of appropriate personnel,
 - d. Provide for independent review to monitor and maintain the adequacy of the program,
 - e. Provide for procedures to use all available information to verifiably determine the name, address, social security number and other information of a person; the occurrence of any suspicious transactions or patterns of transactions required to be reported and whether any record must be made and retained, and
 - f. Provide for the inclusion of existing automated programs in the policies, procedures and internal controls to aid in assuring compliance. (31 CFR 1021.210)

4.26.9.3.4
(11-12-2019)
Records Commonly Found

- (1) Casino accounting systems related to gaming operations of a casino are generically referred to as casino management systems. These systems are separate from the traditional general ledger systems used to track income and expenses for business and tax purposes, although certain summarized information will flow to the general ledger. A typical casino management system is usually a hybrid system made up of financial accounting records, banking-style deposit, credit records, and non-financial marketing records. In some small casinos, systems may involve the use of manual records. Larger casinos tend to utilize complex and automated computerized systems. Even the smallest casinos have computerized their systems as a low-cost and efficient means of recordkeeping and marketing. Casino oriented software is commercially available from several manufacturers for use on stand-alone or networked desktop computer systems. Casino records that can be used to identify customer transactions will vary depending upon state tribal, and local laws and regulations, as well as the needs of casino management.
- (2) A typical casino management system will have many components, but the most relevant are:
 - a. Casino Marketing System
 - b. Credit Management System
 - c. Customer Master File

4.26.9.3.4.1
(11-12-2019)
Casino Marketing System

- (1) The casino marketing system is used to track customer gaming activities and generally referred as player ratings. Most player ratings are associated table games and slots. Generally, other gaming departments such as poker, race and sports, bingo, and keno have limited tracking details and are included within the marketing system. Casinos often offer incentives to customers to entice them to increase their gaming activity. Typically, the incentives are offered through a player's club system where customers earn points based on their play. Points can often be redeemed for food, beverage, rooms, free play and even cash. Casino revenue is mostly derived from slots and table games. Therefore, player tracking, and monitoring will generally focus on these two departments.
- (2) Table games player tracking is exclusively monitored through observation. A designated casino employee who monitors a customer's play will usually complete a player rating slip or inputs player information by swiping players card or some manual process directly into a computerized table games system each time a rated player begins gaming activity at a table. The employee keeps track of the customer's buy-ins, average bets, style of play, wins/losses, and others. Casinos often utilize player ratings for marketing purposes, however, the information gathered for marketing purposes is critical and can be used for detection of reportable currency transactions and possible identification of reportable suspicious activity. Table games player rating information generally includes:
 - Customer Account Number
 - Date of Rating
 - Time Rating Began; Time Rating Ended
 - Pit where rating occurred; Table where rating occurred
 - Type of Game Played
 - Average Bet

- Cash Buy-in Amount; Chip Buy-in Amount; Credit Buy-in Amount
- Chips Out (often associated with Chip Walk)
- Estimated Win or Loss

(3) Slot play is almost always tracked electronically through the slot computerized system. Casinos usually facilitate player tracking through a player's club system. A customer wishing to be rated will obtain a player's club card. This card could be used in all gaming departments depending on the casino's marketing program. These cards are often inserted in the slot machine and track the customer's play. The player's club system will gather information such as bill-in, coin-in, number of games or hands played, jackpots, or coin-out. Slot ratings are primarily used by the casino to determine the slot machine performance and customer's gaming play. For BSA purposes the slot ratings can be used to review customers' gaming play. It is important to understand that coin-in and bill-in are entirely different. Coin-In is associated with actual wagers whereas bill-in is associated with actual currency accepted by the slot machine. Most slot computerized systems have the ability to track customers' currency placed in the bill acceptor and slot tickets produced by the slot machine with carded play. Slot bill-in information provides valuable information for reportable currency transactions. Slot rating information generally includes:

- Customer Account Number
- Date of Rating
- Time Rating Began
- Time Rating Ended
- Location
- Coin In
- Coin Out
- Jackpots
- Actual Win ((Coin In - Coin Out) Less Jackpots)
- Theoretical Win (Based on hold percentage)
- Type of wagers played
- Average Bet

4.26.9.3.4.2
(11-12-2019)

Credit Management System

(1) A Credit Management System (CMS) is a financial accounting system used to record and track customer account transactions including deposits, deposit withdrawals ("front money accounts"), credit issuances ("markers issuance"), and credit payments ("marker redemptions"). While many files make up a credit management system, the two files that are important for currency transaction reporting, recordkeeping requirements, and detection of potential suspicious activity are the Marker Detail File and the Front Money File, further explained below.

(2) A Marker Detail File is a file that includes separate records of each individual marker issued and redeemed. The file details, in chronological order, the issuance of a marker and its eventual disposition (payment, deposit or write-off). The marker detail file generally includes the following:

- Customer account number
- Marker number
- Date issued
- Time issued
- Pit/Table/Machine number where issued
- Type of marker (Table/Slot)
- Amount of the marker

- Date redeemed
- Time redeemed
- Amount paid by cash
- Amount paid by chips
- Amount paid by check
- Amount paid by front money or wire transaction
- Identity of employee that conducted the transaction

(3) A Front Money File is a file that includes records of each deposit and withdrawal. Deposits and withdrawals are generally made at the cage. However, customers can withdraw front money funds at the pit in the form of chips or at the slot high limit area in the form of cash or purchase tickets. The front money file contains, in a chronological order, a customer's deposit and withdrawal activity. The file generally includes:

- Customer Account Number
- Date transaction
- Time of transaction
- Gaming department where the transaction was conducted
- Identity of employee who conducted the transaction
- Type of Transaction Conducted
- Voucher Number
- Amount of cash involved
- Amount of chips involved
- Number of negotiable instruments involved
- Amount of wires in/out

4.26.9.3.4.3 (11-12-2019) **Customer Master File**

(1) A customer master file is used to record personal information about individual customers. The casino creates a customer master file record when a customer opens any type of account with the casino. Generally, a customer will only have one master file record and one account number assigned. Consequently, where a customer maintains a deposit account, credit account, player rating account and slot club account, the casino will use the same account number to track all of the customer's gaming activity. The customer's name, address, identification and social security number should always be recorded for deposit and/or credit accounts as they are required by the recordkeeping requirements. (31 CFR 1021.410, *Additional records to be made and retained by casinos*) However, for customers who only maintain a player rating and/or slot club account, the customer master file may only include the customer's name, address, and identification. Information in the customer master file record typically contain dozens or more than a hundred data fields for each single customer. The data fields relevant to BSA for each customer generally include but are not limited to the following:

- Customer Account Number
- Customer Name
- Residential Address
- Business Address
- Social Security Number
- Identification (Government Issued)
- Passport Information (Aliens)
- Date of Birth
- Employer (associated with credit approval)

- Occupation (associated with credit approval)
- Annual Income (associated with credit approval)
- Assets and Liabilities (associated with credit approval)
- Bank Account Information (associated with credit approval)
- Credit History
- Telephone Number
- Aliases Used (if known)

- (2) Generally, transactions occurring on the gaming floor can be identified through casino Player Rating Systems and/or Multiple Transaction Logs (MTLs), while transactions occurring at the cage can be identified through the casino CMS and other cage records which may also include MTLs.

4.26.9.3.4.3.1
(11-12-2019)

Multiple Transaction Logs

- (1) Multiple Transaction Logs (MTLs) are often maintained in the pit, cage, or slot areas pursuant to state, tribal, or local laws. MTLs are used to record currency transactions above a given threshold, usually \$2,500 - \$3,000. On these logs, casinos typically record customers' purchases and redemptions of chips or tokens with currency or bets of currency. BSA regulations require the creation of MTLs for card clubs, 31 CFR 1021.410(b)(11), *Additional records to be made and retained by casinos*, but do not specifically require the creation of MTLs (although the retention of these records, if made, is required) for other casinos. The BSA regulations, however, do require all casinos to monitor for structured transactions, 31 CFR 1021.210(b), *Compliance programs* and 31 CFR 1021.320(a)(2)(ii), *Reports by casinos of suspicious transactions*, for which MTLs provide such a method. MTL use, format, and required information will vary from jurisdiction to jurisdiction. Casinos may use computerized MTLs and link transactions from various gaming departments. Manual MTLs are individual logs maintained by each gaming department. Information recorded on the log for currency transactions generally includes:

- Date of Transaction
- Time of Transaction
- Location (Pit/Table/Cage Window Number)
- Transaction
- Cash-in or Cash-Out Amount
- Customer Account
- A physical description of the customer usually including height, weight, approximate age, hair color, eye color, clothing, and distinguishing features
- Identity of employee who recorded the transaction

- (2) While MTLs identify certain currency transactions associated with customers, they do not always identify the customer by name. Often, only a vague physical description of the customer is recorded on the MTL. The customer will usually have a designation of "unknown" or "refused".

- (3) In addition to the required MIL or Negotiable Instruments Log (NIL) (31 CFR 1021.410(b)(9)) casinos often maintain the following records (which may or may not be computerized):

- Cage Reconciliation Report
- Marker Log
- Front Money and Safekeeping Logs
- Wire Transfer Log
- Cage Checks Issued Register

- Bank Statements
- Form W-2G and/or Form 1099 Issued Log
- Surveillance Logs of activities that are unusual, suspicious or potentially criminal
- Slot Tickets Redemptions
- Credit - Debit Transaction Reports
- Mail-In Marker Payments

- (4) In most casinos, these systems may be highly computerized, and the records may be computer-generated. Casino records that are processed by or through a computer must be retained by the casino in machine-readable form. See 31 CFR 1021.410(c)(1), *Additional records to be made and retained by casinos*.

4.26.9.3.5 (11-12-2019)

Pre-Audit, Interview and Tours

- (1) The pre-plan of a casino examination will include the development of an audit plan. The audit plan should cover all areas that conduct, monitor and review gaming activity. When developing the audit plan, the examiner must consider the size of the casino operation, types of gaming provided, types of financial services offered, types of records likely maintained, the casino's CTR and SAR filing history and any prior examination and affiliates' prior exam results. The scope and direction of the examination is determined by the audit plan and can vary case by case.
- (2) The pre-plan procedures will include:
- a. Performing a risk assessment
 - b. Determining the examination scope period (typically 3 months for a casino examination due to the significant amount of data)
 - c. Development of initial IDRs
 - d. Determining casino departments/employees to be interviewed
 - e. Designing interview outlines
 - f. Making initial contact with the casino to set first appointment
 - g. Performing FCQ research
 - h. Perform internet and other research on the casino
- (3) Prior to any contact with a tribal casino, the examiner must prepare a referral for an ITG Specialist. ITG is the official IRS designated contact for all federally recognized Native American tribes. Referrals are made through the SRS. A referral is created by going to <https://srs.web.irs.gov/>. Once a referral is approved and processed, an ITG manager will assign the referral to the ITG specialist that covers the Indian tribe operating the casino. The ITG specialist will coordinate with the BSA examiner and will attend the opening and closing conferences if possible. The ITG specialist will provide BSA examiner with information about the tribe, such as certain protocols to follow in dealing with the tribe. The ITG specialist does not assist in the Title 31 examination.
- (4) A critical process in the scoping and planning phase (pre-audit) of a BSA casino examination is an extensive review and analysis of all BSA reports filed by and on the casino. A thorough review and analysis of the BSA reports filed by the casino is used to determine the adequacy of the reports as well as identifying trends in the reports. A BSA report is deemed adequate if it is timely, complete, and accurate. The preliminary determination of the timeliness of CTRs is easily and routinely accomplished in the pre-audit phase of an examination. The determination of the timeliness of SARs, however, typically

requires a review of internal casino documentation later in the examination. An examiner will review and analyze a casino's broad historical trends as well as detailed transaction trends of filed BSA reports for the current time period. Although there are no targeted volumes of CTRs or SARs, overall filing history trends and data trends in the reports are compared to other data such as gross annual gaming revenue, types of gaming offered, and types of transactions offered. This comparison combined with a review of the casino's AML program is then used by the examiner to facilitate the scope and planning of the examination.

- (5) As part of the initial contact, the examiner will determine what records the casino maintained, and which records need to be requested. Some but not all records will be required to be reviewed by the examiner prior to the initial appointment. Both the initial IDR and the computerized IDR (IDR requesting computerized records) are issued with initial appointment Letter 3494, *Bank Secrecy Act (Title 31) Casino Appointment Letter*. Both IDRs include records to be provided prior to the initial appointment and records to be available at the initial appointment.
- (6) Discuss the IDR items with the IT contact person to ensure they understand the casino data to be provided electronically.
- (7) The initial interview should be held at the casino's place of business and should be attended by all IRS personnel who will be involved in the examination including the examining agent, assisting agents ITG Specialist (if the casino is a tribal casino) and the examination case manager.
- (8) A CAS may be requested if the casino's computerized data is not available in a file format or size that an examiner can use.
- (9) The appointment letter should request that the following casino personnel attend the initial meeting:
 - a. Vice President Finance,
 - b. Casino Controller,
 - c. Casino Manager,
 - d. Casino Cage Manager,
 - e. Director of Information Systems (Computers),
 - f. Title 31 Compliance Office, and
 - g. Any directly involved in Title 31 compliance.
- (10) The casino should be advised of the purpose of the examination, and any questions should be answered. Physical arrangements should be made for adequate work space and access to necessary equipment. A principal contact person from the casino and a casino IT contact person should be identified for the examining agent.
- (11) The casino should be advised that examining agent(s) will only review information relative to BSA compliance. However, it should also be advised that if during the examination, information relative to possible violations of other laws or regulations is discovered, a referral must be made. This notification should be documented.
- (12) The interview should identify any related institutions, branches, entities, or other NBFIs operating within the casino including ownership and relationship of

MSBs and ATMs. The BSA examiner should immediately submit the information to the BSA Exam Case Selection (ECS) casino coordinator to be added to the Title 31 database.

- (13) Determine the gaming day used by the casino for aggregating reportable currency transactions. Record whether the casino cage and gaming floor are both using the same gaming day cut-off time (including the computerized player rating system) as required by 31 CFR 1021.100(d), *Gaming day*. Request that the casino provide a document at the start of the examination that cites the opening and ending times for the gaming day that are in effect during the period being examined.

Note: For purposes of aggregating reportable currency transactions, a casino must have only one gaming day which is common to all its gambling operating divisions or departments (such as, cage and floor).

- (14) Ask open-ended questions throughout the interview. Do not ask questions that require only a “yes” or “no” answer.
- (15) The examination should include departmental interviews. Each interview should be documented in the case file. Owners/operators, shareholders, directors, floor and cage managers, and employees responsible for preparing currency reports and securing and maintaining records pertaining to the reporting requirements under the BSA should be questioned as to their knowledge and training of the BSA recordkeeping and reporting requirements. Knowledge is one of the elements needed to prove willfulness with respect to a violation of the regulations. Examples of possible casino personnel to be interviewed include:

- Title 31 Compliance Officer
- Casino Controller
- IT Manager/Supervisor
- Internal Auditor
- Revenue Auditor
- Cage Manager/Supervisor/Cashier
- Surveillance Manager/Supervisor/Officer
- Table Games Manager/Supervisor
- Poker Room Manager/Supervisor
- Slot Manager/Supervisor/Attendant
- Off-Track Betting Manager/Supervisor/Cashier
- Bingo Manager/Supervisor/Cashier
- Keno Manager/Supervisor
- Security Manager/Supervisor/Officer
- Marketing Manager/Supervisor
- Guest Services (Players Club) Attendant
- Tribal Gaming Commission Member

- (16) A guided tour of the casino operation is essential and should be scheduled as early in the examination as possible. The examiner must understand the casino’s operation and layout. It is important the tour include all areas both on and off the gaming floor. Areas of attention should be the cage, pit, surveillance, compliance and any high-stake limit areas. Enough time must be spent observing employees conducting transactions, compiling and reviewing reports.

The types of documents completed, any reviews conducted on these documents and subsequent processing of these documents must be understood.

4.26.9.3.6
(06-01-2006)

Systems Analysis

- (1) Because casino records will vary depending upon applicable laws and regulations, as well as the needs of casino management, a complete systems analysis should be conducted of the casino accounting system used to record and process records related to customer transactions. This analysis will establish the audit trail and the casino's knowledge of BSA requirements pertaining to reportable transactions. The analysis should include:
 - a. Identifying the flow of information through the system,
 - b. Determining what kinds of original source documents and records are prepared relative to customer transactions, who prepares them, and how they are stored and organized,
 - c. Determining what records are prepared by the casino that specifically identify customer currency transactions,
 - d. Determining the kinds of reports prepared by the casino in the ordinary course of its business that may identify and/or summarize recorded, customer transactions, particularly currency transactions, and
 - e. Determining what kind of records and reports are prepared by the casino that identify customers who may be structuring transactions to evade CTR reporting requirements, or who are engaging in other unusual or suspicious transactions or patterns of such transactions.
- (2) If the casino accounting systems are computerized, the examiner should determine:
 - a. What computer files and records are maintained relative to customer transactions and what information is stored in those files and records,
 - b. What computer files and records are prepared that specifically identify customer currency transactions including currency specific transactions,
 - c. Whether the casino has retained those records in accordance with the BSA recordkeeping and record retention requirements, and
 - d. What kinds of computer-generated reports are prepared by the casino in the ordinary course of its business that may identify and/or summarize recorded customer transactions, particularly currency transactions and potentially suspicious transactions.
- (3) Examiners should familiarize themselves with state, tribal, and local laws and regulations related to any casino being examined since BSA relevant records, documents or manuals required by these jurisdictions are also required to be maintained and utilized for BSA compliance (31 CFR 1021.210(b)(2)(v), *Compliance Programs*, and 31 CFR 1021.410(b)(7)). Attention should be placed on casino records, documents, and reports required by those laws and regulations which may assist in detecting currency transactions, suspicious transactions, and establishing the casino's knowledge of those transactions.

4.26.9.3.7
(11-12-2019)

Review of Records

- (1) Examination techniques used to conduct BSA examinations of casinos will vary significantly depending upon whether the casino inputs and processes its customer transaction records by or through a computer system and has retained those records in machine readable form as required by the BSA. (31 CFR 1021.410(c)(1), *Additional records to be made and retained by casinos*) Even the smallest of casinos have begun to automate their casino systems as

a low cost and efficient means of recordkeeping and marketing. However, some casinos may still maintain only manual records for certain transactions. All casinos typically maintain manual backup procedures in the event its computers go down.

- (2) The four major areas of a casino examination are:
- Review and analysis of the AML program (31 CFR 1021.210)
 - Determining CTR compliance (31 CFR 1021.310, *Reports of transactions in currency*)
 - Determining SAR compliance (31 CFR 1021.320, *Reports of transaction in currency*)
 - Determining recordkeeping compliance (31 CFR 1010.410, *Records to be made and retained by financial institutions*, and 31 CFR 1021.410, *Additional records to be made and retained by casinos*)
- (3) A review and analysis of a casino's AML program should begin prior to the initial interview and continue throughout the examination. A review is critical in planning the scope and depth of examinations. Examiners must determine if the written policies and procedures are implemented and effective. Examiners will also consider the implementation and effectiveness of any unwritten policies and procedures. The BSA regulations do not specify the degree of detail and allow for customization of policies and procedures to mitigate AML risks. It is not a program violation if the written AML program lacks every specific detail of a casino's procedures but there must be enough documentation for efficacy. AML policies and procedures can vary greatly especially the frequency and depth of reviewing records and reports. Variations of different procedures can accomplish the same risk mitigation outcome. Contingent upon BSA risks, an AML program is deficient if:
- an entire AML program pillar is missing,
 - a policy or procedure does not exist, or
 - if a policy does exist (written or unwritten) but fails to be followed (isolated or systemic) or fails to ever be implemented.
- Note:** Examiners must identify if an AML program breakdown, weakness, or deficiency was the cause of any reporting or recordkeeping violation.
- (4) Determining CTR compliance is one of the four major areas of a casino examination. Examiners must determine if:
- CTRs were filed timely,
 - CTRs were filed with complete and accurate information,
 - Copies of CTRs were maintained, and
 - Any CTRs were not filed.
- (5) A review and analysis of filed CTRs begins during pre-audit and continues throughout the examination. A review and analysis of manual and computerized casino records that document cash-in or cash-out transactions (MTLs, MILs, cage and credit transactions, slot data) will be conducted to determine if any CTRs were not filed or have any inaccuracies including the total dollar amount reported. Examiners must identify any amended or back-filed CTRs. Amended and back-filed CTRs must be removed from the list of potentially late filed reports. Although not considered late filed CTRs, any amended and back-

filed CTRs may provide examiners with information on areas of risk. Examiners need to determine the cause of amended or back-filed CTRs and whether the casino's policies and procedures were inadequate. It is also important to determine if the casino amended their procedures to correct any deficiencies which caused subsequent amended or back-filed CTRs. Zero amended CTRs may indicate a lack of procedures to correct inaccurate or incomplete CTRs filed in an after-the fact aggregation.

- (6) Before citing a casino for failure to file a CTR, examiners must prove a reportable transaction occurred. A reportable transaction occurs when the following criteria are met:
 - a. The customer's transaction(s) occurred during the casino's specified gaming day,
 - b. The customer's transaction(s) involved cash in or cash out of over \$10,000, and
 - c. The casino had knowledge of the transaction(s).
- (7) Determining SAR compliance is another one of the four major areas of a casino examination. Examiners must determine if:
 - a. SARs were filed timely,
 - b. SARs were filed with complete and accurate information,
 - c. Copies of SARs and the supportive documentation were maintained and protected from disclosure, and
 - d. Any SARs were not filed.
- (8) The analysis of filed SARs combined with the analysis of the AML program policies and procedures can determine the techniques used to examine for unreported suspicious activity. The following examples of SAR filing trends could identify possible SAR monitoring vulnerabilities and thereby cause an adjustment to the examination plan:
 - a. None or few SARs are filed with certain likely suspicious activity types. For example, if there is "suspicious use of non-cash monetary instruments" that has never been reported, the casino could be vulnerable to not monitoring and reporting for this type of activity.
 - b. Most or all SARs filed are completed transactions instead of attempted transactions or vice versa.
 - c. Most or all SARs filed are on transactions occurring in the cage instead of the gaming floor or vice versa.
 - d. Most or all SARs are filed on transactions in a single gaming floor area instead of all gaming areas. For example, gaming floor SARs have only been initiated from table game and slot transactions but never from race and sports book transactions.
 - e. Most or all SARs filed are from real time observations instead of a review of records or vice versa. The examiner will determine if a real time suspicious activity observation could have been detected from a review of records and if not then why and vice versa.
 - f. Most or all SARs filed are for activity in a single gaming day instead of over a broader period or vice versa.
 - g. None or few SARs have ever been amended.
 - h. None or few SARs are filed on continuing activity.
- (9) Determining recordkeeping compliance is another one of the four major areas of a casino examination. A casino creates millions of records each year and an

examiner must determine what records a casino is required to maintain. 31 CFR 1021.410 and 31 CFR 1010.410 identifies records that a casino must create and/or maintain. The regulations specifically state the information required to be obtained and maintained by the casino. If a casino provides one of the services covered by the regulations, they have a requirement to create and maintain the records prescribed in the regulation. A casino does not have a recordkeeping requirement for services it does not offer. For example, if the casino does not offer wire transfers, it does not have to create a wire listing or log.

- (10) For each deposit of funds, extension of credit, or account opened by the casino, the BSA requires that the casino obtain the customer's name, permanent address and SSN. (31 CFR 1021.410(a)) The name and address must be verified and recorded in the manner described in 31 CFR 1021.312, *Identification required*. Examiners should determine whether the casino's procedures for opening deposit and credit accounts include requirements for securing the customer's name, permanent address, and social security number and verifying the name and address. Additionally, customer deposit and credit accounts should be reviewed to determine if the required information has been obtained. If the casino is unable to obtain the SSN for a customer opening a debit or credit account, the casino is not deemed to be in violation of this recordkeeping requirement if:
 - a. A reasonable effort was made to secure the number, and
 - b. The casino maintains a list containing the names and permanent address of those customers without SSNs and makes the list available to the Secretary upon request. (31 CFR 1021.410(a))
- (11) Examiners should determine whether the casino's retention policies have measures to retain all records described in 31 CFR 1021.410(b) and if the required records are being retained for the BSA's five-year retention period. Examples include, but are not limited to:
 - a. Failure to maintain the \$3,000 MIL (31 CFR 1021.410(b)(9),
 - b. Destruction of player rating records reflecting currency transactions (31 CFR 1021.410(b)(8), and
 - c. Destruction of every debit and credit affecting a customer's debit account. (31 CFR 1021.410(b)(2))
- (12) Examiners should determine whether the casino has procedures to maintain a chronological record (commonly known as the MIL or NIL) of monetary instruments received or issued with a face value of \$3,000 or more. (31 CFR 1020.410(b)(9)) The information required is:
 - a. The time,
 - b. The date,
 - c. Customer name,
 - d. Customer permanent address,
 - e. The type of instrument,
 - f. The name of the drawee or issuer of the instrument,
 - g. All reference numbers such as casino account number and/or personal check number, and
 - h. The employee name or business license number.

The list should be reviewed or tested to determine if the required information has been obtained. Examiners can compare the MIL against the casino's computerized records of customer transactions to identify whether large transactions recorded in the computer as potential "cash" transactions have been accounted for instead of as check transactions. In addition, MIL entries can help identify a customer who may be structuring transactions to evade CTR reporting through currency purchases of multiple checks in amounts of \$3,000 to \$10,000 at different times during a gaming day.

- (13) Some casinos use their own bank accounts to wire funds on behalf of their customers and/or they may have contracts with MSB companies that provide fund transfer services. If the casino wires, or otherwise transfers funds for its customers (or receives wired funds or other such fund transfers on behalf of its customers), and the amount of the transfer is \$3,000 or more, the casino is required to maintain certain records of the funds transfer. (31 CFR 1010.410(f) and 31 CFR 1010.410(g)) Examiners should determine whether the casino's procedures for recording funds transfers in amounts of \$3,000 or more include requirements for verifying customer identification, and for recording customer and transaction information for each money transfer. The records should be reviewed or tested to determine if the required information has been obtained. Also, examiners can review the recorded information to help identify customers who may be structuring transactions through money transfers on a single day or over multiple days. In addition, the funds transfer records can be used in conjunction with each day's player rating records to determine if chips that were redeemed for an outgoing funds transfer, in excess of \$5,000, came from transactions involving minimal gaming. Casinos must maintain specific records for all international wire transfers to or from or on behalf of a customer. There is no dollar threshold for the recordkeeping requirement of international wire transfers. (31 CFR 1021.410(b)(5))

4.26.9.3.7.1
(06-01-2006)
Special Issues

- (1) Examiners should review branch office transactions to ensure that the casino has filed all required CTRs and SARs. Refer to IRM 4.26.9.3 for information on casino branch offices.
- (2) The BSA applies only to casino transactions, therefore, examiners should be alert to unusual transfers of currency between the casino cage and the hotel and other outlets of the casino complex. These outlets may routinely use the cage as a "bank" for depositing and withdrawing excess currency. An unusual transfer may indicate an attempt to circumvent the BSA reporting requirements. This is particularly important for cash-out transactions because the other outlets of the casino complex, which are subject to IRC 6050I reporting requirements, are only required to report cash-in transactions over \$10,000.
- (3) The BSA applies to all casino currency transactions, whether or not the transactions are related to the gaming activities being offered by the casino. Therefore, examiners should be alert to currency transactions between the casino and its vendors that may occur at the casino cage. Examples include the following:
 - a. Entertainment groups, who are usually paid with a casino check, may immediately cash the check at the casino cage to disburse the currency to the individual members.
 - b. Outside businesses, which are not related to the casino, may maintain booths in the casino complex for purposes of advancing currency to individuals by cashing checks, using credit cards, and other similar items.

These businesses often use the casino cage as their “bank” for depositing and withdrawing the currency needed to operate the booth.

- (4) Surveillance logs are a chronological log of activities that are unusual, suspicious or potentially criminal in nature that occur in a casino or card club. Surveillance logs typically contain:
- a. The date and time each surveillance commenced,
 - b. The name and license number of each employee who initiates, performs, or supervises the surveillance,
 - c. The reason for surveillance including the name, if known, alias, or description of everyone being monitored, and a brief description of the activity in which the individual being monitored is engaging,
 - d. The times at which each video or audio recording is commenced and terminated,
 - e. The time at which each activity which is unusual, suspicious or potentially criminal in nature is observed along with a notation of the reading on the control meter, counter, or device in the electronic surveillance system that identifies the point on the recording device (for example, audio or video tape, CD-ROM disc, DVD disc, and other similar items) at which such activity was recorded, and
 - f. The time surveillance was terminated; and summary of the results of the surveillance.

4.26.9.3.8
(06-01-2006)

Evidence

- (1) Examiners should obtain supporting documentation for each potential reporting, recordkeeping, and compliance program violation identified.
- (2) In the case of failures to file required CTRs, the supporting documentation may consist of copies of casino documents, prepared at the time of the transaction, that identify the type and amount of the transaction, the character of the transaction and the identity of the persons conducting the transaction. Such documents may include, but are not limited to, player rating cards, deposit and withdrawal slips, payment and redemption vouchers, customer action cards (also known as buckets), computer-generated reports and printouts of the preceding documents, Multiple Transaction Logs (MTLs), Forms W-2G, and computerized Form W-2G records. The documentation must support each finding that a reportable currency transaction has occurred but was not filed with the IRS.
- (3) In the case of incomplete CTRs, supporting documentation should consist of a duplicate of the casino’s retained copy of the CTR.
- (4) In addition, examiners should obtain supporting documentation establishing that the casino had knowledge that the transaction occurred in an amount greater than \$10,000 and in the form of currency.
- a. Single transactions - In the case of a single transaction, there is prima facie evidence of the casino’s knowledge because one employee conducted the transaction with the customer.
 - b. Multiple transactions - In the case of multiple transactions, knowledge must be established through casino reports and procedures.
- (5) If a report is prepared, manually or by computer, that aggregates and summarizes multiple currency transactions at the end of the gaming day, the casino

has knowledge of any reportable transactions identified in the report, even if the report is not specifically used for BSA reporting purposes.

- (6) If the casino has procedures in place to aggregate multiple currency transactions, the casino has knowledge of any reportable transactions that are identifiable through those procedures, whether or not the procedures are actually followed.
- (7) If it cannot be shown that the casino's employees had knowledge of any potential reporting or recordkeeping violations, the potential violations should be documented to support identified deficiencies in the casino's compliance program.
- (8) In the case of failures to file required SARs, the supporting documentation may consist of copies of casino documents, prepared at the time of the transaction, that identify the type and amount of the transaction, the character of the transaction and the identity of the person(s) conducting the transaction. Such documents may include, but are not limited to, credit slips/redemption vouchers, deposit/withdrawal slips, player rating records, computer-generated reports and printouts of the preceding documents, canceled checks, credit bureau reports, identification credentials, multiple transaction logs, \$3,000 monetary instrument list, money transfer records, slot club records, spreadsheets, photographs, surveillance audio and/or video recording media, surveillance logs, Forms W-2G, and computerized Form W-2Gs. The documentation must support each finding that a reportable suspicious transaction has occurred but was not filed with the SAR.
- (9) In addition, for failures to file SARs, examiners should obtain supporting documentation establishing that the casino knew, suspected, or had reason to suspect that the transaction:
 - a. Involved funds derived from illegal activity, or was intended or conducted to hide or disguise funds or assets derived from illegal activity,
 - b. Designed to evade BSA requirements, whether through structuring or other means,
 - c. Appeared to serve no business or apparent lawful purpose, and the reporting business knew of no reasonable explanation for the transaction after examining all available facts, or
 - d. Involved use of the reporting business to facilitate criminal activity and met reporting threshold of \$5,000 or more (in the single event or when aggregated).
- (10) In the case of incomplete SARs, supporting documentation should consist of a duplicate of the casino's retained copy of the SAR showing the failure to include all available and relevant information about the transaction found in the casino's records described in subparagraph (8) above.
- (11) In the case of incomplete records, supporting documentation should consist of a duplicate of the casino's retained copy of the records (such as credit slips/redemption vouchers, deposit/withdrawal slips, and \$3,000 monetary instrument list).
- (12) In the case of the failure to establish or implement a compliance program, the examination workpapers should contain the examiner's findings with respect to whether the casino failed to develop and/or maintain programs to detect and report large currency transactions or suspicious activities or keep required

records. Also, the workpapers should contain the examiner's findings with respect to any systemic breakdown of internal controls to assure compliance that was observed. In addition, the workpapers should contain the examiner's findings with respect to whether the appropriate casino officials were aware of compliance problems or deficiencies but did not take corrective action.

- (13) Examiners should also obtain supporting documentation that may show the casino employee's knowledge of the BSA reporting and recordkeeping requirements and the duty to file. Such documentation may include, but is not limited to, internal memoranda, minutes of meetings, training materials, notification letter from the IRS, prior examinations, and other similar things.
- (14) Since BSA penalties are assessed by FinCEN, which does not have any field examiners, the examiner must thoroughly document all facts on the issue of intent. After the examiner secures the necessary information and documents the apparent violations, the examiner should follow the procedures detailed in IRM 4.26.8, *Special Procedures*.

4.26.9.3.9 (06-01-2006) **Casino's Position**

- (1) After documenting the potential violations, the examiner should provide a list of the violations to the casino and solicit a written explanation for each of the violations identified. The list should include:
 - a. Gaming date of the transaction(s),
 - b. Customer name,
 - c. Account number (if any),
 - d. Amount of the currency transaction(s), and
 - e. Description of the transaction(s).
- (2) The examiner should advise the casino of any recordkeeping deficiencies as well as any deficiencies in their policies, procedures, internal controls, and compliance programs that might result in noncompliance with the BSA.
- (3) Any additional documents or information, provided by the casino in response, should be reviewed and a determination made as to whether any items should be removed from the list of violations.
- (4) When the casino contends that a CTR was filed and provides its retained copy as evidence, the examiner should query the FCQ system and conduct an exhaustive search before concluding that a CTR was not received. In conducting the search, the examiner should query all customer numerical identification on the CTR such as account number (if available), SSN, and identification credential number.

4.26.9.3.10 (06-01-2006) **Money Laundering Trends**

- (1) Examiners should be alert to situations where casinos or their customers may structure transactions in amounts of \$10,000 or less to circumvent the reporting requirements of the BSA, particularly if the casino does not have a system of aggregation in place.
- (2) Examples of how casino employees may structure transactions or advise customers how to avoid a CTR filing include the following:
 - a. Employees may fragment larger currency transactions into amounts of \$10,000 or less, when preparing source documentation.

- b. Employees may advise customers to limit their cash activity to amounts of \$10,000 or less per transaction.
 - c. Employees at the gaming tables may advise customers, who are buying chips with cash, that they are approaching the reporting threshold thereby suggesting or implying that they should move to another table. This action could be viewed as potentially assisting in structuring transactions.
- (3) Examples of how customers may structure transactions, with or without the knowledge of the casino, to avoid a CTR filing include the following:
- a. A customer may move from table to table limiting their cash buy-ins to amounts of less than \$10,000 per table.
 - b. A customer may conduct currency transactions at the casino cage in increments of \$10,000 or less. They may conduct the transactions at different windows or at different times of the day using different cashiers.
 - c. A customer may maintain more than one account with the casino, sometimes using an alias, and limit their currency transactions to \$10,000 or less per account.
 - d. A customer may fragment his or her transactions into amounts of \$10,000 or less when redeeming or exchanging chips for cash at the casino cage and may use others as agents to conduct the transactions.
 - e. A customer may find out what time of day the casino's business or gaming day is concluded and structure currency transactions around the cut-off time to avoid the filing of a CTR.
 - f. A customer could purchase a large amount of chips with currency (in amounts just below the reporting threshold) at a table, engage in minimal gaming and then go to the cage and redeem the chips for a casino check.
 - g. A customer could make a large deposit using numerous small denomination bills, engage in minimal gaming and then withdraw the funds in large denomination bills, a casino check or a wire transfer.
 - h. A customer could insert currency into a slot machine bill validator, accumulate credits with minimal or no gaming activity and then cash out the credits for large denomination bills or a casino check.
 - i. A customer may furnish an identification document that is false or altered (such as address changed, photograph substituted) in connection with the completion of a CTR, or the opening of a deposit, credit or check cashing account.
 - j. A customer may draw large casino markers to purchase chips, engage in minimal or no gaming activity, and then pay off the markers in currency and subsequently redeem the chips for a casino check.
- (4) When evidence of a money laundering scheme is uncovered, a referral should be made on Form 5104, *Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*. (Refer to IRM 4.26.8, *Special Procedures*)

4.26.9.3.10.1
(06-01-2006)

Examination Techniques

- (1) In addition to the examination techniques outlined in this section, the following techniques can be useful in uncovering money laundering schemes:
- a. When reviewing customer currency transactions, if an examiner identifies transactions at or near the reporting threshold, the examiner should review all other activity by that customer for that day (and prior and subsequent days) to determine if the customer was attempting to structure transactions and whether a CTR was required.

- (2) Examiners should be alert to customers who may be using the casino to facilitate structuring at other financial institutions. Examples include:
 - a. Depositing multiple bank checks of \$10,000 drawn on various banks or on consecutive days at the same bank.
 - b. Depositing or paying off markers with multiple instruments (for example, cashier's checks, money orders, traveler's checks, or foreign drafts) that appear to have been purchased in a structured manner or were issued by several different financial institutions, and none of the instruments is greater than \$3,000.
 - c. Issuing casino checks, each less than \$3,000, made out to third parties or checks without a specified payee.
 - d. Withdrawing a large amount of funds from a deposit account and requesting that multiple casino checks be issued each of which is less than \$3,000.
 - e. Redeeming chips or withdrawing large amounts from a deposit account and requesting multiple casino checks of \$10,000 or less.
- (3) When reviewing computerized player-rating records, the examiner should be alert for patterns in which a customer purchases large amounts of chips with currency, engages in minimal gaming and then leaves the table.

4.26.9.4

(06-01-2006)

Check Casher Overview

- (1) A check casher is any individual or financial institution that provides a check cashing service regardless of whether check cashing is the primary business.
- (2) Check cashers are used by individuals who may not have a bank account or want to cash checks without the delays and restrictions imposed by a conventional bank. Check cashers can cash checks immediately without waiting for funds to be collected as banks often require. The degree of risk involved is significant, and the check casher must take measures to reduce the risk in cashing checks.
- (3) In addition to cashing checks, check cashers may provide additional services such as:
 - a. Issuing or selling money orders, (IRM 4.26.9.7)
 - b. Processing motor vehicle and title registration forms,
 - c. Accepting utility bill payments,
 - d. Selling public transportation tokens,
 - e. Transmitting funds, (IRM 4.26.9.8)
 - f. Providing cash advances on credit cards,
 - g. Offering "Payday loans",
 - h. Selling lottery tickets,
 - i. Faxing services, and
 - j. Exchanging currency.
- (4) Businesses which may conduct check cashing services as a secondary part of their business operations include (list is not all inclusive):
 - a. Truck stops,
 - b. Bars, taverns, or liquor stores,
 - c. Wire services, and
 - d. Supermarkets and convenience stores.

- (5) The location of the check casher may be a key element in identifying the type of transactions conducted. Some examples are:
 - a. Check cashers located in economically depressed areas usually cash checks for state aid, Social Security, unemployment, disability and life insurance, federal and state tax refunds, and support payments for dependent children. Money orders sold, if applicable, are for basic living expenses, such as rent, car loans, insurance, and other similar items.
 - b. Check cashers located in business and financial districts usually cash checks for payroll, professional fees, businesses, escrow checks, legal fees, insurance settlements, wire transfer drafts, traveler's checks, and other money orders or cashier checks. Money orders sold, if applicable, in business and financial districts are frequently in larger denominations. They also sell money orders to "cash" businesses, which do not maintain a security service for transportation of currency. These businesses will purchase a money order to take to their bank instead of cash. Check cashers refer to this type of money order as a "safety check".
 - c. Check cashers, located in middle class areas, tend to be fewer and to have larger but fewer transactions. The money orders sold, if applicable, are more frequently sold in "blank", meaning the remitter is not identified. Many large transactions are conducted with well-known patrons.
- (6) Check cashers are one of the types of financial services providers known as Money Service Businesses (MSBs). Refer to IRM 4.26.5, *Bank Secrecy Act History and Law*, for a discussion on MSBs.

4.26.9.4.1
(06-01-2006)
Organization

- (1) Check cashing businesses can range from large sophisticated chains with interstate franchised facilities to small one owner store front operations.
- (2) The organization of a check casher can vary. There is no uniform management structure. However, check cashing chains and franchises are usually structured into several organizational levels to minimize the risks. Each level is authorized to approve certain size transactions. The number of levels may vary depending on the size of the check cashed and the number of branches. A typical structure has a minimum of three levels for approving large currency transactions.
 - a. Director/Manager — Oversees the daily operation of the check casher. Normally the manager approves the largest currency transactions and is responsible for maintaining the internal control and records of the operations.
 - b. Head Cashier/Teller Supervisor — Reviews all teller reconciliations. Usually the supervisor will approve medium size transactions (between \$3,000 and \$5,000) and often receives shipments of currency to and from the correspondent bank.
 - c. Teller — Responsible for conducting all transactions including reconciling the total currency transactions to the teller's beginning and ending cash balances. The teller usually will have the lowest authorization for conducting currency transactions. The teller is the front-line employee of the check cashing institution who must secure identification from individuals conducting currency transactions.
 - d. BSA Compliance Officer — Responsible for implementing and monitoring the operation and internal controls of the program. In a small business

with only a few employees, this person may execute all the tasks himself. In a large, multi-state business, this person may have responsibility for overseeing the system and program.

- (3) Many check cashers belong to the Financial Service Centers of America (FiSCA - web site address: *www.fisca.org*), and/or to state or local associations. FiSCA members receive a BSA compliance manual as part of their membership.

4.26.9.4.2
(11-12-2019)
Law

- (1) 31 CFR 1010.100(ff)(2), *Check casher*, A person that accepts checks (as defined in the Uniformed Commercial Code(UCC)), or monetary instruments (as defined at 31 CFR 1010.100(dd) , *Monetary instruments*), in return for currency or a combination of currency and other monetary instruments or other instruments, in an amount greater than \$1,000 for any person on any day in one or more transactions. Whether a person is a “check casher” as described in this section is a matter of facts and circumstances. The term “check casher” shall not include:
- a. A person that sells prepaid access in exchange for a check (as defined in the UCC), monetary instrument or another instrument,
 - b. A person that solely accepts monetary instruments as payment for goods or services other than check cashing services,
 - c. A person that engages in check cashing for the verified maker of the check who is a customer otherwise buying goods and services,
 - d. A person that redeems its own checks, or
 - e. A person that only holds a customer’s check as collateral for repayment by the customer of a loan.

4.26.9.4.2.1
(11-12-2019)
Reporting Requirements

- (1) A CTR, FinCEN Form 112, must be electronically filed for all single currency transactions of more than \$10,000 in one business day. (31 CFR 1010.311, *Filing obligations for reports of transaction in currency*)
- a. Multiple currency transactions must be aggregated, and a CTR is required, if the business has knowledge that the multiple transactions are by or on behalf of any person and result in either cash in or cash out totaling more than \$10,000 in one business day. (31 CFR 1010.311(b), *Multiple transactions*)
 - b. The CTR must be filed within 15 calendar days following the day the reportable transaction occurs. (31 CFR 1010.306(a)(1), *Filing of reports*)
- (2) Although Check Cashers are not required to file FinCEN Report 111- *Suspicious Activity Report (SAR)*, they may elect to voluntarily file a SAR if they suspect or have reason to suspect suspicious activities have occurred. (31 CFR 1022.320, *Reports by money services business of suspicious transactions*)
- a. Check Cashers are subject to the suspicious activity rules to the extent they offer money transmission, money orders, or traveler’s check products, which are subject to SAR reporting.
 - b. MSBs generally are required to file SARs to report suspicious transactions of at least \$2,000 in funds or other assets conducted or attempted by, at or through an MSB. (31 CFR 1022.320)

- c. A check casher is prohibited from notifying any person involved in the suspicious transaction that a SAR has been filed. (31 CFR 1022.320(d), *Confidentiality of SARs*)

- (3) The financial institution may be required to file additional reports. Refer to IRM 4.26.5, *Bank Secrecy Act, Bank Secrecy Act History and Law*, for BSA reporting requirements.
- (4) FinCEN requires that most FinCEN reports be filed electronically through its E-file system.

4.26.9.4.2.2
(06-01-2006)
**Registration
Requirements**

- (1) A check casher is required to electronically register on FinCEN Form 107, *Registration of Money Services Business*, and biannually renew their registration if they are not acting in an agent capacity and are not a branch location. (31 CFR 1022.380, *Registration of money services businesses*)
- (2) Certain events require re-registration which is different from a renewal registration. (31 CFR 1022.380(b)(4), *Events requiring re-registration*)

4.26.9.4.2.3
(06-01-2006)
**Recordkeeping
Requirements**

- (1) For records required of all financial institutions, refer to IRM 4.26.5, *Bank Secrecy Act History and Law*.
- (2) Copies of all filed CTRs must be retained by the financial institution for five years from the date of the report. (31 CFR 1010.306(a)(2), *Filing of reports*)
- (3) Copies of all filed SARs and the original or record of any supporting documentation shall be maintained for five years from the date of filing the SAR. (31 CFR 1022.320(c), *Retention of records*)
- (4) All records created from the AML Program Requirements must be retained for five years.
- (5) Check cashers are not required to maintain any additional records under BSA regulations. They may be required to maintain additional records if providing other money services, in addition to check cashing, regulated by the BSA.
- (6) Copy of RMSB registration and renewals, if applicable, must be retained for five years. (31 CFR 1010.430(d), *Nature of records and retention period*)
- (7) Current annual agent list and agent list(s) for the past five years must be maintained, if applicable. (31 CFR 1022.380(d), *Nature of records and retention period*)

4.26.9.4.2.4
(11-12-2019)
**AML Program
Requirements**

- (1) All money services businesses must establish and implement a written, risk-based AML Program reasonably designed to prevent the business from being used to facilitate money laundering and the financing of terrorism. (31 CFR 1022.210, *Anti-money laundering programs for money services businesses*)
- (2) Refer to IRM 4.26.5.8, *Anti-Money Laundering (AML) Compliance Program*, for information on AML Compliance Program requirements for MSBs.
- (3) IRM 4.26.6.5.1.2, *Evaluation of AML program*, contains information on evaluating the AML program.

4.26.9.4.3
(11-12-2019)
Records Commonly Found

- (1) Since there are no required records for check cashers under the BSA you may find that there are few records available to examine.
- (2) A check casher's records, when the check casher is a chain or franchise include:
 - a. Daily Cash Reconciliation: a record summarizing the total currency transactions during the day which reconciles to the beginning and ending cash on hand,
 - b. Teller Reconciliation: a record detailing teller transactions, for both currency and monetary transactions. It reconciles beginning and ending cash on hand and is used to prepare the daily cash reconciliation,
 - c. Daily Bank Reconciliation: reconciles the daily cash transactions to various bank account balances,
 - d. Income Statement: a record of fees received from money order sales, wire transfers, and checks cashed,
 - e. Canceled money orders or cashier's check,
 - f. Bank Statements,
 - g. Signature Cards,
 - h. Transaction Account detailing an individual's record of checks cashed, and
 - i. Copies of checks cashed.
- (3) Records may be stored electronically.
- (4) If the records are maintained off site, the check casher must make the records accessible within a reasonable period, taking into consideration the nature of the records, and the amount of time expired since each record was made.
- (5) Use of a CAS should be considered if records are voluminous.

4.26.9.4.4
(11-12-2019)
Interview

- (1) IRM 4.26.6.5.3.3, *Interview*, contains additional information on interviews.
- (2) The BSA examination should include several interviews. Each interview should be documented in the case file. Owners/operators, shareholders, directors, managers, tellers, and employees responsible for preparing currency reports, and securing and maintaining records pertaining to the reporting requirements under the BSA should be questioned as to their knowledge and training of the BSA recordkeeping and reporting requirements. Knowledge is one of the elements needed to prove intent for any apparent violation of the regulations.
- (3) Tellers handling currency transactions should be interviewed. The examiner should ascertain:
 - a. The types of records maintained by the tellers,
 - b. The tellers' knowledge of currency transaction reporting requirements,
 - c. Their limit for cashing checks without approval and the procedures for cashing large checks,
 - d. The procedures and records maintained for large money orders or cashier's checks sold, and
 - e. Their procedures for preparing CTRs.

- (4) Responsible officers and supervisory personnel who approve large currency transactions and/or are responsible for filing CTRs should be interviewed. Examples may include the head cashier, the manager, the compliance officer, or the owner/operator.
- (5) The examiner should document the responsibilities and duties of the officers and secure the officers' identifying information.
- (6) During the interview of selected employees, the examiner should determine if the check casher maintains an internal compliance program and whether the program is written. If it is written, a copy of the procedures should be secured. The individual responsible for the internal compliance program must be interviewed.
- (7) The interview should document enough information to describe the operations of the check casher including:
 - a. Internal Control
 - b. Internal Audits
 - c. Chart of Accounts
 - d. Currency Controls
 - e. On-Site Records
 - f. Offsite Records on medium other than hard copy
 - g. Training
- (8) The interview should identify any related institutions, branches, entities, or lists of other related check cashing facilities. The BSA examiner should follow the new entity procedures found in IRM 4.26.6.3, *Identification*.
- (9) Ask specific questions relating to the business, area and services offered. The examiner must consider all financial services or products offered by the business, such as money remittance, check cashing and sales of money orders.
- (10) Ask the owners or management of the financial institution if they have knowledge of structuring, or if any suspicious transactions have occurred. This question must also be asked while interviewing employees who have customer contact.
- (11) Ask open-ended questions throughout the interview. Do not ask questions that require only a "yes" or "no" answer.
- (12) Additional information may be found on the BSA Policy SharePoint.

4.26.9.4.5
(11-12-2019)

Review of the Records

- (1) Any records the check casher maintains for his own business that are relevant to the BSA examination can be requested and reviewed. The BSA examiner will determine whether the check casher maintains adequate records to ascertain if multiple transactions or structuring are taking place. Major record-keeping inadequacies must be documented in a Letter 1112, *Title 31 Violation Notification Letter*, or Form 5104, *Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*.
- (2) BSA examiners should review the records to familiarize themselves with the check casher's business transactions. The examiner will determine the scope of the records review based on the initial interview. When determining the scope of the examination, the examiner should consider that check cashers

who are part of a chain or franchise have internal controls for the handling, recording, and summarizing of cash transactions.

- (3) The examiner should consider the following steps when reviewing the check casher's records:
 - a. Become familiar with the components of the summary records including both the daily cash reconciliation and teller reconciliations.
 - b. Trace the teller reconciliation totals to the teller summary.
 - c. Trace the teller summary totals to the daily cash reconciliation.
 - d. Trace the daily cash reconciliation totals to the vault reconciliation, bank reconciliation, and bank statements.
 - e. Trace deposit slips to the teller summary totals and the correspondent bank records. Determine if the total amount of checks deposited agree with amount of checks cashed. The check casher's transactions for "cash in" and "cash out" are frequently netted against each other before being deposited into the correspondent bank. Therefore, the items of deposit often reflect the netted transactions for the day. Monetary instruments are deposited, and currency is returned to the check casher's vault.
 - f. The above records should allow the examiner to determine specific dates when money orders were sold (if applicable) or checks were cashed that require a CTR.
 - g. Verify that summary documents accurately record information from source documents for the selected period.
 - h. Inspect filed copies of CTRs for accuracy and completeness of information and verify they were timely filed. A copy of each CTR filed must be retained by the financial institution for a period of five years from the date of the report.
 - i. Determine if all the required information for purchases of money orders involving currency in amounts of \$3,000 to \$10,000, inclusive, is maintained, if applicable.
 - j. Test check signature cards.
- (4) Analyze the bank reconciliations, the cash on hand records, and the teller reconciliations to identify large transactions. The examiner should look for decreases in the amount of ending cash on hand or amounts withdrawn from the correspondent bank. Large decreases or withdrawals of cash could indicate large checks were cashed. The examiner should note the dates when amounts could exceed \$10,000 or transactions appear to be structured to avoid the \$10,000 threshold.
- (5) Review the check register or the copies of cashed checks for transactions over \$10,000 that may indicate money laundering and/or structuring. The examiner may elect to select a dollar cutoff for inspecting cashed checks. Because of the dollar amounts involved, most of the checks cashed by a typical check casher may not be relevant to the BSA examination. These generally include social security checks, welfare checks, payroll checks, and other similar financial instruments.
- (6) If a determination is made that records are inadequate, destroyed, or not maintained, the examiner should:
 - a. Expand the scope of the BSA examination,
 - b. Document all problem areas and findings in the workpapers, and

- c. Consider issuing a summons to a third-party recordkeeper for missing or incomplete information. If the third-party recordkeeper is a bank, sample periods should be selected carefully based on existing records. Refer to IRM 4.26.8, *Special Procedures*, for summons procedures.
 - (7) If the examiner determines a CTR should have been filed or the required recordkeeping or reporting requirements are not met, the transaction should be traced to the internal compliance program. The examiner should:
 - a. Determine the reason the internal procedures failed, and
 - b. Verify that adequate identification was required by the check casher by inspecting the appropriate signature card or similar record.
 - (8) Review any SARs filed by the NBF.
 - (9) Review relevant audit reports or reviews that address BSA policies, procedures, or operations for BSA relevant issues.
 - (10) Review filed registrations (if applicable) for accuracy and completeness.
 - (11) Determine whether the check casher is required to register.
-
- (1) The examiner must obtain supporting documentation for each type of violation:
 - a. Reporting – The date of the transaction, the amount, the individuals involved and a detailed statement regarding the violation, including copies of source documents such as cash in/out slips, control registers, and teller cash proofs which support the violation.
 - b. Recordkeeping – The details of the specific records which were not maintained or were inadequate, including management’s response to the violations.
 - (2) The financial institution’s knowledge of the BSA requirements must be determined during the examination.
 - a. The key officers and employees should be interviewed to document the check casher’s response to any apparent violations.
 - b. The existence of an internal compliance program may indicate knowledge. For example, if knowledge of the reporting and recordkeeping requirements is limited to upper management and the tellers are not similarly educated, the check casher may be at least negligent (for not properly instructing the tellers). The tellers need to know what their BSA obligations are. The tellers are the initial contact point where the information is obtained.
 - (3) Other factors indicating the money services business’ knowledge of the BSA registration, reporting, recordkeeping, and compliance program requirements are:
 - a. Prior BSA violations and BSA compliance related contacts with the IRS.
 - b. Training programs offered by the money services business.
 - c. The MSBs formal BSA compliance procedures.
 - d. Active involvement of management in oversight and internal control activities.
 - (4) In situations where knowledge cannot be established within the scope of selected records, the examiner should expand the period to include recent

4.26.9.4.6
(11-12-2019)
**Supporting
Documentation**

transactions that occurred after knowledge can be clearly documented. For example, the examiner selected records for January, February, and March. The inspection of these records disclosed currency transactions that appear to be structured and which should have been reported. The check casher denied knowledge of the structuring regulations during the initial interview. In April, the examiner informed the check casher about the suspicious transactions and of the structuring regulations. The examiner later expanded the examination period to include May and June transactions. The examiner found violations in May and June. The check casher's knowledge was documented during the notification of the structuring violations and took no action to prevent the recurrence of violations. The check casher's intent not to comply should be documented.

- (5) Because willfulness is a state of mind, generally only circumstantial evidence of willfulness will be available. A willful violation is the intentional violation of a known legal duty.
- (6) IRS does not have the authority to assess penalties under the BSA except for FBAR violations. Significant BSA violations or deficiencies are therefore referred to FinCEN unless a fraud referral is appropriate. The examiner and manager will decide whether to refer the case to FinCEN for consideration of civil money penalties. The examiner must thoroughly document all facts on the issue of intent. See IRM 4.26.8 if the case is to be referred to FinCEN.

4.26.9.4.7 (11-12-2019)

Closing the Examination

- (1) Refer to IRM 4.26.6.5.3.10, *Notification of Findings*, for information on notifying the business of examination results.
 - a. If no BSA violations or significant AML program issues have been found, prepare Letter 4029, *Bank Secrecy Act No Change Letter*.
 - b. If BSA violations are found which are technical, minor, infrequent, isolated, or not substantive, a Letter 1112, *Title 31 Violation Notification Letter*, should be issued. (IRM 4.26.8)
 - c. If apparent BSA violations are found which appear to meet the referral criteria, prepare a referral on Form 5104, *Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*. (IRM 4.26.8.6, *Form 5104, Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*)
 - d. If the apparent BSA violations appear to meet criminal referral guidelines, the BSA manager will contact the Fraud Technical Advisor to determine if a Form 2797, *Referral Report of Potential Criminal Fraud Cases*, is warranted. (IRM 4.26.8.6, *Coordination with a Fraud Technical Advisor*)
- (2) A closing conference must be held at the close of the examination. See IRM 4.26.6.5.3.11, *Holding the Closing Conference*, for additional information.
- (3) When a Letter 1112 is issued, the financial institution is asked to provide a response, amend the AML program, and implement recommendations. Refer to IRM 4.26.6.5.3.12, *Letter 1112 Response*, for additional guidance.
 - a. See IRM 4.26.6.5.3.13, *Delinquent BSA Forms Procedures*, for the process to secure delinquent returns discovered during the examination.
 - b. See IRM 4.26.6.5.3.14, *Case File Closing Procedures*, for procedures when closing the case file.

- c. See IRM 4.26.6.5.3.16, *Examination Information Report, Form 5346*, for information on preparing and submitting Form 5346, *Examination Information Report*.
- d. IRM 4.26.6.5.3.17, *Information Items*, provides information on submitting other information items.
- e. IRM 4.26.6.5.3.18, *Examiner-Filed SARs*, provides procedures for submitting examiner filed SARs.

4.26.9.4.8
(06-01-2006)
**Money Laundering
Trends**

- (1) The financial institution and/or the customer can be involved in potential money laundering schemes. The examiner must focus on both the financial institution and the transactor(s) during the BSA compliance examination.
- (2) Money laundering techniques which could be used by the financial institution include:
 - a. Failing to maintain complete records,
 - b. Failing to record specific transactions,
 - c. Failing to obtain the required information to comply with the recordkeeping requirements,
 - d. Failing to file CTRs on reportable transactions,
 - e. Filing incomplete CTRs or SARs,
 - f. Structuring a transaction by breaking one transaction into several to circumvent the reporting requirements,
 - g. Issuing money orders, drafts or IOU's to keep transactions under the \$10,000 reporting requirement, or
 - h. Receiving currency from an outside source in exchange for checks received from the check casher's customers.
- (3) Money laundering techniques which could be used by the customer/transactor include:
 - a. Using multiple locations to conduct transactions,
 - b. Using several individuals at one or more locations to conduct a transaction,
 - c. Using aliases when conducting transactions,
 - d. Conducting numerous transactions at the same location at different times for one day,
 - e. Requesting money orders, drafts or IOU's when cashing checks to circumvent a reporting requirement, or
 - f. Check cashing conducted by the same customer in which the payee name varies.
- (4) When evidence of a money laundering scheme is uncovered, a referral should be made on Form 5104, *Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*. Refer to IRM 4.26.8 for referral procedures.

4.26.9.4.8.1
(06-01-2006)
Examination Techniques

- (1) The following techniques can be useful in uncovering money laundering schemes:
 - a. Review all bank statements to ensure the check casher is withdrawing sufficient currency to meet the requirements of any checks cashed. If not sufficient, then sources of cash should be investigated in greater depth.

- b. Review records for any indications of false recordkeeping entries, for example IOU's, backdating or postdating transactions, or multiple transactions during one day in which the books and records indicate different posting days.
- c. Determine if the business has paid out funds for cashed checks more than what it has withdrawn from its bank. This might indicate that the business is laundering funds for someone else by exchanging their cash for checks. Compare the cash withdrawn for a period to the amount of checks deposited. The amounts should be close in value unless the business has significant sales of other products or services. Also, compare fees earned from cashing checks for a period to the fees that should have been earned from the amount of checks deposited.
- d. Review all financial services offered to see if the financial institution and/or customers are structuring transactions by using a variety of financial services.

4.26.9.5
(06-01-2006)
Credit Unions Overview

- (1) Credit unions are financial cooperatives which are owned by their respective members. The members must share a common characteristic such as belonging to the same organization, work for a common employer, or live within a specific geographic area.
- (2) The primary function of a credit union is to provide savings accounts and make low interest loans to its members. Larger credit unions provide other financial services for their members including:
 - a. Share draft/demand deposit accounts
 - b. Share certificate/money market accounts
 - c. Check cashing services
 - d. Sales of traveler's checks
 - e. Sales of money orders
 - f. Sales of cashier's checks or credit union drafts
 - g. Wire transfer services
 - h. Credit card services
- (3) The members' transactions with the credit union include share deposits, share drafts and share loans.
- (4) Most credit unions are not members of the Federal Reserve System. Therefore, they require commercial bank accounts to conduct transactions within the Federal Reserve System such as clearing share drafts written on member accounts and currency withdrawals and deposits.
- (5) Credit unions operate under a charter issued by either the Federal Government or the State where they are located. The National Credit Union Shares Insurance Fund, which is administered by the National Credit Union Association (NCUA), provides federal share insurance for all the nations' federally chartered and most state-chartered credit unions. Federal insurance can be obtained by those institutions that are state-chartered. Several states require state-chartered credit unions to maintain federal share insurance.
- (6) The NCUA, an independent federal agency, is responsible for the examination and supervision of federally chartered credit unions.
- (7) There are three types of credit unions:

- a. Federally Chartered, Federally Insured - The NCUA is the primary regulator for these financial institutions and examines these annually for safety and soundness.
 - b. State Chartered, Federally Insured - The NCUA has jurisdiction over these financial institutions, but a state regulator agency is typically the primary regulator.
 - c. State Chartered, Non-Federally Insured - The NCUA has no jurisdiction over these financial institutions and state agencies are the primary regulators.
- (8) There are gaps in the responsibility for examining credit unions for BSA compliance. The NCUA has no authority over state chartered, non-federally insured credit unions and only partial responsibility for state chartered, federally insured credit unions. IRS examination has the responsibility for conducting BSA examinations of state chartered, non-federally insured credit unions.
 - (9) The Federal Credit Union Act, promulgated by Congress on June 26, 1934, requires the NCUA to adopt regulations requiring federally insured credit unions to establish and maintain procedures designed to assure and monitor compliance with the requirements of Subchapter II of Chapter 53 of Title 31, United States Code (the BSA reporting and recordkeeping requirements).
 - (10) Every state except Delaware, South Dakota, and Wyoming, has enabling legislation, which allow states to charter credit unions.
 - (11) The NCUA examines federally chartered and federally insured credit unions for compliance with the BSA reporting and recordkeeping requirements.
 - (12) The Credit Union National Association is a national trade association for credit unions and provides various services to member institutions.

4.26.9.5.1
(11-12-2019)
Terminology

- (1) Cash Control System - A centralized recordkeeping and control system to monitor cash transfers within the credit union and cash sent to and received from correspondent banks.
- (2) Cash Received Voucher/Cash Payment Voucher - Individual receipts for transactions conducted with members that reflect activities conducted with both currency and negotiable instruments, such as checks.
- (3) Cash In/Out Slips - Individual documents prepared by the teller to reflect currency taken in and paid out.
- (4) Exempt Customer - A credit union member who meets the requirements of 31 CFR 1010.315, *Exemptions for non-bank financial institutions*, to be excluded from the Currency Transaction Report reporting requirement.
- (5) Share - Ownership interest in a credit union. A typical par value is \$5.
- (6) Share Draft Account - This is like a checking account with a bank. The member may write drafts (checks) to 3rd parties.
- (7) Share Savings Account - The member's savings account with the credit union. The interest earned on the savings account is called a dividend.

4.26.9.5.2
(11-12-2019)
Organization

- (1) The operating parameters and limitations of a credit union are defined by its charter and bylaws. Strategic planning and direction of operations is performed by a Board of Directors and various committees. The Board and committee members are directly elected by the shareholders/members of the credit union.
- (2) A supervisory committee oversees operations. The committee usually reviews books and records at least every six months and makes a complete verification of records at least every two years. The committee's task may include testing of internal control procedures for BSA compliance.
- (3) Since the members directly elect the Board and oversight committees, failures associated with privately owned institutions may not occur. However, the examiner should be alert to failures on the part of the officers and employees.
- (4) Operations Personnel:
 - a. BSA Compliance Officer - Is designated by the Board to implement BSA control procedures. The compliance officer performs oversight review of the books and records to ensure compliance with the BSA. BSA training for personnel, if any, is normally conducted by this function.
 - b. Manager/Branch Manager - Oversees the day to day operations of the credit union and is responsible for BSA compliance.
 - c. Cash Control/Head Teller - Monitors currency in and out of the cash control system and currency transfers between tellers. This individual monitors all currency received and shipped by the credit union. This teller's approval is usually required on all large dollar transactions conducted with members. Credit unions may require that all large dollar transactions be conducted by this teller.
 - d. Teller - Conducts transactions with and provides services to members. Tellers are usually responsible for initiating the BSA reporting and record-keeping requirements such as verifying the customer's identification and soliciting required information.

4.26.9.5.3
(11-12-2019)
Law

- (1) Credit unions are defined as banks or depository institutions per 31 CFR 1010.100(d)(6), *A credit union*.
- (2) Credit unions may exempt, from the CTR reporting requirements, certain transactions between themselves and customers which meet the qualifications of an exempt person as defined in 31 CFR 1020.315(b), *Exempt person*.
- (3) Federally insured credit unions (federally chartered and state chartered) are required to implement and maintain an anti-money laundering program. (31 CFR 31 CFR 1020.210, *Anti-money laundering program requirements for financial institutions regulated only by a Federal functional regulator, including banks, savings associations, and credit unions*, and 12 CFR 748.2, *Procedures for monitoring Bank Secrecy Act (BSA) compliance*)
- (4) Although 31 CFR 1020.220(a)(1) requires credit unions, including non-federally insured credit unions, to implement written Customer Identification Programs, non-federally insured credit unions have been temporarily exempted from the requirement to establish anti-money laundering programs. (31 CFR 1010.205(b)(2), *Temporary exemption for certain financial institutions*)

- (5) All credit unions (federally chartered or state chartered and federally insured or privately insured) are required to implement a written Customer Identification Program. (31 CFR 1020.220, *Customer identification programs for banks, savings associations, credit unions, and certain non-Federally regulated banks*)

4.26.9.5.3.1
(11-12-2019)
Reporting Requirements

- (1) FinCEN Form 112, *Currency Transaction Report*, must be filed for all currency transactions of more than \$10,000 in one business day. (31 CFR 1010.311, *Filing obligation for reports of transaction in currency*)
- (2) Multiple currency transactions must be aggregated, and a CTR is required, if the business has knowledge that the multiple transactions are by or on behalf of any one person and result in either cash in or cash out totaling more than \$10,000 in one business day. Deposits made at night or over a weekend or holiday shall be treated as if received on the next business day following the deposit. (31 CFR 1010.313, *Aggregation*)
- (3) The CTR must be electronically filed within 15 calendar days following the day the reportable transaction occurs. (31 CFR 1010.306(a)(1), *Filing of reports*)
- (4) FinCEN Form 105, *Currency and Other Monetary Instruments Report*, (CMIR) must be filed by any person who transports, mails or ships or has someone else transport, mail or ship currency or monetary instruments in excess of \$10,000 into or out of the country or who receives such items into the United States from abroad. (31 CFR 1010.340, *Reports of transportation of currency or monetary instruments*)
- (5) A CMIR must be filed with the U.S. Customs Service at the time of entry into the United States or at the time of departure, mailing or shipping from the United States. (31 CFR 1010.306(b)(1), *Filing of reports*)
- (6) Any person receiving more than \$10,000 in currency or monetary instruments from outside the United States is required to file a CMIR within 15 days. (31 CFR 1010.306(b)(2))
- (7) FinCEN Form 114, *Report of Foreign Bank and Financial Accounts*, must be filed for any financial interest in or signature or other authority over a bank, securities, or other financial account which exceeds \$10,000 at any time during the calendar year. (31 CFR 1010.350, *Reports of foreign financial accounts*)
- (8) The FBAR must be electronically filed by April 15th of the succeeding year for foreign financial accounts maintained during calendar years 2016 and later. The annual due date for filing FBARs required for foreign financial accounts maintained during calendar years 2015 and earlier is June 30 of the following year. FinCEN will grant filers failing to meet the FBAR annual due date of April 15 an automatic extension to October 15 each year. When the April or October due date falls on a Saturday, Sunday, or legal holiday, the due date is delayed until the next business day.
- (9) FinCEN Form 111, *Suspicious Activity Report*, (SAR) is required to be made by banks or other depository institutions if they suspect or have reason to suspect suspicious activities have occurred. (31 CFR 1020.320, *Reports by banks of suspicious transactions*)
- (10) This report applies to suspicious transactions of at least \$5,000 in funds or other assets conducted or attempted by, at or through banks or other depository institutions. (31 CFR 1020.320(a)(2))

- (11) Generally, a bank is required to electronically file the SAR with FinCEN, no later than 30 calendar days after the date of detection, or 60 calendar days after the date of detection but, if no suspect was identified on the date of detection, the bank may delay filing the SAR for an additional 30 calendar days to identify the suspect. (31 CFR 1020.320(b)(3), *When to file*)
- (12) A bank or other financial institution is prohibited from notifying any person involved in the transaction that the transaction has been reported. (31 CFR 1020.320(e), *Confidentiality of SARs*)
- (13) FinCEN Form 110, *Designation of Exempt Person*, must be filed on each person being designated as exempt by the close of the 30-day period beginning after the day of the first reportable transaction in currency with that person sought to be exempted. (31 CFR 1020.315(c), *Designation of certain exempt persons*)

4.26.9.5.3.2 (11-12-2019) **Recordkeeping Requirements**

- (1) For records required of all financial institutions, refer to IRM 4.26.5, *Bank Secrecy Act History and Law*.
- (2) Copies of all filed CTRs must be retained by the financial institution for five years from the date of the report. (31 CFR 1020.306(a)(2), *Filing of reports*)
- (3) Copies of all filed SARs and the original or record of any supporting documentation shall be maintained by the financial institution for five years from the date of filing the SAR. (31 CFR 1020.320(d), *Retention of records*)
- (4) Additional records must be made and retained by credit unions. (31 CFR 1020.410, *Records to be made and retained by banks*)
- (5) Records are required to be maintained for exempt customers, including FinCEN Form 110, *Designation of Exempt Person*. (31 CFR 1020.315(e), *Operating rules*)
- (6) Records are required to be maintained for the issuance or sale of credit union checks, cashier's checks, money orders or traveler's checks which involve currency in amounts of \$3,000 to \$10,000, inclusive. (31 CFR 1010.415(a), *Purchase of bank checks and drafts, cashier's checks, money orders and traveler's checks*)
- (7) Records are required to be maintained for funds transfers (wires) of \$3,000 or more. (31 CFR 1010.410(a))
- (8) Records are required to be maintained by persons having a financial interest in or signature or other authority in foreign financial accounts. (31 CFR 1010.420, *Records to be made and retained by persons having financial interests in foreign financial accounts*)
- (9) Records must be retained by the financial institution for five years. (31 CFR 1010.430(d), *Nature of records and retention period*)

4.26.9.5.3.3
(06-01-2006)
**AML Program
Requirements**

- (1) All federally insured credit unions must establish and implement a written, risk-based AML Program reasonably designed to prevent the business from being used to facilitate money laundering and the financing of terrorism. Non-federally insured credit unions have been temporarily exempted from the requirement to establish anti-money laundering programs. (31 CFR 1010.205(b)(2), *Temporary exemption for certain financial institutions*)

4.26.9.5.4
(06-01-2006)
**Records Commonly
Found**

- (1) Credit unions vary significantly in size and the types of services offered. Therefore, the nature of the credit union's books and records vary.
- (2) Smaller institutions, whose services are limited to share deposit and share loan accounts may not conduct any currency transactions. These institutions often have very simple handwritten transaction records and manual bookkeeping systems.
- (3) Larger institutions may have several branches and offer extensive financial services. These institutions usually have on line data processing systems, detailed currency control policies, and sophisticated internal control procedures.
- (4) In addition to the required records listed in IRM 4.26.9.5.3.2, records commonly found at credit unions include:
 - a. Daily teller drawer and vault reconciliations,
 - b. Customer deposit, withdrawal and payment vouchers,
 - c. Summary reports of outstanding loans, certificates of deposit,
 - d. Cashier's check, money order, traveler's check and other negotiable instrument logs, and
 - e. Credit union bank statements, deposit slips and canceled checks.
- (5) Additional records may include:
 - a. A journal and cash record/daily transactions report which is a permanent record of daily transactions. All member transactions conducted during the day are individually posted to this journal. It may be summarized daily, depending on the accounting system.
 - b. A large currency transaction report or suspicious transaction report which lists all cash transactions over a management defined dollar limit. Supervisory personnel review this report to ensure all required Currency Transaction Reports are prepared each day.

4.26.9.5.4.1
(06-01-2006)
Cash Control System

- (1) Operating cash is ordered and received from a correspondent bank. Source documents which support this transaction include credit union checks made to cash, bank account debit memos, and currency order sheets.
- (2) When the cash is received, the cash control teller makes an entry in the credit union's cash control system. The appropriate debit and credit is recorded in the cash in bank and cash on hand account.
- (3) Cash is then disbursed to each teller for conducting daily transactions. An entry is made in the cash control system to record the amount of cash issued.
- (4) Each teller maintains an individual teller cash control sheet to record daily transactions. The teller cash control sheet details the amount of cash received by denomination. The teller also records additional internal cash transfers that occur during the day.

- (5) Tellers conduct cash in transactions for share deposits, sales of money orders, traveler's checks and cashier's checks and loan payments. All deposits and sales are not conducted with cash. Members may deposit checks into share accounts and may use share drafts or share savings withdrawals to purchase negotiable instruments.
- (6) Tellers conduct cash out transactions for share withdrawals and check cashing. Share withdrawals may be paid by cash or a credit union share draft.
- (7) When cash is used during a teller transaction, a document for cash in/out should be prepared. This could include a cash in slip or computer coding for cash transactions on a cash received/payment voucher.
- (8) At the end of the day, tellers reconcile their cash control sheets to their ending cash balance and source records. The control sheet, source records and currency are turned into the cash control teller.
- (9) The cash control teller then enters all ending currency balances into the cash control system log. The ending cash on hand is then reconciled to the daily activities. A cash control system reconciliation proof/report is prepared to account for the financial institution's total cash on hand.
- (10) If cash on hand exceeds the operating requirements of the credit union, the excess funds are deposited into the bank. If the currency amount is less than the required amount, a currency request is prepared and sent to the bank. At this point, the daily currency cycle has ended.

4.26.9.5.5 (11-12-2019) **Interview**

- (1) An interview should be conducted at the credit union's main location, with a credit union officer, Bank Secrecy Act (BSA) compliance officer and/or other key personnel who have knowledge of the credit union's operations, policies and internal control procedures. Determine who is responsible for compliance with the BSA recordkeeping and reporting requirements.
- (2) Document the credit union's background history, the number of branches operated and affiliated organizations.
- (3) Identify the BSA compliance officer and all other personnel who are responsible for conducting, recording and reporting of BSA transactions and evaluate their understanding of the BSA recordkeeping and reporting requirements. It is important to determine the extent of the interviewee's knowledge of the BSA requirements should any violations be noted during the examination. These individuals should be identified by name, title and specific responsibilities.
- (4) Tellers handling currency transactions should be interviewed. The examiner should ascertain:
 - a. The types of records maintained by the tellers,
 - b. Their knowledge of currency transaction reporting requirements,
 - c. Their dollar limit for cashing checks without approval and the procedures for cashing large checks, and
 - d. Their procedures for preparing Currency Transaction Reports (CTRs).
- (5) Responsible officers and supervisory personnel, who approve large currency transactions and/or are responsible for filing CTRs, should be interviewed.

These individuals may include the BSA compliance officer, manager and/or head teller. The examiner should ascertain:

- a. The procedures for recording currency transactions and the filing of CTRs, CMIRs, FBARs and SARs, and
- b. Their knowledge of structuring or if any suspicious transactions have occurred.

Note: This question also must be asked while interviewing employees who have customer contact.

- (6) Each interview should be documented in the case file.
- (7) Ask specific questions to determine the financial services offered by the credit union. The examiner must consider all financial services or products offered by the credit union such as money remittance, check cashing, and sales of money orders and/or traveler's checks.
- (8) Ask open-ended questions throughout the interview. Do not ask questions that require only a yes or no answer.

4.26.9.5.6 (11-12-2019)

Review of the Records

- (1) Any records the credit union maintains that are relevant to the BSA examination can be requested and reviewed. The examiner will determine if the credit union is maintaining adequate records and must document any recordkeeping violations.
- (2) Ask to see the credit union's policy and procedures manual regarding the BSA identification, recordkeeping, reporting and exemption requirements. The examiner should determine if the institution's BSA information is correct and its procedures are adequate.
- (3) Review in house training programs and inspect retained training records. The examiner should inspect records of external training such as certificates of course completion. Most individual state credit union leagues and trade associations offer BSA training courses for all levels of personnel and provide documentation of attendance.
- (4) Identify dates during which large currency transactions occurred. The examiner should review currency received from or shipped to the correspondent bank using:
 - a. Bank statements and reconciliations, deposit tickets and source documents for currency withdrawals such as debit memoranda,
 - b. Cash on hand ledger account or other summary currency reports, and
 - c. Cash control system records which reflect daily cash reconciliations, change fund ledger account, bank statements or other activity summary records to determine dates during which large transactions may have occurred.
- (5) Review relevant audit reports or reviews that address BSA policies, procedures or operations for BSA-relevant issues.
- (6) Inspect the tellers' cash control proofs and supporting cash in/out documents to identify specific large currency transactions. Based on the information

obtained from the preplan, interviews, and review of written records, select a sample of transactions consisting of amounts ranging from a minimum of \$3,000 to greater than \$10,000.

- (7) Trace the sampled transactions through the internal control system to CTR filings for amounts greater than \$10,000. If there is a transaction over \$10,000 and no CTR was filed, check to see if the customer has been designated as an exempt person before determining if an apparent reporting violation has occurred.
- (8) Review the credit union's retained copies of CTRs for accuracy and completeness.
- (9) Compare the credit union's retained copies of CTRs to the FinCEN Query (FCQ) record to insure they have been filed.
- (10) Review FinCEN Form 114, *Report of Foreign Bank and Financial Accounts*, if the credit union maintains foreign bank accounts or has signature authority or financial interests in foreign countries.
- (11) Review FinCEN Form 105 (CMIR) if the credit union is involved with the transportation of currency into or out of the U.S.
- (12) Review the credit union's records maintained for the sale of bank checks or drafts, cashier's checks, money orders, and/or traveler's checks for amounts involving currency in amounts of \$3,000 to \$10,000, inclusive. Ensure all required information has been obtained pursuant to the recordkeeping requirements of 31 CFR 1010.415(a), *Purchases of bank checks and drafts, cashier's checks, money orders and traveler's checks*.
- (13) Review the credit union's records to determine if all the required information on money transmittals (such as wire transfers) of \$3,000 or more has been obtained and retained pursuant to the recordkeeping requirements of 31 CFR 1010.410(a), *Records to be made and retained by financial institutions*.
- (14) Evaluate the credit union's recordkeeping procedures relating to customer account activities and certificates of deposits pursuant to the recordkeeping requirements of 31 CFR 1020.410.
- (15) Review the SAR filings to determine if there are recurring patterns of activity by the same or related members of the credit union. If patterns are noted, question the appropriate personnel as to the actions taken regarding the transactions. A detailed analysis of suspicious transactions may be warranted to determine if the individuals are utilizing the credit union for structuring activities.
- (16) If weak internal controls were noted or lack of management oversight was determined, the examiner should consider expanding the scope of the BSA examination. The examiner should also consider expanding the scope to other branches/offices, if applicable.
- (17) If potential reporting and recordkeeping violations are noted, the examiner should discuss the violations with the BSA group manager prior to expanding the scope. Depending on the frequency and nature of the violations, the examiner may not need to expand the scope, for example, minor recordkeeping violations. The manager will decide if a FinCEN referral is warranted.

- (18) Other considerations for expanding a BSA examination include prior violations, management cooperation and the filing history recorded on FCQ.
- (19) When expanding the BSA examination, the examiner should consider performing the following:
 - a. Review the credit union's bank statements for activities conducted on the dates selected. Inspect deposit tickets for currency and currency withdrawal source documents such as debit memos and checks.
 - b. Trace currency withdrawals and deposits from the bank deposit slips and currency withdrawal source documents to the cash control system reconciliation reports.
 - c. Reconcile the individual teller cash control sheets to the cash control system reconciliation report totals. Reconcile the cash control system reconciliation beginning/ending cash on hand balances to prior and subsequent cash on hand balances.
 - d. Review individual teller daily cash control sheets and supporting cash in/cash out slips for currency transactions in excess of \$3,000.
- (20) If the credit union has one teller who conducts all large currency transactions, the examiner should focus on the transactions conducted by that teller.
- (21) Trace transactions for the purchase of money orders, traveler's checks, bank drafts, and cashier's checks involving currency in amounts of \$3,000 to \$10,000, inclusive, to the records required by 31 CFR 1010.415(a).
- (22) Trace all transactions for currency deposited or withdrawn in excess of \$10,000 to the retained copies of CTRs or to the exempt customer list.
- (23) If questionable transactions are identified as being conducted by a customer designated as an exempt person, the examiner may want to review the suitability of the exemption.
- (24) The examiner should be alert to transactions or patterns that may indicate potential structuring activities. If structuring is suspected, the examiner should:
 - a. Review the specific member accounts where unusual patterns of activity have occurred. Statements of account transactions for all accounts held by the member should be inspected.
 - b. Related members accounts should be reviewed for transactions occurring in the same general period.
- (25) If potential violations are being conducted through the purchase of traveler's checks, money orders, bank drafts, and cashier's checks, the examiner should review the specific control register used for the negotiable instrument sales to determine the extent of the potential violations.
- (26) When apparent violations have been detected, the examiner should interview management and any other personnel involved. All discussions should be documented in the case file.
- (27) Follow procedures in IRM 4.26.6, *Bank Secrecy Act, Bank Secrecy Act Examiner Responsibilities for BSA Examinations*, to timely conclude the BSA examination.

- (28) Consider preparing Form 5346, *Examination Information Report*, when information is obtained during the BSA examination that indicates a possible income tax violation warranting referral. (IRM 4.26.6)

4.26.9.5.6.1
(06-01-2006)
Review of Exempt Customers

- (1) The examiner will ensure that the credit union is properly designating customers as exempt persons by filing a FinCEN Form 110, *Designation of Exempt Person*, by the close of the 30-day period beginning after the day of the first reportable transaction in currency with that person sought to be exempted.
- (2) Verify the credit union's procedures for exempting transactions of certain depositors from the CTR reporting requirement conform to the requirements of 31 CFR 1020.315, *Transactions of exempt persons*.
- (3) Obtain copies of FinCEN Form 110 filed by the credit union. Customers designated as exempt persons need to meet the specific requirements of 31 CFR 1020.315(b), *Exempt person*.
- (4) Review those customers designated as exempt persons which are non-listed businesses (as defined in 31 CFR 1020.315(b)(6)) since money launderers would most likely try to use this type of business to disguise the source of their funds. Verify the following:
 - a. The credit union has only exempted customers meeting the requirements of an exempt person as defined in 31 CFR 1020.315(b). Pay close attention to non-listed businesses to ensure that they are not primarily engaged in ineligible businesses as set forth in 31 CFR 1020.315(e)(8), *Ineligible businesses*.
 - b. The credit union annually reviews the information supporting each designation of an exempt person and the application to each account of a non-listed business or payroll customer of the monitoring system required to be maintained to detect suspicious transactions. (31 CFR 1020.315(d), *Annual review*)
 - c. The required documentation has been maintained that shows how the customer was determined to be an exempt person. (31 CFR 1020.315(e)(1), *General rule*)
 - d. All suspicious transactions have been reported, whether the customer has been designated as an exempt person. (31 CFR 1020.315(h)(1), *Obligations to file suspicious activity reports and maintain system for monitoring transactions in currency*)

4.26.9.5.6.2
(06-01-2006)
Review of Customer Identification Program

- (1) Verify that the credit union has implemented a written Customer Identification Program (CIP). (31 CFR 1020.220(a)(1), *In general*)
- (2) Verify that the CIP has been approved by the Board of Directors.
- (3) Verify that the written CIP is appropriate for the size and type of business of the credit union, and includes each of the requirements of 31 CFR 1020.220(a), *Customer Identification Program: minimum requirements*, specifically:
 - a. General requirements,
 - b. Identity verification procedures,
 - c. Recordkeeping,

- d. Comparison with government lists, and
- e. Customer notice.

4.26.9.5.7
(11-12-2019)

**Supporting
Documentation**

- (1) The examiner must obtain adequate supporting documentation for each type of the following violations:
 - a. Reporting - The date of the transaction, the amount, the individuals involved and a detailed statement regarding the violation, including copies of source documents such as cash in/out slips, control registers and teller cash proofs which support the violation.
 - b. Recordkeeping - The details of the specific records which were not maintained or were determined to be inadequate, including management's response to the violations.
 - c. Exempt Customers - The nature of the violation, the account history, type of business and the frequency of exempt transactions.
- (2) The credit union's knowledge of BSA requirements must be determined before determining whether violations should be formally referred to FinCEN.
 - a. The key officers and employees should be interviewed again to document the credit unions response to any apparent violations.
 - b. The existence of an internal compliance program may indicate knowledge. For example, if knowledge of the reporting and recordkeeping requirements is limited to upper management and the tellers are not similarly educated, the credit union may be at least negligent (for not properly instructing the tellers). The tellers need to know what their BSA obligations are. The tellers are the initial contact point where the information is obtained. Failure by upper management to ensure that factual information is correctly gathered may indicate the credit union's intent not to comply.
- (3) Some factors indicating the financial institution's knowledge of the BSA reporting and recordkeeping requirements and its compliance intentions are:
 - a. Prior BSA violations and BSA related contact with the IRS,
 - b. Training programs operated by the credit union,
 - c. The MSBs formal BSA compliance procedures, and
 - d. Active involvement of management in oversight and internal control activities.
- (4) In situations where knowledge or intent cannot be established within the scope of selected records, the examiner should expand the period to include recent transactions that occurred after knowledge can be clearly documented. For example, the examiner selected records from January, February, and March. The inspection of these records discloses currency transactions that appear to be structured and which should have been reported. The credit union denied knowledge of the structuring regulations during the initial interview. In April, the examiner informed the credit union about the suspicious transactions and of the structuring regulations. The examiner later expanded the examination period to include May and June transactions. The examiner found violations in May and June. The credit union's knowledge was documented during the notification of the structuring violations and took no action to prevent the recurrence of violations. The credit union's intent to not comply should be documented.

- (5) Because willfulness is a state of mind, generally only circumstantial evidence of willfulness will be available. A willful violation is the intentional violation of a known legal duty.
- (6) Since BSA penalties are assessed by the FinCEN, which does not have any field examiners, the examiner must thoroughly document all facts on the issue of the intent. After the examiner secures the necessary information and documents the apparent violations, the examiner should follow the procedures as detailed in IRM 4.26.8, *Special Procedures*.

4.26.9.5.8
(06-01-2006)
Closing the Examination

- (1) After documenting the potential violations, the examiner should provide a list of the violations to the credit union and solicit a written explanation for each of the violations identified. The list should include:
 - a. Date of the transaction,
 - b. Customer name,
 - c. Account number (if any),
 - d. Amount of the currency transaction(s), and
 - e. Description of the transaction(s).
- (2) The examiner should advise the credit union of any recordkeeping deficiencies as well as any deficiencies in their policies, procedures, internal controls, and compliance programs that might result in noncompliance with the BSA.
- (3) Any additional documents or information, provided by the credit union in response, should be reviewed and a determination should be made as to whether any items should be removed from the list of violations.
- (4) When the credit union contends that a CTR was filed, and provides its retained copy as evidence, the examiner should query the FCQ database and conduct an exhaustive search before concluding that a CTR was not received. In conducting the search, the examiner should query all customer numerical identification on the CTR such as account number (if applicable), SSN, and identification credential number.

4.26.9.5.9
(06-01-2006)
Money Laundering Trends

- (1) The financial institution and/or the customer can be involved in potential money laundering schemes. The examiner must focus on both the financial institution and the transactor(s) during the BSA examination.
- (2) Money laundering techniques which could be used by the financial institution include:
 - a. Failing to maintain complete records.
 - b. Failing to maintain copies of FinCEN Form 110 and related records.
 - c. Failing to record specific transactions.
 - d. Failing to obtain the required information to comply with the recordkeeping requirements.
 - e. Failing to file CTRs and SARs on reportable transactions.
 - f. Filing incomplete CTRs or SARs.
 - g. Structuring a transaction by breaking one transaction into several to circumvent the reporting requirements.
 - h. Designating an ineligible business as an exempt person.
 - i. Failing to maintain a monitoring system to detect suspicious transactions of exempt persons.

- j. Failing to conduct annual reviews of information supporting each designation of exempt persons.
- (3) Money laundering trends which could be used by the customer or transactor include:
 - a. Using several individuals at one or more locations to conduct a transaction.
 - b. Making currency deposits into their member's account(s) on consecutive days which are below the reporting threshold.
 - c. Splitting currency deposits between one or more members' accounts in which each are below the reporting threshold but when combined would require a CTR.
 - d. Check cashing by the same individual or business on a frequent or continuous basis in amounts below the reporting threshold.
 - e. Obtaining designation as an exempt person for which they do not qualify.
 - f. Using aliases when conducting transactions.
 - g. Conducting numerous transactions at the same location at different times of one day.
 - h. Splitting currency transactions by purchasing a variety of financial services (for example money orders, traveler's checks and/or funds transmittals).
- (4) For money laundering trends pertaining to check cashing refer to IRM 4.26.9.4.
- (5) For money laundering trends pertaining to money orders refer to IRM 4.26.9.7.
- (6) For money laundering trends pertaining to traveler's checks refer to IRM 4.26.9.9.
- (7) For money laundering trends pertaining to fund transmittals refer to IRM 4.26.9.8.
- (8) When evidence of a money laundering scheme is uncovered, a referral should be made on Form 5104, *Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*. (IRM 4.26.8)

4.26.9.5.9.1
(06-01-2006)

Examination Techniques

- (1) The following techniques can be useful in uncovering money laundering schemes:
 - a. Identify dates in which large currency transactions have occurred paying attention to currency transactions that are just below the CTR reporting threshold.
 - b. Review all financial services offered on these dates to see if customers are structuring transactions by using a variety of financial products.
 - c. Inspect retained copies of CTRs and SARs to determine if there are any recurring patterns of activity by the same or related members of the credit union.
- (2) The BSA examiner should enter all suspicious transactions recorded for a selected period into a database. Use of the database isolates patterns of suspicious transactions. If transactions are conducted by a specific member, inspect account statements for all accounts held by that member and any other related members.

- (3) Review retained copies of FinCEN Form 110, *Designation of Exempt Person*, looking for any unusual requests for exempt status or ineligible businesses, which have been granted exempt status, which could be used as a front for money laundering.
- (4) For examination techniques pertaining to check cashing refer to IRM 4.26.9.4.
- (5) For examination techniques pertaining to money orders refer to IRM 4.26.9.7.
- (6) For examination techniques pertaining to traveler's checks refer to IRM 4.26.9.9.
- (7) For examination techniques pertaining to fund transmittals refer to IRM 4.26.9.8.

4.26.9.6 (11-12-2019) **Dealers in Foreign Exchange**

- (1) Dealers in foreign exchange provide many of the same services as banks and other regulated financial institutions. In addition to currency exchange these services may include:
 - a. Transmittal of funds (domestic and foreign)
 - b. Check cashing
 - c. Temporary custody of funds on deposit
 - d. Selling money orders or other monetary instruments
 - e. Other related financial services
- (2) Dealers in foreign exchange operate along international borders, in port of entry cities (where international flights land), or near communities of resident aliens.
- (3) A dealer in foreign exchange near the Southwest border may be known as a "Casa de Cambio", Spanish for house of exchange. "Casas de Cambio" deal in exchanging U.S. dollars and Mexican pesos and are found on both sides of the border. Personal exchanges of routine amounts are commonly referred to as "front window" operations. Large and or unusual transactions are referred to as "back room" operations.
- (4) Dealers in foreign exchange are one of the types of financial services providers known as "money services businesses" or MSBs. (IRM 4.26.5, *Bank Secrecy Act History and Law*, for a discussion on MSBs)

4.26.9.6.1 (11-12-2019) **Law**

- (1) A dealer in foreign exchange is a person that accepts the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more countries in exchange for the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more other countries in an amount greater than \$1,000 for any other person on any day in one or more transactions, whether or not for same-day delivery. (31 CFR 1010.100(ff)(1), *Dealer in foreign exchange*)

4.26.9.6.1.1 (11-12-2019) **Reporting Requirements**

- (1) FinCEN Form 112, *Currency Transaction Report*, must be filed for all currency transactions of more than \$10,000 by or on behalf of any one person in one business day. (31 CFR 1010.311, *Filing Obligations for reports of transactions in currency*)

- a. Multiple currency transactions must be aggregated, and a CTR is required, if the business knows or has reason to know that the multiple transactions are by or on behalf of any person and result in either cash in or cash out totaling more than \$10,000 in one business day. (31 CFR 1010.3131(b), *Multiple transactions*)
 - b. The CTR must be filed within 15 calendar days following the day the reportable transaction occurs. (31 CFR 1010.306(a)(1), *Filing of reports*)
- (2) FinCEN Form 111, *Suspicious Activity Report, (SAR)*, is required to be made by dealers in foreign exchange if they suspect or have reason to suspect suspicious activities have occurred. (31 CFR 1022.320, *Reports by money services business of suspicious transactions*)
 - a. A SAR must be filed for suspicious transactions of at least \$2,000 in funds or other assets conducted or attempted by, at, or through the money services business. (31 CFR 1022.320(a)(2), *General*)
 - b. An MSB is required to file the SAR with FinCEN, no later than 30 calendar days after the date of detection. (31 CFR 1022.320(b)(3), *When to file*)
 - c. An MSB is prohibited from notifying any person involved in the transaction that a SAR has been filed. (31 CFR 1022.320(d)(1), *Confidentiality of SARs*)
- (3)) FinCEN Form 105, *Report of International Transportation of Currency or Monetary Instruments (CMIR)*, must be filed by any person who physically transports, mails, or ships or has someone else transport, mail, or ship currency or monetary instruments in an aggregate amount exceeding \$10,000 into or out of the country or who receives such items into the United States from abroad. (31 CFR 1010.340, *Reports of transportation of currency or monetary instruments*)
 - a. FinCEN Form 105 must be filed with the U.S. Customs Service at the time of entry into the United States or at the time of departure, mailing, or shipping from the United States. (31 CFR 1010.306(b))
 - b. CMIR reports are required to be filed within 15 days after receipt of the currency or other monetary instruments. (31 CFR 1010.306(b)(2))
- (4) FinCEN Form 114, *Report of Foreign Bank and Financial Accounts*, must be filed for any financial interest in or signature or other authority over a foreign bank, securities, or other financial account which exceeds certain thresholds by April 15th (for FBARs required for foreign financial accounts maintained during calendar years 2016 and later) or June 30 (for FBARs required for foreign financial accounts maintained during calendar years 2015 and earlier) of the succeeding year. (31 CFR 1010.350, *Reports of foreign financial accounts*) An officer or employee of the following institutions need not report signature or other authority over a foreign financial account owned or maintained by the institution if the officer or employee has no financial interest in the account. (IRM 4.26.16.3.4.1, *Signature Authority Exceptions*)
- (1) A dealer in foreign exchange is required to register on a FinCEN Form 107, *Registration of Money Services Business*, and biannually renew their registration if they are not acting in an agent capacity and are not a branch location. (31 CFR 1022.380, *Registration of money services businesses*)

4.26.9.6.1.2
(11-12-2019)
**Registration
Requirements**

4.26.9.6.1.3
(11-12-2019)
**Recordkeeping
Requirements**

- a. Certain events require re-registration which is different from a renewal registration. (31 CFR 1022.380(b)(4), *Events requiring re-registration*)
- (1) For records required of all financial institutions, refer to IRM 4.26.5, *Bank Secrecy Act, Bank Secrecy Act History and Law*.
- (2) Copies of all filed CTRs must be retained by the financial institution for five years from the date of the report. (31 CFR 1010.306(a)(2), *Filing of reports*)
- (3) Copies of all filed SARs and the original or record of any supporting documentation shall be maintained for five years from the date of filing the SAR. (31 CFR 1022.320(c), *Retention of records*)
- (4) Dealers in foreign exchange are required to make and retain additional records. (31 CFR 1022.410, *Additional records to be made and retained by dealers in foreign exchange*)
 - a. A dealer in foreign exchange is required to secure and maintain a record of the taxpayer identification number of each person who opens a transaction account or is extended a line of credit within 30 days after an account is opened or credit line extended.
 - b. If the person is a non-resident alien, a record of the person's passport number or description of some other government document used to verify identity is required.
 - c. If the account or credit line is in the names of two or more persons, a dealer is required to secure the taxpayer identification number of a person having a financial interest in the account or credit line. (31 CFR 1022.410(a)(1))
 - d. If the dealer is unable to secure a person's identification within the 30-day period, they will not be in violation if a reasonable effort was made to secure the identification and a list is maintained containing the names, addresses, and account or credit line numbers of those persons for which they were unable to secure the required identification. (31 CFR 1022.410(a)(1))
 - e. The 30-day period may be extended if the person opening an account or credit line has applied for a taxpayer identification or social security number. (31 CFR 1022.410(a)(2))
 - f. There are certain instances when a taxpayer identification number need not be secured. (31 CFR 1022.410(a)(3))
- (5) In addition, dealers in foreign exchange are required to retain either the original, microfilm or other copy of the following records pursuant to 31 CFR 1010.410(b):
 - a. Statements of bank accounts, including paid checks, deposit slips, charges, or other debit or credit memoranda.
 - b. Daily work records, including purchase and sales slips or other memoranda needed to identify and reconstruct currency transactions with customers and foreign banks.
 - c. A record of each exchange of currency involving transactions in excess of \$1,000 including the customer's name and address, passport number or taxpayer identification number, date and amount of the transaction, and currency name, country and total amount of each foreign currency.

- d. Signature cards or other documents evidencing signature authority over each deposit or security account, containing the name, address, Taxpayer Identification Number (TIN) of the depositor, the signature of the depositor or other person authorized to sign on the account (if customer accounts are maintained in a code name, a record of the actual owner of the account).
 - e. Each item, including checks, drafts, or transfers of credit of more than \$10,000 remitted or transferred to a person, account or place outside the United States.
 - f. A record of each receipt of currency, other monetary instruments, investment securities, and checks, and of each transfer of funds or credit, or more than \$10,000 received on any one occasion directly and not through a domestic financial institution, from any person, account or place outside the United States.
 - g. Records prepared or received by a dealer in the ordinary course of business, that would be needed to reconstruct an account and trace a check in excess of \$100 deposited in such account through its internal recordkeeping system to its depository institution, or to supply a description of a deposited check in excess of \$100.
 - h. A record maintaining the name, address and TIN, if available, of any person presenting a certificate of deposit for payment, a description of the instrument, and date of the transaction.
 - i. A system of books and records that will enable the dealer to prepare an accurate balance sheet and income statement.
- (6) If a dealer in foreign exchange has a financial interest in or signature or other authority in foreign financial accounts, records of these accounts must be retained. (31 CFR 1010.420, *Records to be made and retained by persons having financial interests in foreign financial accounts*) The records must contain:
- a. The name in which each account is maintained,
 - b. The number or other designation of such account,
 - c. The name and address of the foreign bank or other person with whom such account is maintained,
 - d. The type of such account, and
 - e. The maximum value of each such account during the reporting period.
- (7) A dealer in foreign exchange must retain these records for five years pursuant to 31 CFR 1010.410, *Records to be made and retained by financial institutions*, and 31 CFR 1010.420, *Records to be made and retained by persons having financial interests in foreign financial accounts*, if applicable.
- (8) Copy of Registration of Money Services Business (RMSB) registration and renewal must be retained for five years, if applicable. (31 CFR 1010.430(d), *Nature of records and retention period*)
- (9) Current annual agent list and agent list(s) for the past five years must be retained, if applicable. (31 CFR 1022.380(d), *Nature of records and retention period*)
- (1) All money services businesses must establish and implement a written, risk-based AML Program reasonably designed to prevent the business from being used to facilitate money laundering and the financing of terrorism. (31 CFR 1022.210, *Anti-money laundering programs for money services businesses*)

- (2) Refer to IRM 4.26.5.8, *Anti-Money Laundering (AML) Compliance Program*, for information on AML Compliance Program requirements for MSBs.
- (3) IRM 4.26.6.5.1.2, *Evaluation of AML Program*, contains information on evaluating the AML program.

4.26.9.6.2
(11-12-2019)
Records Commonly Found

- (1) In addition to the required information listed in IRM 4.26.9.6.1.3 the records for a dealer in foreign exchange usually include:
 - a. Annual Summary Sheet: a record of monthly transaction totals.
 - b. Monthly Summary Sheet: a record of daily transaction totals for the month and the source document for preparing the annual summary sheet.
 - c. Client Ledger Cards: a record of transactions with regular clients (larger businesses may maintain this record).
 - d. Daily Transactions Log: a record summarizing daily transactions. This is the source document for preparing the monthly summary sheet and includes the beginning and ending cash balances. If cash balances are not maintained on this record, a separate cash (vault) inventory record is usually maintained.
 - e. Transaction Vouchers: a record of each transaction that shows the date, amount and rate of exchange. This record may, but usually does not, include customer identification for transactions over \$1000. This is the source document for preparing the daily transaction log.
 - f. Domestic Bank Records: these should include all account statements, duplicate deposit tickets, canceled checks, wire transfer confirmation statements, and other debit and credit memoranda.
 - g. Records may also include foreign bank account records and the records of domestic and foreign agents or nominees.

4.26.9.6.3
(06-01-2006)
Interview

- (1) IRM 4.26.6.5.3.3, *Interview*, contains additional information on interviews. Also, refer to BSA Policy SharePoint.
- (2) The initial interview of a dealer in foreign exchange should include questions to ascertain:
 - a. Historical/background information.
 - b. Management and employee knowledge of the BSA registration, record-keeping, reporting, and AML compliance program requirements.
 - c. Information about related dealers in foreign exchange and domestic and foreign agents or nominees.
 - d. Information on domestic and foreign books and records including records of agents or nominees, especially any bank account records that are maintained on behalf of the dealer in foreign exchange.
 - e. The types of transactions conducted, and the records maintained. The examiner may want to prepare a flowchart of the cash in cycle, the cash out cycle, and the records maintained for each type of transaction.
 - f. Procedures for recording currency transactions over \$1,000 and identification of customers.
 - g. Procedures for recording currency transactions over \$10,000 and filing of CTRs. Also, procedures for filing SARs, CMIRs and FBARs (if applicable).

- (3) The examiner must consider additional services or products offered by a dealer in foreign exchange such as money transmitting, check cashing, and sales of money orders.
- (4) A copy of the written BSA compliance procedures should be requested and included in the case file. An explanation of the BSA training of employees should also be documented.
- (5) Interview all individuals conducting currency transactions and those responsible for compliance with the BSA recordkeeping and reporting requirements.
- (6) Each interview should be documented in the case file.
- (7) Ask the owners or management if they have knowledge of any structuring transactions having occurred or if any suspicious transactions have occurred. These questions must also be asked while interviewing employees who have customer contact.
- (8) Interview former employees if appropriate.
- (9) The examiner should ask to be shown how all “window” and “back room” transactions are conducted and recorded.
- (10) Ask open-ended questions throughout the interview. Do not ask questions that require only a “yes” or “no” answer.

4.26.9.6.4
(11-12-2019)

Review of the Records

- (1) See IRM 4.26.6.5.3.6, *Inspection of Books and Records*, for general information on review of records.
- (2) Conduct the BSA examination at the place of business.
- (3) Review the bank account records for all the domestic and foreign bank accounts over which the dealer in foreign exchange has authority. Many dealers or exchangers have foreign bank accounts or use foreign bank accounts held in agent or nominee names to facilitate conducting their financial services. The examiner should probe and ask for foreign bank account records.
- (4) Determine if the records include all financial services provided by the business that have been identified during interviews and from visual observation of the business operations. Pursue any records that have not been provided.
- (5) Select records from a current period to evaluate. The period with the highest money flow should be considered.
- (6) Select dates within the period and reconcile the transaction vouchers, daily transaction log, client ledger, and the monthly and annual summary sheets.
- (7) Analyze the summary and transaction records for cash in and cash out for transactions conducted by business. All large or unusual items should be pursued.
- (8) Trace daily transactions through the daily transaction log. Reconcile the transaction log's beginning and ending cash balances to prior and subsequent logs. Also, trace the transaction log cash balances to the cash (vault) inventory balances and then to the balance sheets and books. Any unexplained varia-

tions should be investigated. If cash balances are not entered on the transaction log, the examiner should ask how the currency dealer or exchanger reconciles the cash on hand.

- (9) Trace transactions to the transaction vouchers, checking for compliance with 31 CFR 1022.410, *Additional records to be made and retained by dealers in foreign exchange*, requirements and trace all transactions over \$10,000 to CTRs.
- (10) Review copies of CTRs, SARs, CMIRs (if applicable) and FBARs (if applicable) for accuracy and completeness. FCQ should also be checked to verify that the reports were filed.
- (11) Review relevant audit reports or reviews that address BSA policies, procedures, or operations for BSA relevant issues.
- (12) Review fund transmittal documents. Records for the transmission of funds abroad should include copies of receipts issued to customers and records evidencing interbank transfers (for example, wire confirmations or drafts).
- (13) Review the written BSA AML compliance program and obtain a copy for the case file.
- (14) Consider using a spreadsheet or database to input information from the transaction records, for purposes of detecting structuring and other money laundering schemes.
- (15) Analyze sorts of the name, address and phone number fields to detect possible structured transactions, unreported transactions, errors and/or deficiencies in the financial institution's BSA compliance system.
- (16) If structured transactions or BSA violations are detected, the examiner should interview the responsible person or employee who conducted the transaction. Based on the responses, the examiner should consider expanding the scope of the examination. (IRM 4.26.6.5.1.1, *Scope and Depth*) All facts should be discussed with the BSA Group Manager.
- (17) Determine if the business is required to register as an MSB and if so, review copies of filed MSB registration and renewal forms (if applicable) for accuracy and completeness.
- (18) See IRM 4.26.6, *Bank Secrecy Act, Bank Secrecy Act Examiner Responsibilities for BSA Examinations*, for information when examining a business headquarters.

4.26.9.6.5 (11-12-2019) Supporting Documentation

- (1) The examiner must obtain adequate supporting documentation for each type of violation:
 - a. Reporting – The date of the transaction, the amount, the individuals involved, and a detailed statement regarding the violation, including copies of source documents such as cash in/out slips, control registers, and teller cash proofs which document the violation.
 - b. Recordkeeping – The details of the specific records which were not maintained or were inadequate, including management's response to the violations.

- (2) The money services business' knowledge of BSA requirements must be determined before deciding if a Letter 1112, *Title 31 Violation Notification Letter*, should be issued or if the case should be referred to FinCEN.
 - a. The key officers and employees should be interviewed again to document the money services business' response to any apparent violations.
 - b. The existence of an internal compliance program may indicate knowledge. For example, if knowledge of the reporting and recordkeeping requirements is limited to upper management and the other employees are not similarly educated, the money services business may be at least negligent for not properly instructing the employees. The employees need to know what their BSA obligations are. The employees are the initial contact point where the information is obtained. Failure by upper management to ensure that factual information is correctly gathered may indicate the money services business' intent not to comply.
- (3) Other factors indicating the money services business' knowledge of the BSA registration, reporting, recordkeeping, and compliance program requirements and its compliance intentions are:
 - a. Prior BSA violations and BSA-related contacts with the IRS
 - b. Training programs offered by the money services business
 - c. The MSB's formal BSA compliance procedures
 - d. Active involvement of management in oversight and internal control activities
- (4) In situations where knowledge or intent cannot be established within the scope of selected records, the examiner should consider expanding the period to include recent transactions that occurred after knowledge can be clearly documented.

Example: The examiner selected records from January, February, and March. The inspection of these records discloses currency transactions that appear to be structured and which should have been reported. The MSB denied knowledge of the structuring regulations during the initial interview. In April, the examiner informed the MSB about the suspicious transactions and of the structuring regulations. The examiner later expanded the examination period to include May and June transactions. The examiner found violations in May and June. The MSB's knowledge was documented during the notification of the structuring violations and took no action to prevent the recurrence of violations. The business's intent to not comply should be documented.
- (5) Because willfulness is a state of mind, generally only circumstantial evidence of willfulness will be available. A willful violation is the intentional violation of a known legal duty.
- (6) IRS does not have the authority to assess penalties under the BSA except for FBAR violations. Significant BSA violations or deficiencies are therefore referred to FinCEN unless a fraud referral is appropriate. The examiner and manager will make a decision regarding whether to refer the case to FinCEN for consideration of civil money penalties. The examiner must thoroughly document all facts on the issue of intent. See IRM 4.26.8, *Special Procedures*, if the case is to be referred to FinCEN.

4.26.9.6.6
(11-12-2019)

Closing the Examination

- (1) Refer to IRM 4.26.6.5.3.10, *Notification of Findings*, for information on notifying the business of examination results.
 - a. If no BSA violations or significant AML program issues have been found, prepare Letter 4029, *Bank Secrecy Act No Change Letter*.
 - b. If BSA violations are found which are technical, minor, infrequent, isolated, or not substantive, a Letter 1112, *Title 31 Violation Notification Letter*, should be issued. See IRM 4.26.8.
 - c. If apparent BSA violations are found which appear to meet the referral criteria, prepare a referral on Form 5104, *Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*. (IRM 4.26.8.5, *Form 5104, Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*)
 - d. If the apparent BSA violations appear to meet criminal referral guidelines, the BSA manager will contact the Fraud Technical Advisor to determine if a Form 2797, *Referral Report of Potential Criminal Fraud Cases*, is warranted. (IRM 4.26.8)
- (2) A closing conference must be held at the close of the examination. See IRM 4.26.6.5.3.11, *Holding the Closing Conference*, for additional information.
- (3) When a Letter 1112, *Title 31 Violation Notification Letter*, is issued, the financial institution is asked to provide a response, amend the AML program, and implement recommendations. Refer to IRM 4.26.6.5.3.12, *Letter 1112 Response*, for additional guidance.
 - a. See IRM 4.26.6.5.3.13, *Delinquent BSA Forms Procedures*, for the process to secure delinquent returns discovered during the examination.
 - b. See IRM 4.26.6.5.3.14, *Case File Closing Procedures*, for procedures when closing the case file.
 - c. See IRM 4.26.6.5.3.16, *Examination Information Report, Form 5346*, for information on preparing and submitting Form 5346, *Examination Information Report*.
 - d. IRM 4.26.6.5.3.17, *Information Items*, provides information on submitting other information items
 - e. IRM 4.26.6.5.3.18, *Examiner-Filed SARs*, provides procedures for submitting examiner filed SARs

4.26.9.6.7
(06-01-2006)

Money Laundering Trends

- (1) Money launderers may use the bank accounts and the investment and financial contacts of a dealer in foreign exchange on both sides of an international border to break the paper trail between their currency and themselves. This permits them to transport, convert or invest currency in the legitimate international financial system. A dealer in foreign exchange involved in money laundering may assist in converting the currency into non-monetary assets, and/or physically transporting currency, and/or making wire transfers, and/or otherwise disguising the ownership of funds.
- (2) Common methods used by dealers in foreign exchange involved in laundering money include:
 - a. Failing to maintain records or record specific transactions.
 - b. Failing to file reports of currency or foreign transactions.
 - c. Disguising transactions with false identification or structuring them to avoid the BSA reporting requirements.

- d. Commingling transactions of clients with those of other clients or of the dealer in foreign exchange.
 - e. Commingling transactions with those of other dealers in foreign exchange frequently claiming that transactions with other dealers in foreign exchange are merely “accommodations” or loans and failing to record the details.
 - f. Using foreign bank accounts, agents, or nominees.
 - g. Issuing cashier’s checks, money orders, personal checks, or other monetary instruments in exchange for currency.
- (3) Some examples of tactics used by dealers in foreign exchange involved in money laundering are:
- a. Fictitious names, addresses, and passport numbers are used in the records and on CTRs filed. Foreign governments issue passports, which are usually untraceable.
 - b. Dollars are physically smuggled out of the U.S. and deposited into a foreign bank account. The money is then wired back to the U.S. or elsewhere with the appearance of a legitimate business transaction. Some dealers in foreign exchange along the Canadian border receive U.S. or foreign currency through U.S. Post Office boxes in border cities. Couriers transport the currency into Canada for exchange or further transmission to anywhere in the world.
 - c. Currency may be transported into a foreign country and repatriated through a foreign bank. Even though a transaction may appear as foreign currency in the cash flow of the dealer in foreign exchange, it may still be from an illegal source.
- (4) The examiner may find instances where international funds transfers occurred without the money crossing the international border. This is accomplished by offsetting different client transactions through book entry systems shared with the dealer in foreign exchange foreign office, or with other dealers, agents, or nominees located on either side of the border. This process is similar to the check clearing operation of the banking industry.
- (5) When evidence of a money laundering scheme is uncovered, a referral should be made on Form 5104, *Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*. Refer to IRM 4.26.8 for referral procedures.

4.26.9.6.7.1
(06-01-2006)

Examination Techniques

- (1) The following techniques can be useful in uncovering money laundering schemes:
- a. Prepare flowcharts of cash in and cash out for each type of financial transaction conducted by the dealer in foreign exchange to identify records that may exist but have not been provided.
 - b. Review all bank statements to determine the dealer in foreign exchange is withdrawing enough funds to meet the amounts of currency exchanged. If not sufficient, then sources of cash should be investigated in greater depth.
 - c. Review the transaction logs and client ledger sheets for large or suspicious transactions. If the paper trail ends before the conclusion of a transaction, ask the dealer in foreign exchange to explain the transaction. Record the explanation and if necessary obtain additional documents.

- d. Review the list of foreign beneficiaries for large amounts, few destinations, or any other factors that may indicate money laundering or other illegal activities by the dealer in foreign exchange or clients.
- e. Review wire transfer confirmations for suspicious items.
- f. Review bank account documents for large or unusual items. Trace these items to the transaction and summary documents. Try to identify records that are not provided for the examination, such as foreign bank accounts or agent and nominee records.
- g. Review the records for transactions with other dealers in foreign exchange. Money laundering often occurs with the cooperation of more than one currency dealer or exchanger.
- h. Isolate and trace all transactions through the records. Client transactions may be commingled to conceal currency transactions. If the transactions cannot be separated, ask the dealer in foreign exchange to provide a complete breakdown of the individual transactions. Document the currency dealer's or exchanger's response.
- i. Identify the profits on all large, structured or suspicious transactions. If individual profits cannot be identified, ask how profits on the transactions are determined and have the currency dealer or exchanger reconstruct them.
- j. Group unusual items to identify any common or similar features such as names or addresses. Once any large, structured or suspicious transactions are identified, all similar transactions within the compliance examination period should be identified and reviewed.

4.26.9.7

(06-01-2006)

Money Orders Overview

- (1) Money orders are issued by national companies such as Money gram, American Express, or the U.S. Post Office. Large companies such as WalMart and Safeway also offer money orders. In addition, there are small regional or local money order companies or some businesses, such as, check cashers, that may issue their own money orders.
- (2) Money orders are negotiable monetary instruments. Money orders are usually purchased by individuals, who do not have a bank checking account to pay their everyday bills.
- (3) Sales agents of money orders usually provide other services such as check cashing, wire services, or operate a business such as a grocery store, truck stop, or a convenience store.
- (4) Rather than run the risk of robbery, some businesses in high-risk areas will buy money orders throughout the day instead of transporting cash to the bank.
- (5) Most money order transactions occur at the \$200 - \$300 level.
- (6) An issuer or seller of money orders is one of the types of financial services providers known as an MSB. Refer to IRM 4.26.5, *Bank Secrecy Act History and Law*, for a discussion on MSBs.
- (7) Many money order sellers have limits on the amount of money orders they will sell.

4.26.9.7.1
(06-01-2006)
**Nationwide Money
Orders**

- (1) Financial institutions that sell money orders for national companies are agents. The agent's relationship to the issuer of the money orders is governed by a trust agreement.
- (2) The agent may advertise that it sells the national company's money orders and is authorized to fill in the dollar amount on behalf of the national companies.
- (3) Money orders are drawn on the national company's bank account and the transaction is not complete until the national company receives the face amount from the agent and the money order clears the bank.
- (4) The dollar value of money orders sold by an agent can be limited by the bonding company's trust agreement or by the agent's policy, but in theory they can be in any denomination.
- (5) The national company issues and the agent maintains sales records, of money orders using a sequential numbering system.
- (6) An agent's summary sales report is sent daily to the national company and the correspondent bank sends a clearing report. Using these reports, the national company keeps a record of all money orders sold and cashed. Agents are sent a discrepancy statement for money orders cashed but not reported as sold.
- (7) Money received from the sale of money orders is usually deposited, by the agent, into a separate bank account. Payment is made to the national company by check, wire transfer, or electronic payment.
- (8) National money order companies either collect their fee up front when the money orders are given to the agents or have their agents remit the fee together with the face amount of the money orders sold.
- (9) Agents may receive commission statements or reconciliations of money orders sold. The agent's commission can be accounted for this way.
- (10) Identification of persons purchasing money orders in amounts under \$3,000 is often left to the individual agents, and in many instances, little or no identification is requested from the purchaser.
- (11) National companies keep a copy of the front and back of all cashed and canceled money orders.

4.26.9.7.1.1
(06-01-2006)
Private Money Orders

- (1) Generally, private companies maintain and reconcile daily records of money orders sold and cashed. Like checks, money orders are cleared by a correspondent bank. If adequate records are not maintained, additional information should be obtained from the correspondent bank.
- (2) Traditionally, private companies do not require identification to purchase money orders unless the amount purchased meets the reporting or recordkeeping levels.

4.26.9.7.2
(11-12-2019)
Law

- (1) A money services business includes an issuer or seller of traveler's checks or money orders and includes a person that:
 - a. Issues money orders that are sold in an amount greater than \$1,000 to any person on any day in one or more transactions (31 CFR 1010.100(ff)(3)(i)) or

- b. Sells traveler's checks or money orders in an amount greater than \$1,000 to any person on any day in one or more transactions. (31 CFR 1010.100(ff)(3)(ii))
- (2) A person who sells money orders in an amount greater than \$1,000 to any person on any day in one of more transactions is defined as a money services business. (31 CFR 1010.100(ff)(3))

4.26.9.7.2.1
(11-12-2019)
Reporting Requirements

- (1) FinCEN Report 112, *Currency Transaction Report*, must be electronically filed for all currency transactions of more than \$10,000. (31 CFR 1010.311, *Filing Obligations for reports of transactions in currency*)
 - a. Multiple currency transactions must be aggregated, and a CTR is required, if the business has knowledge that the multiple transactions are by or on behalf of any person and result in either cash in or cash out totaling more than \$10,000 in one business day. (31 CFR 1010.313(b), *Multiple transactions*)
 - b. The CTR must be filed within 15 calendar days following the day the reportable transaction occurs. (31 CFR 1010.306(a)(1), *Filing of Reports*)
- (2) FinCEN Form 111, *Suspicious Activity Report*, is required to be filed by the money services business if they suspect or have reason to suspect suspicious activities have occurred. (31 CFR 1022.320, *Reports by money services business of suspicious transactions*)
 - a. A SAR must be filed for suspicious transactions of at least \$2,000 in funds or other assets conducted or attempted by, at, or through the money services business. (31 CFR 1022.320(a)(2), *General*)
 - b. To the extent that the identification of suspicious transactions required to be reported is derived from a review of clearance records or other similar records of money orders that have been sold or processed, an issuer of money orders shall only be required to report a suspicious transaction or pattern of transactions that involves or aggregates funds or other assets of at least \$5,000. (31 CFR 1022.320(a)(3))
 - c. An MSB is required to file the SAR with FinCEN, no later than 30 calendar days after the date of detection (31 CFR 1022.320(b)(3), *When to file*)
 - d. An MSB is prohibited from notifying any person involved in the transaction that a SAR has been filed. (31 CFR 1022.320(d)(1), *Confidentiality of SARs*)
- (3) The financial institution may be required to file additional reports. See IRM 4.26.5, *Bank Secrecy Act, Bank Secrecy Act History and Law*, for BSA reporting requirements.
- (4) FinCEN requires that most FinCEN reports be filed electronically through its E-file system.

4.26.9.7.2.2
(06-01-2006)
Registration Requirements

- (1) A money order issuer or seller is required to register on a FinCEN Form 107, *Registration of Money Services Business (RMSB)*, and biannually renew their registration if they are not acting in an agent capacity and are not a branch location. (31 CFR 1022.380, *Registration of money services businesses*)

4.26.9.7.2.3
(11-12-2019)
**Recordkeeping
Requirements**

- (2) Certain events require re-registration which is different from a renewal registration. (31 CFR 1022.380(b)(4), *Events requiring re-registration*)
- (1) For records required of all financial institutions, see IRM 4.26.5, *Bank Secrecy Act, Bank Secrecy Act History and Law*.
- (2) Copies of all filed CTRs must be retained by the financial institution for five years from the date of the report. (31 CFR 1010.306(a)(2), *Filing of reports*)
- (3) Copies of all filed SARs and the original or record of any supporting documentation shall be maintained for five years from the date of filing the SAR. (31 CFR 1022.320(c), *Retention of records*)
- (4) Certain records are required to be maintained for the issuance or sale of money orders which involve currency in amounts of \$3,000 to \$10,000, inclusive, by or on behalf of one individual in one business day. (31 CFR 1010.415(a)(2), *Purchases of bank checks and drafts, cashier's checks, money orders and traveler's checks*)
- (5) The following information must be obtained for the records:
 - a. The purchaser's name and address,
 - b. The purchaser's social security number or alien identification number,
 - c. The purchaser's date of birth,
 - d. The date of purchase,
 - e. The type of instruments purchased,
 - f. The serial numbers of the instruments purchased,
 - g. The amount in dollars of each instrument purchased, and
 - h. The financial institution is required to verify the purchaser's name and address and record the specific identifying information (for example, State of issuance and purchaser's driver's license number). (31 CFR 1010.415(a)(2)(ii))
- (6) These records must be retained by the financial institution for five years. (31 CFR 1010.415(c))
- (7) Copy of RMSB registration and renewal, if applicable, must be retained for five years. (31 CFR 1010.430(d), *Nature of records and retention period*)
- (8) Current annual agent list and agent list(s) for the past five years if applicable. (31 CFR 1022.380(d), *Nature of records and retention period*)

4.26.9.7.2.4
(06-01-2006)
**AML Program
Requirements**

- (1) All money services businesses must establish and implement a written, risk-based AML program reasonably designed to prevent the business from being used to facilitate money laundering and the financing of terrorism. (31 CFR 1022.210, *Anti-money laundering programs for money services businesses*)
- (2) Refer to IRM 4.26.5.8, *Anti-Money Laundering (AML) Compliance Program*, for information on AML Compliance Program requirements for MSBs.
- (3) IRM 4.26.6.5.1.2, *Evaluation of AML Program*, contains information on evaluating the AML program.

4.26.9.7.3
(11-12-2019)
Records Commonly Found

- (1) In addition to the required information listed in IRM 4.26.9.7.2.3, money order agent records may include:
 - a. Bank statements and deposit slips
 - b. Daily sales summaries
 - c. Customer records (electronic or hard copies)
 - d. Carbons or duplicates of money orders
 - e. Commission statements
- (2) In addition to the above, issuers of money orders will have records of cleared money orders.

4.26.9.7.4
(11-12-2019)
Interview

- (1) IRM 4.26.6.5.3.3, *Interview*, contains additional information on interviews.
- (2) Interview the officers, owners and employees to determine their knowledge of the BSA and the financial institution's procedures to comply with the reporting and recordkeeping requirements. The duties and responsibilities of the officers and employees should be documented along with a description of the financial institution's records and an explanation of the flow of transactions through the records. Knowledge is one of the elements needed to prove willfulness with respect to apparent violations of the regulations.
- (3) Ask specific questions relating to the business, area, and services offered. The examiner must consider all services offered by the business, such as money transmitting, check cashing, and sales of money orders. For example, a customer could attempt to launder \$15,000 by sending a wire transfer for \$8,000 and purchasing \$7,000 in money orders.
- (4) Ask the owners or management of the financial institution if they have knowledge of any structured transactions having occurred, or if any suspicious transactions have occurred. This question should be asked again while interviewing employees who have customer contact.
- (5) Interview all individuals who handle currency transactions. Question their knowledge and training of the BSA recordkeeping and reporting requirements.
- (6) Ask open-ended questions throughout the interview. Do not ask questions that require only a yes or no answer.
- (7) Additional information can be found on the BSA Policy SharePoint. (IRM 4.26.9.1.5)

4.26.9.7.5
(11-12-2019)
Review of the Records

- (1) See IRM 4.26.6.5.3.6, *Inspection of Books and Records*, for general information on the review of records.
- (2) Any records the financial institution maintains that are relevant to the BSA examination can be requested and reviewed. The examiner will determine if the financial institution is maintaining adequate records and must document any recordkeeping violations.
- (3) Review the written policy statements and procedures of the financial institution as they relate to the BSA.
- (4) Analyze the records of the financial institution for all types of financial services offered. Each type of financial service should be examined separately.

- (5) Determine the money order register completeness by reconciling this to the summary sales reports sent to the issuing company, the discrepancy report from the issuing company, and the bank deposits.
- (6) Trace large block sales or large dollar single transaction sales of money orders in the money order register or money order close out reports to the records required for recordkeeping, SAR reporting and CTR reporting. Block sales are a group of sequentially numbered money orders sold concurrently for the maximum denomination, or right below the maximum dollar amount. The maximum amount allowed for each money order is usually set at \$300, \$500 or \$1,000 by the issuing company. The review should identify:
 - a. Blocks of money orders at \$2,000 or right below for SAR reporting,
 - b. Blocks of money orders at \$3,000 to \$10,000, inclusive, for recordkeeping requirements, and
 - c. Blocks of money orders greater than \$10,000 for CTR reporting.
- (7) Inspect any copies of money orders retained by the financial institution.
- (8) The examiner can request copies of money orders from the money order issuer for any questionable or suspicious transactions. It may be necessary to issue a Title 31 summons to obtain this information. Refer to IRM 4.26.8, *Special Procedures*, before issuing any Title 31 summons.
- (9) Review the financial institution's records to determine if all the required information on the purchasers of money orders involving currency in amounts of \$3,000 to \$10,000, inclusive, has been maintained and verified pursuant to the recordkeeping requirements of 31 CFR 1010.415(a)(2).
- (10) It is recommended that a spreadsheet be used when the compliance examination is part of a multiple location local project or there are many block sales or large dollar sales. All single or block transactions, exceeding a dollar amount cutoff should be entered in the spreadsheet from source documents to see if the transactions are related.
- (11) At a minimum, analyze sorts of the sender name field, receiver name field, and the address field to detect possible structured transactions, unreported transactions, errors, and deficiencies in the financial institution's BSA compliance system.
- (12) The records, if applicable, of BSA examinations of nearby financial institutions in geographical targeting projects should be consolidated and sorted to detect related structuring activity occurring at more than one location.
- (13) Review copies of CTRs filed by the financial institution to ensure they are accurate and complete. Ensure filed CTRs have been retained by the financial institution for the required five-year period. Use the FCQ database to verify that the CTRs were timely filed and contain the same information as the copies maintained by the financial institution.
- (14) Query FCQ database for transactions conducted by owners, managers, and employees of the financial institution to detect possible unreported transactions of the financial institution that were instead reported under the individual's name.
- (15) If structured transactions or other BSA violations are detected, the examiner should interview the responsible person or employee who conducted the trans-

action. Based on the answers given, the examiner should consider expanding the scope of the examination. (Refer to IRM 4.26.6, *Bank Secrecy Act Examiner Responsibilities for BSA Examinations*, and IRM 4.26.13, *Structuring*). All facts should be discussed with the BSA Group Manager.

- (16) Review relevant audit reports or reviews that address BSA policies, procedures, or operations for BSA issues.
- (17) Review copies of filed MSB registrations and renewals (if applicable) for accuracy and completeness.
- (18) Determine whether the business was required to register as an MSB.
- (19) Review agent list (if applicable) for all required elements.
- (20) Forward agent list to a Centralized Exam (HQ) coordinator.
- (21) Review agent contracts and terms for acceptance and termination as an agent.

4.26.9.7.6 (11-12-2019) **Supporting Documentation**

- (1) The examiner must obtain documentation for each type of the following violations:
 - a. Reporting – The date of the transaction, the amount, the individuals involved, and a detailed statement regarding the violation, including copies of source documents such as cash in/out slips, control registers, and teller cash proofs which support the violation.
 - b. Recordkeeping – The details of the specific records which were not maintained or were inadequate, including management’s response to the violations.
- (2) The knowledge of the MSB must be established before determining if a Letter 1112, *Title 31 Violation Notification Letter*, should be issued or if the case should be referred to FinCEN.
 - a. The key officers and employees should be interviewed to document the money services business’ response to any apparent violations.
 - b. The existence of an internal compliance program may indicate knowledge.
 - c. If knowledge of the reporting and recordkeeping requirements is limited to upper management and the other employees are not similarly educated, the money services business may be negligent for not properly instructing the employees. The employees need to know what their BSA obligations are. The employees are the initial contact point where the information is obtained.
- (3) Other factors that may indicate the MSB had knowledge of the BSA registration, reporting, recordkeeping, and compliance program requirements, and its compliance intentions are:
 - a. Prior BSA violations and BSA compliance related contacts with the IRS,
 - b. Training programs offered by the business,
 - c. The MSB’s formal BSA compliance procedure, and
 - d. Active involvement of management in oversight and internal control activities.

- (4) In situations where knowledge cannot be established within the scope of selected records, the examiner should expand the period to include recent transactions that occurred after knowledge and intent can be clearly documented. For example, the examiner selected records from January, February, and March. The inspection of these records discloses currency transactions that appear to be structured and which should have been reported. The MSB denied knowledge of the structuring regulations during the initial interview. In April, the examiner informed the MSB about the suspicious transactions and of the structuring regulations. The examiner later expanded the examination period to include May and June transactions. The examiner found violations in May and June. The MSB's knowledge was documented during the notification of the structuring violations and took no action to prevent the recurrence of violations. The MSB's intent to not comply should be documented.
- (5) Because willfulness is a state of mind, generally only circumstantial evidence of willfulness will be available. A willful violation is the intentional violation of a known legal duty.
- (6) IRS does not have the authority to assess penalties under the BSA except for FBAR violations. Significant BSA violations or deficiencies are therefore referred to FinCEN unless a fraud referral is appropriate. The examiner and manager will make a decision regarding whether to refer the case to FinCEN for consideration of civil money penalties. The examiner must thoroughly document all facts on the issue of intent. See IRM 4.26.8 if the case is to be referred to FinCEN.

4.26.9.7.7
(11-12-2019)

Closing the Examination

- (1) Refer to IRM 4.26.6.5.3.10, *Notification of Findings*, for information on notifying the business of examination results.
 - a. If no BSA violations or significant AML program issues have been found, prepare Letter 4029, *Bank Secrecy Act No Change Letter*.
 - b. If BSA violations are found which are technical, minor, infrequent, isolated, or not substantive, a Letter 1112, *Title 31 Violation Notification Letter*, should be issued. See IRM 4.26.8.
 - c. If apparent BSA violations are found which appear to meet the referral criteria, prepare a referral on Form 5104, *Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*. See IRM 4.26.8.6, *Form 5104, Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*.
 - d. If the apparent BSA violations appear to meet criminal referral guidelines, the BSA manager will contact the Fraud Technical Advisor to determine if a Form 2797, *Referral Report of Potential Criminal Fraud Cases*, is warranted. (IRM 4.26.8)
- (2) A closing conference must be held at the close of the examination. See IRM 4.26.6.5.3.11, *Holding the Closing Conference*, for additional information.
- (3) When a Letter 1112, *Title 31 Violation Notification Letter*, is issued, the financial institution is asked to provide a response, amend the AML program, and implement recommendations. Refer to IRM 4.26.6.5.3.12, *Letter 1112 Response*, for additional guidance.
 - a. See IRM 4.26.6.5.3.13, *Delinquent BSA Forms Procedures*, for the process to secure delinquent returns discovered during the examination.

- b. See IRM 4.26.6.5.3.14, *Case File Closing Procedures*, for procedures when closing the case file.
- c. See IRM 4.26.6.5.3.16, *Examination Information Report, Form 5346*, for information on preparing and submitting Form 5346, *Examination Information Report*.
- d. IRM 4.26.6.5.3.17, *Information Items*, provides information on submitting other information items.
- e. IRM 4.26.6.5.3.18, *Examiner-Filed SARs*, provides procedures for submitting examiner filed SARs.

4.26.9.7.8
(06-01-2006)
**Money Laundering
Trends**

- (1) The financial institution and/or the customer can be involved in potential money laundering schemes. The examiner must focus on both the financial institution and the transactor(s) during the BSA compliance examination.
- (2) Money laundering techniques which could be used by the financial institution include:
 - a. Failing to maintain complete records.
 - b. Failing to record specific transactions.
 - c. Failing to obtain the required information to comply with the recordkeeping requirements.
 - d. Failing to file CTRs or CMIRs on reportable transactions.
 - e. Structuring a transaction by breaking one transaction into several to circumvent the reporting requirements.
 - f. Issuing money orders, instead of cash (for example, a check casher) to avoid the \$10,000 reporting requirement.
- (3) Money laundering techniques which could be used by the customer/transactor include:
 - a. Using multiple locations to conduct transactions.
 - b. Using several individuals at one or more locations to conduct a transaction.
 - c. Using aliases when conducting transactions.
 - d. Conducting several transactions at the same location at different times for one day.
 - e. Requesting money orders, instead of cash, when cashing checks to circumvent a reporting requirement.
- (4) When evidence of a money laundering scheme is uncovered, a referral should be made on Form 5104, *Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*. (Refer to IRM 4.26.8 for referral procedures)

4.26.9.7.8.1
(11-12-2019)
Examination Techniques

- (1) The following techniques can be useful in uncovering money laundering schemes:
 - a. Review the financial institution's sales logs and/or daily summaries for block purchases. Trace these purchases to records of sales of \$3,000 or more,
 - b. Request copies of money orders from the issuer, if necessary, to determine if transactions have been structured.

4.26.9.8
(06-01-2006)
**Money Transmitter
Overview**

- (1) There are currently several major and many regional money transmission companies that operate within the United States. Some of the largest include, but are not limited to, Western Union, Vigo Remittance, and Money Gram. In addition, many banks are aggressively competing in this business.
- (2) A money transmitter may allow customers to send and receive money throughout the United States or anywhere in the world. A customer can send money by visiting any participating outlet, filling out a money transfer form and paying for the transaction. The same is true for the receiving side of the transaction. Some money transmitters also allow sending money by logging in to their system online.
- (3) Each money transmitter has a home office, a transaction clearing center or service center, and several regional offices.
- (4) Each major money transmission company contracts with independent agents. These agents include individuals, as well as, businesses such as grocery stores, truck stops, check cashers, pharmacists, travel agents, and supermarket chains.
- (5) The money transmission home office pays its agents using a “fee schedule” that provides predetermined charges (fees) for money transfers.
- (6) Agents (agencies) receive a commission on the fees charged for transferring money.
- (7) Agents (agencies) are in the 50 States, Puerto Rico, the U.S. Virgin Islands, and Guam. Some are open 24 hours a day.
- (8) Each money transmission company has its own forms to send and receive money. General characteristics include, but are not limited to:
 - a. The date of transaction,
 - b. The amount of the transaction,
 - c. The name of the person sending money (sender/payer),
 - d. The name of the person receiving the money (recipient/receiver/pay to), and
 - e. The reference (transaction) number assigned by the service center.
- (9) When a transaction to send or to receive money is initiated by a customer, the money transmitter will contact the service center. This can be done by either dialing a toll-free telephone number or using an on-line computer system (optional equipment for agent). The information from the customer transaction form is entered into the service center computer system.
- (10) The original transaction documents to send or to receive money are kept by the money transmitter anywhere from six months to several years. The retention period is usually determined by the money transmission home office.
- (11) Identification and verification of identification on certain thresholds of transactions are governed by 31 CFR 1010.311, *Filing obligations*, for reports of transactions in currency and 31 CFR 1010.400, *Records to be made and retained by financial institutions*. Below the thresholds that trigger identification and verifications requirements, identification may not be required by the companies for either the person sending the money or the person receiving the

money. There is a “test question” on some sending forms that waives identification on the recipient side of the transaction if the recipient knows the correct answer.

- (12) Money transmission companies usually give policy and procedure guidelines to each of their agents through periodic newsletter updates.
- (13) Money transmitters are one of the types of financial services providers known as “money services businesses” or MSBs. Refer to IRM 4.26.5, *Bank Secrecy Act, Bank Secrecy Act History and Law*, for a discussion on MSBs.

4.26.9.8.1 (11-12-2019) Terminology

- (1) Date - The date of the transaction.
- (2) Destination - Where the money is being sent.
- (3) Draft Number - A number assigned by the money transmitter on its pre-numbered forms.
- (4) Identification - This is generally required of the person receiving the wire transfer.

Note: The identification of the recipient can be avoided by answering the test question.

- (5) Message - Additional remarks given by the sender for the recipient.
- (6) Method of Payment - Cash, Visa, MasterCard.
- (7) Origin of Transaction - The city where the transaction originated.
- (8) Pay To - The person designated as the one to receive the money transfer.
- (9) Payee’s Name - The person designated to receive the money.
- (10) Receiver - This is the name of the person receiving the money transfer.
- (11) Recipient’s Name/Receiver - The person designated to receive the money.
- (12) Reference Number - A number assigned by the agent’s service center to each specific transaction being sent. It can be used to trace a specific transaction.
- (13) Sender -The customer sending the money.
- (14) Test Answer - This is the response required for the test question.
- (15) Test Question - Secret password or words provided by the sender wherein identification is waived for the recipient.
- (16) Transaction Number - Number assigned to the transaction for tracing.

4.26.9.8.2 (11-12-2019) Law

- (1) A money transmitter is defined as a person that provides money transmission services. The term “money transmission services” means the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means. (31 CFR 1010.100(ff)(5), *Money transmitter*)

4.26.9.8.2.1
(11-12-2019)

Reporting Requirements

- (1) FinCEN Form 104, *Currency Transaction Report*, must be electronically filed for all currency transactions of more than \$10,000 in one business day. (31 CFR 1010.311, *Filing Obligations for reports of transactions in currency*)
 - a. Currency received from the sender through a money transmitter or paid to the receiver through a money transmitter can trigger the reporting requirement.
 - b. Multiple currency transactions must be aggregated and a CTR is required if the business has knowledge that the multiple transactions are by or on behalf of any one person and result in either cash in or cash out totaling more than \$10,000 in one business day. (31 CFR 1010.313(b), *Multiple transactions*)
 - c. The CTR must be filed within 15 calendar days following the day the reportable transaction occurs. (31 CFR 1010.306(a)(1), *Filing of reports*)
- (2) FinCEN Form 111, *FinCEN suspicious activity report*, is required to be made by the money services business if they suspect or have reason to suspect suspicious activities have occurred. (31 CFR 1022.320, *Reports by money services business of suspicious transactions*)
 - a. A SAR must be filed for suspicious transactions of at least \$2,000 in funds or other assets conducted or attempted by, at, or through the money services business. (31 CFR 1022.320(a)(2), *General*)
 - b. An MSB is required to file the SAR with FinCEN no later than 30 calendar days after the date of detection. See 31 CFR 1022.320(b)(3), *When to file*.
 - c. An MSB is prohibited from notifying any person involved in the transaction that a SAR has been filed. (31 CFR 1022.320(d)(1), *Confidentiality of SARs*)
- (3) The financial institution may be required to file additional reports. (IRM 4.26.5, *Bank Secrecy Act, Bank Secrecy Act History and Law for BSA reporting requirements*)
- (4) FinCEN requires that most FINCEN reports be filed electronically through its E-file system.

4.26.9.8.2.2
(06-01-2006)

Registration Requirements

- (1) A money transmitter is required to register on a FinCEN Form 107, *Registration of Money Services Business*, and biannually renew their registration if they are not acting in an agent capacity and are not a branch location. (31 CFR 1022.380, *Registration of money services businesses*)
- (2) Certain events require re-registration which is different from a renewal registration. (31 CFR 1022.380(b)(4), *Events requiring re-registration*)

4.26.9.8.2.3
(11-12-2019)

Recordkeeping Requirements

- (1) For records required of all financial institutions, refer to IRM 4.26.5, *Bank Secrecy Act, Bank Secrecy Act History and Law*.
- (2) Copies of all filed CTRs must be retained by the financial institution for five years from the date of the report. (31 CFR 1010.306(a)(2), *Filing of reports*)
- (3) Copies of all filed SARs and the original or record of any supporting documentation shall be maintained for five years from the date of filing the SAR. (31 CFR 1022.320(c), *Retention of Records*)

- (4) Certain records are required to be retained for funds transfers (wires) of \$3,000 or more sent or received by or for an individual on any one business day. (31 CFR 1010.410(e), *Nonbank financial institutions*)
- (5) The following information must be obtained for the records (CFR 1010.410(e)(1), *Recordkeeping requirements*):
 - a. The transmitter's name and address.
 - b. The amount of the transmittal order.
 - c. The execution date of the transmittal order.
 - d. Any payment instructions received from the transmitter.
 - e. The identity of the recipient's financial institution.
 - f. The name and address of the recipient received with the transmittal order.
 - g. The account number of the recipient received with the transmittal order.
 - h. Any other specific identifier of the recipient received with the transmittal order.
 - i. Any form relating to the transmittal of funds that is completed or signed by the person placing the order received with the transmittal order.
- (6) If the transmitter is not an established customer, generally the following records also must be retained. (31 CFR 1010.410(e)(2), *Transmitters other than established customers*) If the transmittal order is made in person, prior to acceptance the transmitter shall verify the identity of the person placing the transmittal order.
 - a. Verification of the transmitter's name and address.
 - b. The type and number of identifications reviewed (for example, driver's license).
 - c. The transmitter's taxpayer identification number (for example, social security number, or, if none, alien identification number, passport number, and country of issuance, or notation in the record of the lack thereof).
- (7) If the recipient is not an established customer, the following records must be retained:
 - a. The original, microfilm, other copy, or electronic record of the transmittal order.
 - b. Verification of the recipient's name and address.
 - c. The type and number of the identification reviewed (for example, driver's license).
 - d. The recipient's taxpayer identification number (for example, social security number, alien identification number, passport number, and country of issuance).
- (8) These records must be retained by the financial institution for five years. (31 CFR 1010.430(d))
- (9) Copy of MSB registration form, if applicable.
- (10) Current annual agent list and agent list(s) for the past five years must be retained, if applicable. (31 CFR 1022.380(d), *Nature of records and retention period*)

4.26.9.8.2.4
(11-12-2019)
**AML Program
Requirements**

- (1) All money services businesses must establish and implement a written, risk-based AML program reasonably designed to prevent the business from being used to facilitate money laundering and the financing of terrorism. (31 CFR 1022.210, *Anti-money laundering programs for money services businesses*)
- (2) All AML programs must be tailored to each business and its services.
- (3) Money transmitters should consider the concept of “Enhanced Due Diligence” in their program. This requires procedures to ensure those customers conducting a higher volume of recurrent transactions are not using their services to facilitate money laundering. Financial institutions need to be able to identify these customers and they should have procedures to ensure the funds are from a legitimate source and there is a business purpose for the transactions. If they cannot ensure they are not being used to facilitate money laundering, they need to consider whether they want to continue to allow these customers to use their services. See the DOJ’s settlement with Sigue on the BSA Policy SharePoint.
- (4) Not all financial institutions are required to have a KYC (Know Your Customer) program. However, all financial institutions, except check cashers, are required to have a SAR program. It is virtually impossible to have an effective SAR program unless the institution also has a KYC program, the financial institutions should have enhanced due diligence procedures that require them to obtain additional information on customers who do a higher volume of recurrent transactions in significant sums which places the financial institution at risk for potential money laundering or other illegal activity.
- (5) Refer to IRM 4.26.5.8, *Anti-Money Laundering (AML) Compliance Program*, for information on AML Compliance Program requirements for MSBs.
- (6) IRM 4.26.6.5.1.2, *Evaluation of AML Program*, contains information on evaluating the AML program.

4.26.9.8.3
(11-12-2019)
**Records Commonly
Found**

- (1) In addition to the required information listed in IRM 4.26.9.8.2.3 a money transmitter’s records usually include:
 - a. Bank statements and deposit slips,
 - b. The money transmitter’s send and receive forms completed by the customers,
 - c. Commission statements,
 - d. Agent records of \$3,000 transactions, and
 - e. Teller’s daily reconciliations.
- (2) Examiners may also request downloads of transactions from the principal money transmitter.

4.26.9.8.4
(11-12-2019)
Interview

- (1) IRM 4.26.6.5.5.3, *Interview*, contains additional information on interviews. Also, refer to BSA Policy SharePoint.
- (2) Ask specific questions relating to the business, area, and services offered. The examiner must consider all financial services or products offered by the business, such as money remittance, check cashing, and sales of money orders. For example, a customer could attempt to launder \$15,000 by sending a wire transfer for \$8,000 and purchasing \$7,000 in money orders.

- (3) Identify the BSA compliance officer and all other personnel who are responsible for conducting, recording, and reporting of BSA transactions and evaluate their understanding of the BSA recordkeeping and reporting requirements. It is important to establish knowledge of the BSA should any violations be noted during the examination. These individuals should be identified by name, title, and specific responsibilities.
- (4) Ask the owners or management of the financial institution if they have knowledge of structuring transactions having occurred, or if any suspicious transactions have occurred. This question also must be asked while interviewing employees who have customer contact.
- (5) Interview all individuals who handle currency transactions (for example, prepare currency reports, maintain records, and other similar items.). Determine their knowledge and amount of training received on the BSA recordkeeping and reporting requirements.
- (6) Ask open-ended questions throughout the interview. Do not ask questions that require only a yes or no answer.
- (7) Each interview should be documented in the case file.
- (8) Interview the AML compliance officer, as well as compliance program employees. Determine the level of familiarity with internal compliance programs and internal controls.

4.26.9.8.5 (11-12-2019) **Review of the Records**

- (1) See IRM 4.26.6.5.3.6, *Inspection of Books and Records*, and IRM 4.26.6.5.3.1, *BSA Examination Techniques*, for general information on the review of records.
- (2) Any records the financial institution maintains for the business that are relevant to the BSA examination can be requested and reviewed. The examiner will determine if the financial institution is maintaining adequate records and must document any recordkeeping violations.
- (3) Ask to see the money transmission company's policy and procedures manual regarding the BSA registration, recordkeeping, reporting, and AML compliance program requirements. The examiner should review the information for completeness and determine if AML compliance program procedures are adequate. Determine how risk of money laundering was assessed and how this risk assessment figured into the establishment of the compliance program. See IRM 4.26.6.5.1.1.1, *Risk Assessment*, for additional information on risk assessments.
- (4) Inspect a sample of copies of CTRs and SARs filed by the money services business to ensure they are accurate and complete. Ensure filed CTRs and SARs have been retained by the financial institution for the required five-year period. Use FCQ to verify that the CTRs and SARs were timely filed and contain the same information as the copies maintained by the financial institution.
- (5) Review internal audits and external agency audits and reviews specific to BSA policies, procedures, or operations for BSA issues.
- (6) Review monthly commission statements to detect large daily transactions or transactions conducted over a period of several days (multiple transactions)

which appear to be related. (Each money transmitter receives commission statements from their respective money transmission business center or home office)

- (7) The examiner should determine whether it is appropriate to request electronic downloads based on the records available at the financial institution. Third-party downloads should be requested for entities that do not have sufficient POS systems or other records to make proper BSA compliance determinations. If the electronic downloads are requested, they may be used in some of the steps mentioned below.
- (8) Review the daily cash reports and reconcile these to the bank deposit slips. Generally, a money transmitter will deposit all monies received each day. The daily cash reports can be traced to the daily summary sheets and the deposit slips to the monthly bank statements.
- (9) Review the daily summary sheets for all send and receive transactions. If the daily summary sheet has 20 transactions recorded, there should be 20 transaction documents to support them. The amounts listed on the daily summary sheet can be reconciled to the original send or receive documents. Review the original send and receive transaction forms for completeness. Determine if all the required information has been obtained and recorded on the forms. The examiner may use dollar amount criteria for selecting forms for inspection.
- (10) Review the original send and receive transaction forms for completeness. Determine if all the required information has been obtained and recorded on the forms. The examiner may elect to select dollar criteria for inspection of these forms.
- (11) Look at the transaction and fee amounts recorded on the transaction forms. The total amount collected line should include both the transaction amount and fees collected. These totals can be traced to the daily summary sheets.
- (12) Scan each group of records for possible structured transactions occurring on the same day or over a period of several days. For example, a 5:00 PM transaction with the transactor sending \$6,000, and again at the same location on the same day a 5:10 PM transaction with the transactor sending \$5,000, could be structured transactions. Examiners should be aware of these or similar situations and must be prepared to discuss suspicious transactions with the money transmitter.
- (13) When reviewing money transmitter transactions, note the telephone numbers given. A sender may give a false name and address but may use a correct telephone number. The reason is that if the money cannot be delivered, the sender will want to be notified. Also watch for repetitive addresses, and sender and/or receiver names.
- (14) Review the financial institution's records to determine if all the required information on money transmittals of \$3,000 or more has been obtained and retained pursuant to the recordkeeping requirements of 31 CFR 1010.410(e), *Nonbank financial institutions*.
- (15) The examiner may elect to use a database to input information from the transaction records into a spreadsheet for purposes of detecting structuring and other money laundering schemes.

- (16) Conduct sorts of the various fields to detect possible structured transactions, unreported transactions, errors, and/or deficiencies in the financial institution's BSA compliance system.
- (17) When sorting a large volume of records, especially with wire transfer downloads, it is virtually impossible to identify any underlying pattern of suspicious activity without "linking" related transactions. Linking related sender and beneficiary transactions is accomplished by assigning a unique code to the related transactions when conducting the various sorts. When additional related transactions are identified, the unique code is added to those transactions. Sorting the data by the "Code" field identifies the unusual patterns of transactions which warrant further scrutiny. See ELMS course 36005, *BSA Title 31 Unit II – Structuring & SARs for additional information*.
- (18) If structured transactions or other BSA violations are detected, the examiner should interview the responsible person or employee who conducted the transaction. Based on the answers given, the examiner should consider expanding the scope of the examination. (IRM 4.26.6.5.1.1, *Scope and Depth*) All facts should be discussed with the BSA Group Manager. The examiner and BSA Group Manager will decide whether to refer the violation to FinCEN for possible enforcement action.
- (19) Obtain copies of all source documents that document any apparent BSA violations.
- (20) Determine if the business is required to register as an MSB and if so, review copies of filed MSB registration and renewal forms for accuracy and completeness.
 - a. Review agent list (if applicable) for all required elements.
 - b. Forward agent list to a Centralized Exam (HQ) coordinator.
- (21) Review agent contracts and terms for acceptance and termination as an agent.
- (22) During a BSA compliance examination of a national money transmitter's headquarters, obtain and review information on the agent network, sales/ transmission and commission records, compliance program records, and internal processes for money transmission and reconciliation. Exams at the corporate level should focus on: compliance monitoring of operations, compliance training of issuer personnel and of agents, and internal reporting of compliance issues or of unusual transaction activity. See IRM 4.26.6, *Bank Secrecy Act Examiner Responsibilities, for BSA Examinations*, for information when examining a business headquarters.

4.26.9.8.6
(11-12-2019)
**Supporting
Documentation**

- (1) The examiner must obtain documentation for each violation.
 - a. Reporting – The date of the transaction, the amount, the individuals involved, and a detailed statement regarding the violation, including copies of source documents such as cash in/out slips, control registers, and teller cash proofs which support the violation.
 - b. Recordkeeping – The details of the specific records which were not maintained or were inadequate, including management's response to the violations.

- (2) The knowledge of the money services business must be determined before determining if a Letter 1112, *Title 31 Violation Notification Letter*, should be issued or if the case should be referred to FinCEN.
 - a. The key officers and employees should be interviewed again to document the money services business' response to any apparent violations.
 - b. The existence of an internal compliance program may indicate knowledge. For example, if knowledge of the reporting and recordkeeping requirements is limited to upper management and the other employees are not similarly educated, the money services business may be at least negligent for not properly instructing the employees. The employees need to know their BSA obligations. The employees are the initial contact point where the information is obtained. Failure by upper management to ensure that information is correctly gathered may establish evidence of the money services business' intent not to comply.
- (3) Other factors indicating the money services business' knowledge of the BSA registration, reporting, recordkeeping, and compliance program requirements, and its compliance intentions are:
 - a. Prior BSA violations and BSA compliance related contacts with the IRS,
 - b. Training programs offered by the business,
 - c. The MSBs formal BSA compliance procedures, and
 - d. Active involvement of management in oversight and internal control activities.
- (4) In situations where knowledge cannot be determined within the scope of selected records, the examiner should expand the period to include recent transactions that occurred after knowledge can be clearly documented. For example, the examiner selected records from January, February, and March. The inspection of these records discloses currency transactions that appear to be structured and which should have been reported. The money services business denied knowledge of the structuring regulations during the initial interview. In April, the examiner informed the money services business about the suspicious transactions and of the structuring regulations. The examiner later expanded the examination period to include May and June transactions. The examiner found violations in May and June. The money services business' knowledge was documented during the notification of the structuring violations and took no action to prevent the recurrence of violations. The money services business' intent to not comply should be documented.
- (5) Because willfulness is a state of mind, generally only circumstantial evidence of willfulness will be available. A willful violation is the intentional violation of a known legal duty.
- (6) IRS does not have the authority to assess penalties under the BSA except for FBAR violations. Significant BSA violations or deficiencies are therefore referred to FinCEN unless a fraud referral is appropriate. The examiner and manager will make a decision regarding whether to refer the case to FinCEN for consideration of civil money penalties. The examiner must thoroughly document all facts on the issue of intent. See IRM 4.26.8, *Special Procedures*, if the case is to be referred to FinCEN.

4.26.9.8.7
(11-12-2019)

Closing the Examination

- (1) Refer to IRM 4.26.6.5.3.10, *Notification of Findings*, for information on notifying the business of examination results.
 - a. If no BSA violations or significant AML program issues have been found, prepare Letter 4029, *Bank Secrecy Act No Change Letter*.
 - b. If BSA violations are found which are technical, minor, infrequent, isolated, or not substantive, a Letter 1112, *Title 31 Violation Notification Letter*, should be issued. See IRM 4.26.8.
 - c. If apparent BSA violations are found which appear to meet the FinCEN referral criteria, prepare a referral on Form 5104, *Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*. See IRM 4.26.8.6, *Form 5104, Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*.
 - d. If the apparent BSA violations appear to meet criminal referral guidelines, the BSA manager will contact the Fraud Technical Advisor to determine if a Form 2797, *Referral Report of Potential Criminal Fraud Cases*, is warranted. (IRM 4.26.8)
- (2) A closing conference must be held at the close of the examination. See IRM 4.26.6.5.3.11, *Holding the Closing Conference*, for additional information.
- (3) When a Letter 1112 is issued, the financial institution is asked to provide a response, amend the AML program, and implement recommendations. Refer to IRM 4.26.6.5.3.12, *Letter 1112 Response*, for additional guidance.
 - a. See IRM 4.26.6.5.3.13, *Delinquent BSA Forms Procedures*, for the process to secure delinquent returns discovered during the examination.
 - b. See IRM 4.26.6.5.3.14, *Case File Closing Procedures*, for procedures when closing the case file.
 - c. See IRM 4.26.6.5.3.16, *Examination Information Report, Form 5346*, for information on preparing and submitting Form 5346, *Examination Information Report*.
 - d. IRM 4.26.6.5.3.17, *Information Items*, provides information on submitting other information items.
 - e. IRM 4.26.6.5.3.18, *Examiner-Filed SARs*, provides procedures for submitting examiner filed SARs.

4.26.9.8.8
(06-01-2006)

Money Laundering Trends

- (1) The financial institution and/or the customer can be involved in potential money laundering schemes. The examiner must focus on both the financial institution and the transactor(s) during the BSA examination.
- (2) Money laundering techniques, which could be used by the financial institution, include:
 - a. Failing to maintain complete records.
 - b. Failing to record specific transactions.
 - c. Failing to obtain the required information to comply with the recordkeeping requirements.
 - d. Failing to file CTRs or SARs on reportable transactions.
 - e. Filing incomplete CTRs or SARs.
 - f. Structuring a transaction by breaking one transaction into several to circumvent the reporting requirements.

- (3) Money laundering techniques which could be used by the customer/transactor include:
 - a. Using multiple locations to conduct transactions.
 - b. Using several individuals at one or more locations to conduct a transaction.
 - c. Using aliases when conducting transactions.
 - d. Conducting numerous transactions at the same location at different times for one day.
- (4) When evidence of a money laundering scheme is uncovered, a referral should be made on Form 5104, *Report Apparent Violation of Financial Recordkeeping and Reporting Regulations*. (IRM 4.26.8)

4.26.9.8.8.1
(11-12-2019)

Examination Techniques

- (1) The following techniques can be useful in uncovering money laundering schemes:
 - a. Review electronic records if available. If not, review transmittal forms to ensure the financial institution is obtaining all the required information and verification, and for indications of fictitious information.
 - b. Review transmittal forms looking for handwriting similarities. If similarities are noted, compare signatures on the forms. (Are different names being used?)
 - c. Review send and receive forms, looking for transactions at nearby locations. It could be an indication of money laundering (for example, paying wire transfer fees to convert cash into a check).
 - d. Review electronic records if available. If not, review transmittal forms looking for similar names and addresses for both senders and recipients.
 - e. Review electronic records if available, if not, transmittal forms for similar phone numbers. (Are different customers using the same phone number?)
 - f. Review all financial services offered to see if customers are structuring transactions by using multiple financial services.

4.26.9.9
(11-12-2019)

Traveler's Checks Overview

- (1) Traveler's checks are issued by national companies such as American Express, AAA, or VISA. There are also privately issued traveler's checks.
- (2) Traveler's checks are negotiable monetary instruments. Individuals usually purchase them when they are traveling on vacations or business trips, instead of carrying cash.
- (3) Sales agents of traveler's checks may sometimes provide other services such as check cashing, wire services, or may operate a business such as a credit union or travel agency.
- (4) An issuer or seller of traveler's checks is one type of financial services provider known as an MSB. Refer to IRM 4.26.5, *Bank Secrecy Act, Bank Secrecy Act History and Law*, for a discussion on MSBs.

4.26.9.9.1
(06-01-2006)

Nationwide Traveler's Checks

- (1) Financial institutions typically sell traveler's checks as agents for national companies. The agent's relationship to the issuer of the traveler's checks is governed by a trust agreement.
- (2) The agent can advertise that it sells the national company's traveler's checks.

- (3) Traveler's checks are drawn on the national company's bank account and the transaction is not complete until the national company receives the face amount from the agent and the traveler's check clears the bank.
- (4) The dollar value of traveler's checks sold by an agent can be limited by the issuing company's trust agreement or by the agent's policy, but in theory they can be in any denomination. Most domestic issuers tend to limit the denominations of traveler's checks sold in U.S. currency to \$100, or at most \$1,000. It should be noted that traveler's checks may be issued in any of several currencies by issuers. When examining agents that issue traveler's checks in foreign currency, one should be aware of current exchange rates to evaluate compliance against BSA reporting and recordkeeping requirements.
- (5) The national company issues and maintains records of traveler's check issuance or sales to agents, as well as records of cashed traveler's checks. The agent maintains sales records of traveler's checks using a sequential numbering system.
- (6) An agent's summary sales report is sent to the national company daily and the correspondent bank sends a clearing report. Using these reports, the national company keeps a record of all traveler's checks sold and cashed. The issuer maintains, and agents are sent, a discrepancy statement for traveler's checks cashed but not reported as sold.
- (7) Money received from the sale of traveler's checks is usually deposited, by the agent, into a separate bank account. Payment is made to the national company by check, wire transfer, electronic mail, or draft.
- (8) National traveler's checks companies either collect their fee up front when the traveler's checks are given to the agents, or have their agents remit the fee together with the face amount of the traveler's checks sold.
- (9) Agents may receive commission statements or reconciliations of traveler's checks sold. The agent's commission can be accounted for this way.
- (10) Although identification of persons purchasing traveler's checks in amounts under \$3,000 is often left to the individual agents, in many instances, the MSB requires identification from the purchaser.
- (11) At a minimum, national companies keep a copy of the front and back of all cashed and canceled traveler's checks.

4.26.9.9.2
(11-12-2019)
Law

- (1) An issuer of traveler's checks is defined as an MSB if traveler's checks are issued in an amount greater than \$1,000 to any person on any day in one or more transactions. (31 CFR 1010.100(ff)(3)(i), *Issuer or seller of traveler's checks or money orders*)
- (2) A seller of traveler's checks is defined as an MSB if traveler's checks are sold in an amount greater than \$1,000 to any person on any day in one or more transactions. (31 CFR 1010.100(ff)(3)(ii))

4.26.9.9.2.1
(11-12-2019)
Reporting Requirements

- (1) FinCEN Form 112, *Currency Transaction Report*, must be filed for all currency transactions of more than \$10,000 in one business day. (31 CFR 1010.311, *Filing obligations*)

- (2) Multiple currency transactions must be aggregated and a CTR is required if the business has knowledge that the multiple transactions are by or on behalf of any person and result in either cash in or cash out totaling more than \$10,000 in one business day. (31 CFR 1010.313, *Aggregation*)
- (3) The CTR must be filed within 15 calendar days following the day the reportable transaction occurs. (31 CFR 1010.306(a)(1), *Filing of reports*)
- (4) FinCEN Form 111, *Suspicious Activity Report*, is required to be made by an MSB if they suspect or have reason to suspect suspicious activities have occurred. (31 CFR 1010.320, *Reports of suspicious transactions*)
- (5) A SAR must be filed for suspicious transactions of at least \$2,000 in funds or other assets conducted or attempted by, at, or through the money services business. (31 CFR 1010.320)
- (6) To the extent that the identification of suspicious transactions required to be reported is derived from a review of clearance records or other similar records of traveler's checks that have been sold or processed, an issuer of traveler's checks shall only be required to report a transaction or pattern of transactions that involves or aggregates funds or other assets of at least \$5,000. (31 CFR 1022.320(a)(3))
- (7) An MSB is required to file the SAR electronically via FinCEN's website no later than 30 calendar days after the date of detection. (31 CFR 1022.320(b)(3))
- (8) An MSB is prohibited from notifying any person involved in the transaction that a SAR has been filed. (31 CFR 1022.320(d))
- (9) FinCEN Form 105, *Currency and Other Monetary Instruments Report*, must be filed by any person who transports, mails, or ships or has someone else transport, mail, or ship currency or monetary instruments in excess of \$10,000 into or out of the country or who receives such items in the United States from abroad. (31 CFR 1010.340, *Reports of transportation of currency or monetary instruments*)

4.26.9.9.2.2
(06-01-2006)
**Registration
Requirements**

- (1) Traveler's check issuers and sellers are required to register by filing a FinCEN Form 107, *Registration of Money Services Business*, and to renew their registration biannually if they are not acting in an agent capacity and are not a branch location. (31 CFR 1022.380, *Registration of money services businesses*)
- (2) Certain events require re-registration which is different from a renewal registration. (31 CFR 1022.380(b)(4), *Events reacquiring re-registration*)

4.26.9.9.2.3
(06-01-2006)
**Recordkeeping
Requirements**

- (1) For records required of all financial institutions, refer to IRM 4.26.5, *Bank Secrecy Act, Bank Secrecy Act History and Law*.
- (2) Copies of all filed CTRs must be retained by the financial institution for five years from the date of the report. (31 CFR 1010.306(a)(2), *Filing of Reports*)
- (3) Copies of all filed SAR and the original or record of any supporting documentation shall be maintained by the financial institution for five years from the date of filing the SAR. (31 CFR 1010.320, *Reports of suspicious transactions*)

- (4) Certain records are required to be maintained for the issuance or sale of traveler's checks involving currency in amounts between \$3,000 and \$10,000, inclusive, by or on behalf of one individual in one business day. The following information must be obtained:
 - a. The purchaser's name and address,
 - b. The purchaser's social security number or alien identification number,
 - c. The purchaser's date of birth,
 - d. The date of purchase,
 - e. The type of instruments purchased,
 - f. The serial numbers of the instruments purchased, and
 - g. The amount in dollars of each instrument purchased. (31 CFR 1010.415(a)(2)(i))
- (5) The financial institution is required to verify the purchaser's name and address and record the specific identifying information (for example, State of issuance and purchaser's driver's license number). (31 CFR 1010.415(a)(2)(ii))
- (6) These records must be retained by the financial institution for five years. (31 CFR 1010.415(c))
- (7) Copy of registration and renewal must be retained for five years, if applicable. (31 CFR 1010.430(d), *Nature of records and retention period*)
- (8) Current annual agent list and agent list(s) for the past five years must be retained, if applicable. (31 CFR 1010.430(d))

4.26.9.9.2.4
(06-01-2006)
**AML Program
Requirements**

- (1) All MSBs must establish and implement a written, risk-based AML program reasonably designed to prevent the business from being used to facilitate money laundering and the financing of terrorism.
- (2) At a minimum, the program shall:
 - a. Incorporate policies, procedures, and internal controls reasonably designed to assure compliance with the BSA and its implementing regulations,
 - b. Designate a compliance officer,
 - c. Provide for education or training of appropriate personnel, and
 - d. Provide for independent review to monitor and maintain the adequacy of the program. (31 CFR 1022.210, *Anti-Money laundering programs for money service businesses*)

4.26.9.9.3
(11-12-2019)
**Records Commonly
Found**

- (1) Traveler's check agents records usually include, but are not limited to:
 - a. Inventory sheets of traveler's checks sold,
 - b. Inventory sheets of traveler's checks received from the issuer,
 - c. Inventory sheets of traveler's checks currently in stock,
 - d. Bank statements and deposit slips,
 - e. Teller drawer reconciliations or summaries, and
 - f. A copy of the executed trust agreement between the agent and the issuer.

4.26.9.9.4
(11-12-2019)
Interview

- (1) Ask specific questions relating to the business, area, and services offered. The examiner must consider all services offered by the business, such as money transmitting, check cashing, and sales of money orders. For example, a customer could attempt to launder \$15,000 by sending a wire transfer for \$8,000 and purchasing \$7,000 in traveler's checks.
- (2) Interview the AML compliance officer and compliance program employees, as well as the officers and employees of the traveler's check issuer or seller to determine their knowledge of the BSA and the financial institution's procedures to comply with the reporting and recordkeeping requirements. The duties and responsibilities of the officers and employees should be documented along with a description of the financial institution's records and an explanation of the flow of transactions through the records. Knowledge is one of the elements needed to prove willfulness with respect to violations of the regulations.
- (3) Ask the owners or management of the financial institution if they have knowledge of any structuring transactions having occurred, or if any suspicious transactions have occurred. This question should be asked again while interviewing employees who have customer contact.
- (4) Interview all individuals who handle currency transactions. Question their knowledge and training of the BSA recordkeeping and reporting requirements.
- (5) Ask open-ended questions throughout the interview. Do not ask questions that require only a yes or no answer.

4.26.9.9.5
(11-12-2019)
Review of the Records

- (1) Any records the financial institution maintains that are relevant to the BSA examination can be requested and reviewed. The examiner will determine if the financial institution is maintaining adequate records and must document any recordkeeping violations.
- (2) Review the written policy statements and procedures of the financial institution as they relate to the BSA.
- (3) Analyze the records of the financial institution for all types of financial services offered. Each type of financial service should be examined separately.
- (4) Determine the traveler's check register completeness by reconciling it to the summary sales reports sent to the issuing company, the discrepancy report from the issuing company, and the bank deposits.
- (5) Trace large block sales or large dollar single transaction sales of traveler's checks in the traveler's check register or close out reports to the records required for recordkeeping, SAR reporting and CTR reporting. Block sales are a group of sequentially numbered traveler's checks sold concurrently for the maximum denomination. The review should identify:
 - a. Blocks of traveler's checks at \$2,000 or right below for SAR reporting,
 - b. Blocks of traveler's checks at \$3,000 to \$10,000, inclusive, for recordkeeping requirements, and
 - c. Blocks of traveler's checks greater than \$10,000 for CTR reporting.
- (6) Inspect any copies of traveler's checks retained by the NBF.
- (7) Request that the NBF obtain copies of traveler's checks from the traveler's check issuer for any questionable or suspicious transactions. It may be

necessary to issue a Title 31 summons to obtain this information. Refer to IRM 4.26.8, *Special Procedures*, before issuing a Title 31 summons.

- (8) Review the NBFIs records to determine if all the required information on the cash purchasers of traveler's check sales involving currency in amounts of \$3,000 to \$10,000, inclusive, has been maintained and verified pursuant to the recordkeeping requirements of 31 CFR 1010.415, *Purchases of bank checks and drafts, cashier's checks, money orders and traveler's checks*.
- (9) It is recommended that a computer database be used when the examination is part of a multiple location local project or there are a large number of block sales or large dollar sales. All transactions exceeding the elected dollar cutoff should be entered in the database, from source documents, to see if the transactions are related.
- (10) Analyze database sorts of the name field and the address field to detect possible structured transactions, unreported transactions, errors, and deficiencies in the financial institution's BSA compliance system.
- (11) The databases, if applicable, of BSA examinations of nearby financial institutions in geographical targeting projects should be consolidated and sorted to detect related structuring activity occurring at more than one location.
- (12) Review copies of CTRs filed by the financial institution to ensure they are accurate and complete. Ensure filed CTRs have been retained by the financial institution for the required five-year period. Use the FCQ database to verify that the CTRs were timely filed and contain the same information as the copies maintained by the financial institution.
- (13) Query the FCQ database for transactions conducted by owners, managers, and employees of the financial institution to detect possible unreported transactions of the financial institution that were instead reported under the individual's name.
- (14) If structured transactions or BSA violations are detected, the examiner should interview the responsible person or employee who conducted the transaction. Based on the answers given, the examiner should consider expanding the scope of the examination. (IRM 4.26.6, *Bank Secrecy Act, Bank Secrecy Act Examiner Responsibilities for BSA Examinations*) All facts should be discussed with the BSA Group Manager.
- (15) Review relevant audit reports or reviews that address BSA policies, procedures, or operations for BSA issues.
- (16) Follow procedures in IRM 4.26.6 to timely conclude the BSA examination.
- (17) Prepare Form 5346, *Examination Information Report*, when information is obtained during the BSA examination that indicates a possible income tax violation warranting referral. (IRM 4.26.6) Keep in mind, however, that the primary purpose of the BSA exam is not to detect Title 26 violations.
- (18) Review copies of filed MSB registration and renewal forms (if applicable) for accuracy and completeness.
- (19) Determine if the business is required to register.

- (20) Review agent list (if applicable) for all required elements.
- (21) Forward agent list to a Centralized Exam (HQ) coordinator.
- (22) Review agent contracts and terms for acceptance and termination as an agent.
- (23) Review all agents rejected or terminated as an agent and forward list to the Centralized Exam (HQ) coordinator.

4.26.9.9.6
(11-12-2019)
**Supporting
Documentation**

- (1) The examiner must obtain adequate supporting documentation for each type of the following violations:
 - a. Reporting – The date of the transaction, the amount, the individuals involved, and a detailed statement regarding the violation, including copies of source documents such as cash in/out slips, control registers, and teller cash proofs which document the violation.
 - b. Recordkeeping – the details of the specific records which were not maintained or were inadequate, including management's response to the violations.
- (2) The MSBs knowledge of BSA requirements must be determined before determining whether violations should be formally referred to FinCEN.
 - a. The key officers and employees should be interviewed again to document the business' response to any apparent violations.
 - b. The existence of an internal compliance program may indicate of knowledge. For example, if knowledge of the reporting and recordkeeping requirements is limited to upper management and the other employees are not similarly educated, the business may be at least negligent (for not properly instructing their employees). The employees need to know what their BSA obligations are. The employees are the initial contact point where the information is obtained. Failure by upper management to ensure that information is correctly gathered may indicate the business' intent not to comply.
- (3) Other factors that may indicate the MSB's knowledge of the BSA registration, reporting, recordkeeping, and compliance program requirements, and its compliance intentions are:
 - a. Prior BSA violations and BSA related contacts with the IRS,
 - b. Training programs offered by the business,
 - c. The MSB's formal BSA compliance procedures, and
 - d. Active involvement of management in oversight and internal control activities.
- (4) In situations where knowledge cannot be determined within the scope of selected records, the examiner should expand the period to include recent transactions that occurred after knowledge can be clearly documented. For example, an examiner initially selects records from January, February, and March. Inspection of these records discloses currency transactions that appear to be structured and which should have been reported. The business denies knowledge of the structuring regulations during the initial interview. In April, the examiner informs the business about suspicious transactions and of the structuring regulations. The examiner then expands the examination period to include May and June transactions. The examiner finds violations in May and June. The business' knowledge was documented during the April notification,

yet it took no action to prevent the recurrence of violations. The business' intentional noncompliance should be documented.

- (5) Because willfulness is a state of mind, generally only circumstantial evidence of willfulness will be available. A willful violation is the intentional violation of a known legal duty.
- (6) Since BSA penalties are assessed by the FinCEN, which does not have any field examiners, the examiner must thoroughly document all facts on the issue of willfulness. After the examiner secures the necessary information and documents the apparent violations, the examiner should follow the procedures detailed in IRM 4.26.8.

4.26.9.9.7
(11-12-2019)

Closing the Examination

- (1) After documenting the potential violations, the examiner should provide a list of the violations to the MSB and solicit a written explanation for each of the violations identified. The list should include:
 - a. Date of the transaction,
 - b. Customer name,
 - c. Account number (if any),
 - d. Serial number of the traveler's check(s) involved,
 - e. Amount of the currency transaction(s), and
 - f. Description of the transaction(s).
- (2) The examiner should advise the MSB of any recordkeeping deficiencies as well as any deficiencies in their policies, procedures, internal controls, and compliance programs that might result in noncompliance with the BSA.
- (3) Any additional documents or information provided by the MSB in response should be reviewed and a determination should be made as to whether any items should be removed from the list of violations.
- (4) When the MSB contends that a CTR was filed and provides its retained copy as evidence, the examiner should query the FCQ database and conduct an exhaustive search before concluding that a CTR was not received. In conducting the search, the examiner should query all customer numerical identification on the CTR such as account number (if applicable), SSN, and identification credential number.
- (5) Refer to IRC 4.26.6, *Bank Secrecy Act Examiner Responsibilities for BSA Examinations*, for complete closing procedures.

4.26.9.9.8
(06-01-2006)

Money Laundering Trends

- (1) The financial institution and/or the customer can be involved in potential money laundering schemes. The examiner must focus on both the financial institution and the transactor(s) during the BSA examination.
- (2) Money laundering techniques, which could be used by the financial institution, include:
 - a. Failing to maintain complete records.
 - b. Failing to record specific transactions.
 - c. Failing to obtain the required information to comply with the recordkeeping requirements.
 - d. Failing to file CTRs, SARs, or CMIRs on reportable transactions.

- e. Structuring a transaction by breaking one transaction into several to circumvent the reporting requirements.
- (3) Money laundering techniques which could be used by the customer/transactor include:
 - a. Using multiple locations to conduct transactions.
 - b. Using several individuals at one or more locations to conduct a transaction.
 - c. Using aliases when conducting transactions.
 - d. Conducting several transactions at the same location at different times for one day.
- (4) When evidence of a money laundering scheme is uncovered, a referral should be made on Form 5104, *Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*. See IRM 4.26.8 for referral procedures.

4.26.9.9.8.1
(06-01-2006)

Examination Techniques

- (1) The following techniques can be useful in uncovering money laundering schemes:
 - a. Review the financial institution's sales logs, inventory sheets, and /or daily summaries for block purchases. Trace these purchases to records of sales of \$3,000 or more.
 - b. Request copies of traveler's checks from the issuer, if necessary, to determine if transactions have been structured.
 - c. Conduct BSA examinations of financial institutions within the same geographical area.
 - d. Create a database to consolidate transactions of the financial institutions, which can be sorted to identify related transactions.

4.26.9.10
(11-12-2019)

Precious Metals, Precious Stones, or Jewels (PMSJ) Overview

- (1) FinCEN issued regulations at 31 CFR Part 1027, *Rules for Dealers in Precious Metals, Precious Stones, Jewels*, in June 2005 requiring dealers to establish and implement an anti-money laundering compliance program. The regulations were effective as of July 11, 2005, with an implementation deadline of January 1, 2006.
- (2) FinCEN issued 31 CFR Part 1027 to better protect those who deal in precious metals, precious stones, or jewels (PMSJ) from potential abuse by criminals and terrorists, thereby enhancing the protection of the U.S. financial system generally and the (PMSJ) industry. The characteristics of PMSJs that make them valuable also make them potentially vulnerable to those seeking to launder money.
- (3) PMSJs are sold by both retailers and wholesalers.
 - a. A retail sale is any sale made in the course of a trade or business, if that trade or business principally consists of making sales to ultimate consumers. See IRM 4.26.12.9, *Other Retail Overview*, for requirements under Title 26.
 - b. Wholesalers sell products to other wholesalers and retailers. Wholesale transactions of PMSJs may involve large amounts of cash. See IRM 4.26.12.11, *Wholesale Distributor Overview*, for requirements under Title 26.

4.26.9.10.1
(11-12-2019)
Terminology

- (1) 31 CFR 1027.100, *Definitions*, contains a complete listing of key terms that relate to the dealer industry. Understanding these terms will help understand the regulation and the PMSJ industry.
- (2) Terms commonly used in this industry include:
 - a. Assay - Testing a metal or ore to determine its ingredients and quality.
 - b. Bid - Amount offered to purchase.
 - c. Bourses - Traditional trading floors where diamonds are safely bought and sold.
 - d. Bullion - Precious metal in the form of bars or ingots.
 - e. Customer cards - Record of customer purchases or account receivable cards.
 - f. Gold doré (pronounced gold doh-rey) is a bar of semi-purified gold (such as bullion). After being mined, the first stage in the purification process of the gold ore produces a cast bar (gold dore) that is approximately 90% gold. The other 10% is mostly metals like silver and copper.
 - g. Pawn Ticket - Record of stock held for customer retrieval by a specific date in exchange for cash.
 - h. Public Auction - Can draw large cash transactions depending on items presented.
 - i. Selling goods on memo - A consignment agreement that provides possession of the product to a potential buyer and payment is due only when the deal is struck.
 - j. Shot - Small pellets of gold.

4.26.9.10.2
(11-12-2019)
Definition of a Dealer

- (1) A dealer is defined in 31 CFR 1027.100(b), *Dealer*, as a:
 - a. Person engaged in the United States as a business in the purchase and sale of covered goods and finished goods deriving 50% or more of their value from Precious Metals, Precious Stones or Jewels (PMSJ), and who during the prior calendar or tax year purchased more than \$50,000 in covered goods **and** sold more than \$50,000 in covered goods,
 - b. Wholesaler, and
 - c. Retailer in certain circumstances.
- (2) There are exceptions to the law that determine if a person is a dealer. There are factors to consider, early in the examination, to ensure the entity is in fact a dealer and subject to the requirements of the BSA. Per 31 CFR 1027.100(b)(2) the term dealer does **not** include:
 - a. A retailer, unless the retailer, during the prior calendar or tax year, purchased more than \$50,000 in covered goods from persons other than dealers or other retailers such as members of the general public or foreign sources of supply.
 - b. A foreign person who ships products into the U.S. without any further business activity or attends a trade show at which it does not purchase and sell covered goods above the \$50,000 threshold amounts.
 - c. A business that purchases PMSJ for use in machinery or equipment to be used for industrial purposes and sells it for industrial purposes.

Note: FinCEN determined that the purchase of PMSJ for use in industrial products, and the purchase or sale of such products, appears to be less susceptible to money laundering and terrorist financing risks,

because precious metals, precious stones, or jewels typically do not constitute a significant component of the value of an industrial product. Therefore, persons who engage in these activities are not dealers to the extent of such activities for purposes of the regulations at 31 CFR Part 1027, *Rules For Dealers In Precious Metals, Precious Stones, Or Jewels*.

- d. A person licensed or authorized under the laws of any state (or political subdivision thereof) to conduct business as a pawnbroker, but only to the extent that such person is engaged in pawn transactions including the sale of pawn loan collateral.

(3) In determining if the \$50,000 threshold has been met:

- a. The \$50,000 threshold is calculated based on the value of the precious metals, precious stones, or jewels contained in the jewelry, not on the overall value of the jewelry. This distinction ensures that the focus of the regulations remains on precious metals, precious stones, or jewels, not on value due to other reasons.
- b. Trade-ins are not considered purchases for defining who is a dealer so long as the value of the trade-in is credited to the account and so long as the business does not provide funds to the customer in exchange for the trade-in.

4.26.9.10.2.1
(11-12-2019)

Retailer Exception

- (1) FinCEN has defined the term retailer as a person engaged in the United States as a business in sales of covered goods, primarily to the public. FinCEN believes that retailers as defined do not pose the same level of risk for money laundering as wholesale dealers. Because of this, most retailers will not be required to establish AML programs. However, because some will, an examiner must determine at the onset of an examination whether a retailer is required to have an AML program.
- (2) Retailers are exempt from the BSA requirement to have an AML program if they purchase less than \$50,000 in covered goods from the public or foreign supplier.
- (3) If a retailer purchases more than \$50,000 in covered goods from the public or foreign supplier, the retailer is a dealer under the BSA and must have an AML program.
- (4) If a retailer purchases covered goods from non-dealers and the purchases total more than \$50,000, then only their purchases will be addressed to determine if they are required to have an AML program on those purchases from non-dealers. For example, a retail jeweler who sometimes buys jewelry from the general public or foreign sources of supply and re-sells it in his store would be required to establish an AML program if, during the prior calendar or tax year:
 - a. He sold jewelry containing more than \$50,000 in precious metals, precious stones, or jewels (PMSJ) and the value of the PMSJs comprised 50 percent or more of the value of the jewelry; **and**
 - b. He purchased from the public or foreign sources of supply jewelry containing more than \$50,000 in PMSJs, and the value of the PMSJs comprised 50 percent or more of the purchase price of the jewelry.
 - c. The retailer would be required to have an AML program that would only need to address the risks associated with purchases from the public or

foreign sources of supply of jewelry that derives 50 percent or more of its value from PMSJs. It would not need to address the sale of covered goods.

- (5) Retailers who conduct more wholesale activities, such as sales to other dealers, than retail activities are not considered retailers under this regulation and the retailer exception does not apply.

4.26.9.10.2.2 (11-12-2019) **Pawnbrokers**

- (1) FinCEN's position is that a person licensed or authorized under the laws of any State or political subdivision to conduct business as a pawn broker does not pose the same level of risk for money laundering as dealers only to the extent such person is engaged in pawn transactions, including the sale of pawn loan collateral. If a pawnshop has other business activities, it may be a dealer for those transactions.
- (2) Businesses licensed or registered as pawnbrokers under state or municipal law are specifically exempted from the definition of "dealer" for purposes of the regulations at 31 CFR 1027.100, *Definitions*. Therefore, pawnbrokers are not required to establish AML programs under the regulations at 31 CFR 1027.100 if they are properly licensed or registered with the appropriate state or local government and engaged in pawn transactions only.

4.26.9.10.3 (11-12-2019) **Covered Goods**

- (1) Only the products listed in 31 CFR 1027.100, *Definitions*, are deemed to be covered goods and therefore the BSA requirements apply only to the purchase and sale of covered goods.
- (2) Covered goods include finished goods, jewels, precious metals, and precious stones. The items included in covered goods are defined further to mean:
 - a. Finished goods includes (but not limited to) jewelry, numismatic items, and antiques that derive 50 percent or more of their value from jewels, precious metals, or precious stones contained in or attached to the finished goods.
 - b. Jewel means an organic substance with gem quality market-recognized beauty, rarity, and value. Jewels include only pearl, amber, and coral.
 - c. Precious metals are gold, iridium, osmium, palladium, platinum, rhodium, ruthenium, or silver having a level of purity of 500 or more parts per thousand; and an alloy containing 500 or more parts per thousand, in the aggregate, of two or more of the metals listed above.

Note: FinCEN Ruling 2006-1 – Anti-Money Laundering Programs for Dealers in Silver dated December 30, 2005 states that purchases and sales of silver are excluded from the BSA requirements. <https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/anti-money-laundering-programs-dealers-silver>.

Note: See also Definition of Precious Metals in the Interim Final Rule Requiring Anti-Money Laundering Programs for Dealers in Precious Metals, Stones, or Jewels dated 06/08/2012 at <https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/definition-precious-metals-interim-final-rule>.

- d. Precious stones are substances with gem quality market-recognized beauty, rarity, and value. Includes diamond, corundum (including rubies

and sapphires), beryl (including emeralds and aquamarines), chrysoberyl, spinel, topaz, zircon, tourmaline, garnet, crystalline and cryptocrystalline quartz, olivine peridot, tanzanite, jadeite jade, nephrite jade, spodumene, feldspar, turquoise, lapis lazuli, and opal.

4.26.9.10.4
(11-12-2019)
Law

- (1) Dealers are required to file Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business under Title 26 and Title 31*.
- (2) In addition, dealers must create and maintain an AML program as required by 31 CFR 1027.210, *Anti-money laundering for dealers in precious metals, precious stones, or jewels*.
- (3) Dealers are not MSBs and are not required to register with FinCEN as such.
- (4) Dealers are not required to file SARs but are encouraged to do so. An integral part of a dealer's AML program is an assessment of the risks and vulnerabilities of the business and the development of policies, procedures and internal controls to address those risks. This should include procedures and controls for identifying suspicious activities and dealing with them accordingly. Procedures for dealing with suspicious activities may include guidance for when it is appropriate in the context of the business and the activity to:
 - a. Contact local or federal law enforcement authorities.
 - b. Voluntarily file a suspicious activity report.
 - c. Check the suspicious activity box on a Form 8300 filed voluntarily on a transaction.
 - d. Report suspected terrorist activities to FinCEN using its Financial Institutions Hotline (1-866-556-3974).
- (5) Dealers are required to file FinCEN Form 114, *Report of Foreign Bank and Financial Accounts (FBAR)*.
- (6) Dealers must also file FinCEN Form 105, *Report of International Transportation of Currency or Monetary Instruments (CMIR)*.
 - a. FinCEN Form 105 must be filed with the customs officer in charge at any port of entry or departure.
 - b. If an examiner determines that a dealer failed to file FinCEN Form 105 or meet the CMIR requirements, the examiner must make a referral to Customs through the BSA Policy Liaison to FinCEN.

4.26.9.10.4.1
(11-12-2019)
Form 8300 Filing Requirement

- (1) For a detailed explanation of Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, under Title 26 and Title 31, see IRM 4.26.10, *Form 8300 History and Law*, and IRM 4.26.11, *BSA Examiner Responsibilities for Form 8300 Examinations*.
- (2) Dealers must file Form 8300 they receive cash of more than \$10,000 in one transaction or two or more related transactions under as required under IRC 6050I, *Returns relating to cash received in trade or business*, and 31 USC 5331, *Reports relating to coins and currency received in nonfinancial trade or business*. Under this dual reporting regime, the business is only required to file one Form 8300 for a transaction subject to both IRC 6050I and 31 USC 5331.
 - a. 31 USC 5331 copies IRC 6050I with some exceptions such as the customer notification requirement. The regulations governing the filing of Form 8300 under 31 USC 5331 appear at 31 CFR 1010.330, *Reports*

relating to currency in excess of \$10,000 received in a trade or business, and for PMSJ dealers at 31 CFR 1027.330, Reports relating to currency in excess of \$10,000 received in a trade or business.

- (3) Reporting certain monetary instruments as cash on Form 8300 depends on whether the dealer in PMSJ is a retailer or a wholesaler.
 - a. Retailers are required to report receipts of cash equivalents as cash. PMSJ sales are included in the definition of a “designated reporting transaction” under the definition of “collectibles”, which includes “any metal or gem”.
 - b. Wholesalers are not required to report receipts of cash equivalents as cash unless the wholesaler knows, or has reason to know, that they are being used to evade the reporting of the transaction.
- (4) Dealers can report suspicious activity by checking the “Suspicious” box on Form 8300. Checking the “Suspicious” box is voluntary. Dealers are not required to file SARs but may voluntarily file one.
- (5) Under IRC 6050I any business filing a required Form 8300 must also furnish a written statement to each person identified on the Form 8300 by January 31 of the succeeding calendar year. This is not a requirement of 31 USC 5331 and **must not** be discussed during the Title 31 examination.

4.26.9.10.4.2
(11-12-2019)
AML Program

- (1) Dealers are required to have an AML program in place no later than six months after becoming a dealer.
- (2) If during the prior tax or calendar year a retailer both purchased more than \$50,000 of covered goods from persons other than U.S. dealers or retailers, such as foreign sources and members of the public, and sold more than \$50,000 of covered goods, that retailer would be considered a dealer and would have to develop and implement an AML program. However, under such circumstances the AML program would only be required to address purchases from foreign sources and members of the public; the program would not be required to address sales.
- (3) A dealer is required to develop and implement a written AML program reasonably designed to prevent the dealer from being used to facilitate money laundering or the financing of terrorist activities through the purchase and sale of covered goods.
- (4) The AML program must be based on a risk assessment. Guidance in determining risk is available on the FinCEN web site. For example, see Guidance (Frequently Asked Questions) - *Interim Final Rule on Anti-Money Laundering Programs for Dealers in Precious Metals, Stones, or Jewels* (06/03/2005).
- (5) At a minimum, the AML program must include:
 - a. Policies, procedures, and internal -- 31 CFR 1027.210(b)(1), *Anti-money laundering program requirements*.
 - b. Designation of a compliance officer -- 31 CFR 1027.210(b)(2), *Minimum requirements*.
 - c. Ongoing training of appropriate persons concerning their responsibilities under the program - 31 CFR 1027.210(b)(3).

- d. Independent testing to monitor and maintain an adequate program - 31 CFR 1027.210(b)(4).

4.26.9.10.4.2.1
(11-12-2019)

**Policies, Procedures,
and Internal Controls**

- (1) A dealer's AML program must incorporate policies, procedures, and internal controls based upon the dealer's assessment of the money laundering and terrorist financing risks associated with its line(s) of business.
- (2) The program must include policies, procedures, and internal controls to assist the dealer in identifying transactions that may involve use of the dealer to facilitate money laundering or terrorist financing. The AML program must include provisions for making reasonable inquiries to determine whether a transaction involves money laundering or terrorist financing, and for refusing to consummate, withdrawing from, or terminating such transactions.
- (3) A dealer's AML program should include internal procedures that:
 - a. Ensure regulatory record keeping and reporting requirements are met, and changes in regulatory requirements are incorporated.
 - b. Implement risk-based counterparty due diligence procedures.
 - c. Provide adequate controls for higher risk counterparties, transactions and products.
 - d. Enable the timely identification of reportable transactions and ensure accurate and timely filing of a required Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*.
 - e. Provide for adequate monitoring.
 - f. Provide for adequate supervision of employees.
 - g. Provide for appropriate and updated training.

4.26.9.10.4.2.2
(11-12-2019)

Compliance Officer

- (1) The dealer must designate a compliance officer responsible for administering the AML program. The person should be competent and knowledgeable regarding BSA requirements, money laundering issues and risks, and the precious metals, precious stones, or jewelry industry.
- (2) The compliance officer must ensure that:
 - a. The program is properly implemented.
 - b. The program is updated as necessary to reflect changes in the risk assessment, current requirements, and further guidance issued by the Department of the Treasury.
 - c. The appropriate personnel are trained as necessary.

4.26.9.10.4.2.3
(11-12-2019)

Training

- (1) The dealer must ensure that the employees are trained about their responsibilities under the AML program. Employees should be trained to recognize possible signs of money laundering and terrorist financing.
- (2) Training should be ongoing and should be based on the employee's responsibilities, any revisions to the law, and the activities of the dealer.
- (3) Training can be conducted by internal or external parties and can include videos, computer-based training, and booklets.
- (4) The level, frequency, and focus of the training should be determined by the responsibilities of the employees and to the extent their functions bring them in contact with the BSA requirements or possible money laundering activities.

4.26.9.10.4.2.4
(11-12-2019)

Independent Testing

- (1) Independent testing is required to be conducted to ensure the AML program is adequate. It must be conducted periodically, based on the risks of the dealer's operations and should be conducted by personnel who are knowledgeable regarding BSA requirements.
- (2) The testing does not need to be performed by an external party. It may be conducted by an employee, but it must be objective. Independent testing cannot be conducted by the dealer's compliance officer, anyone who reports to the compliance officer, or by a person involved in the operations of the AML program.
- (3) There are no specific guidelines for independent testing; however, the scope of the independent testing should be sufficient to test the adequacy and effectiveness of the dealer's AML program, including appropriate transaction testing. This may include but is not limited to:
 - a. Verifying that management has adopted and approved an AML program, conducted employee training, and appointed a compliance officer.
 - b. Ensuring that the AML program includes the appropriate elements such as internal controls to ensure ongoing compliance, risk assessment guidance, designation of a compliance officer, employee training, and independent testing.
 - c. Interviewing senior management to determine their commitment to and understanding of the program.
 - d. Interviewing the compliance officer to assess his or her understanding of the law, the regulations, and the management of the AML program.
 - e. Reviewing due diligence procedures for new suppliers, including verification of identification and assessing the risks of foreign suppliers.
 - f. Determining whether records of suppliers and customers have been compared against various terrorist lists and how frequently.
 - g. Evaluating training materials to determine appropriateness. Are records being kept on training sessions and participation? Are the appropriate employees receiving training? What is the frequency of training?
 - h. Determining whether a Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, was required and have been filed. Are appropriate records of these forms being kept?
 - i. Examining a sample of transactions to determine whether their procedures, policies, and internal controls are adequate to identify transactions that might involve them being used to facilitate money laundering or terrorist financing. This would include the dealer having reasonably performed inquiries on transactions that might be suspicious and either refusing, withdrawing from the transaction, or terminating the transaction.

4.26.9.10.4.2.5
(11-12-2019)

AML Program for Foreign Dealers

- (1) The AML program requirement applies only to a person in the United States engaged as a business in the purchase and sale of covered goods. This would include a person with a U.S. office, a person who comes to the United States to make purchases and sales of covered goods above the threshold amount, and a foreign-located person who maintains sales staff engaged in such purchases and sales within the United States.
- (2) The AML program requirement does not apply to a foreign dealer who ships products into the United States without conducting further business activity

within the United States, or a foreign dealer that merely advertises in the United States or attends a trade-show in the United States at which it does not purchase and sell covered goods above the threshold amounts.

4.26.9.10.5
(11-12-2019)
Risk Assessment

- (1) Precious metals, precious stones, or jewels are easily transportable, highly concentrated forms of wealth, easily converted to cash. As such, they are highly attractive to money launderers and other criminals, including those involved in the financing of terrorism and narcotics.
- (2) The purpose of a risk assessment is to determine the major risks, so a dealer can develop a risk-based AML program to mitigate those risks.
- (3) Dealers should:
 - a. Assess the money laundering and terrorist financing risks associated with its products, including the nature of the dealer's customers, suppliers, distribution channels, geographic locations, and operations.
 - b. Take into consideration the extent in which the dealer engages in transactions other than with established customers, established suppliers, and third parties subject the BSA regulations.
 - c. Analyze the extent to which it engages in transactions for which payment or account reconciliation is routed to or from jurisdictions that have been identified as a sponsor of international terrorism, non-cooperative with international anti-money laundering principles, or vulnerable to money laundering.
- (4) Dealers are expected to implement their AML programs on a risk-assessed basis. This means considering all the relevant factors to make a risk assessment, including but not limited to:
 - a. The extent to which the business engages in transactions other than with established customers or sources of supply or other dealers subject to BSA requirements.
 - b. The extent to which the business engages in transactions for which payment or account reconciliation is routed to or from accounts located in jurisdictions that have been identified as vulnerable to terrorism or money laundering.
 - c. Indicators that a transaction may involve money laundering or terrorist financing. Take reasonable steps to determine whether its suspicions are justified and respond accordingly, including refusing to enter into, or complete, a transaction that appears designed to further illegal activity.
 - d. Procedures for making reasonable inquiries. For example, it may be appropriately determined that reasonable inquiry with respect to a transaction conducted by a new customer or supplier involves considerable scrutiny, including verification of customer identity, income source, or the purpose of a transaction. In contrast, reasonable inquiry with respect to an established customer may not involve additional steps beyond those normally required to complete the transaction, unless the transaction appears suspicious or unusual.

4.26.9.10.5.1
(11-12-2019)
Product Risk

- (1) The level of risk varies depending on the value of the product. Unless transactions involve very large quantities, lower value products are likely to carry less risk than higher value products. Values can be volatile dependent upon supply and demand. Relative values of some materials can vary between different countries, and over time.

4.26.9.10.5.2
(11-12-2019)
**Customer and
Counterparty Risk**

- (2) The physical characteristics of the products offered are also a factor to consider. Products that are easily portable and which are unlikely to draw the attention of law enforcement are at greater risk of being used in cross border money laundering. For example, diamonds are small, light in weight, and not detected by metal detectors. A very large value is easily concealed.
 - (3) The risk of dealing in stolen or fraudulent products must also be considered.
- (1) A customer can be a retail customer or a supplier from whom the dealer buys covered goods. A customer can also be someone to whom the dealer sells covered goods such as a refiner.
 - (2) Generally, retail customers will not have a business purpose for a jewelry purchase. They are most likely buying for personal reasons that cannot be factored into an anti-money laundering risk assessment. However, higher risk may be seen in certain retail customer transaction methods such as:
 - a. Use of cash. It should be noted that for personal reasons having no connection to money laundering or terrorist financing, many persons desire total anonymity or at least the absence of paper records in jewelry purchases.
 - b. Payment by or delivery to third parties. However, not all third-party payments are indicative of money laundering. For example, it's not unusual for Person A to select a piece of jewelry for himself or herself which is then paid for and delivered by Person B as a gift to A.
 - c. Structuring.
 - (3) Dealers may buy from or sell to other counterparties who also work in the precious metals, precious stones, or jewels industry. Apart from the retail sector, trade in precious stones, precious metals, and jewels is traditionally private, as a matter of commercial protection or security. Dealers have traditionally protected their counterparties, their materials, and their business practices from public knowledge, in the interest of protecting themselves from criminal activity and from potential independent interaction by competitors with their customers, counterparties, or suppliers.
 - (4) Higher risk business suppliers or counterparties include a person who:
 - a. Does not understand the industry in which he proposes to deal, or does not have a place of business, equipment, or finances necessary and appropriate for such engagement, or does not seem to know usual financial terms and conditions.
 - b. Proposes a transaction that makes no sense or that is excessive, given the amount, quality, or potential profit.
 - c. Has significant and unexplained geographic distance from the PMSJ dealer.
 - d. Uses banks that do not specialize in or do not regularly provide services in such areas and are not associated in any way with the location of the counterparty and the products.
 - e. Makes frequent and unexplained changes in bank accounts, especially among banks in other countries.
 - f. Involves third parties in transactions, either as payers or recipients of payment or product, without apparent legitimate business purpose

- g. Will not identify beneficial owners or controlling interests, where this would be commercially expected.
- h. Seeks anonymity by conducting ordinary business through accountants, lawyers, or other intermediaries.
- i. Uses cash in its transactions with the dealer or with his own counterparties in a nonstandard manner.
- j. Uses money services businesses or other non-bank financial institutions for no apparent legitimate business purpose.
- k. Is a politically exposed person (PEP).

Note: PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves.

- (5) FinCEN expects persons engaged in the business of buying and selling covered goods to take reasonable steps to determine whether a supplier is covered by regulations at 31 CFR Part 1027, *Rules for dealers in precious metals, precious stones, or jewels*, or whether the supplier is eligible for the retailer exemption. Suppliers not subject to the regulations or eligible for the retail exemption would raise a red flag.
- (6) Risks associated with dealing with foreign suppliers are different from those associated with domestic suppliers. See FinCEN's *Guidance for Dealers, Including Certain Retailers, of Precious Metals, Precious Stones, or Jewels, on Conducting a Risk Assessment of Their Foreign Suppliers* (03/10/2008).

4.26.9.10.5.3 (11-12-2019)

Geographic Risk

- (1) Geographic risk factors include:
 - a. Where a product is mined, refined, or finished.
 - b. Location of a seller.
 - c. Location of a purchaser.
 - d. Location of the delivery of a product.
 - e. Location of funds being used in the transaction.
- (2) The following factors should be considered to determine if a country may or may not pose a high-risk regarding precious metals, precious stones, or jewels.
 - a. Whether there is known mining or substantial trading of the precious metals, precious stones, or jewels in that country.
 - b. Whether a country would be an anticipated source of large stocks of precious metals, precious stones, or jewels based upon national wealth, trading practices, and culture, or unanticipated (large amounts of old gold jewelry in poor developing countries). It should be recognized, however, that gold and silver have cultural and economic significance in many developing countries and very poor people may have, buy, and sell these metals.
 - c. The level of government oversight of business and labor in mining and/or trading areas.
 - d. The extent to which cash is used in a country.
 - e. The level of regulation of the activity in a country.

- f. Whether informal banking systems operate in a country. For example, informal value transfer systems such as hawalas operate in many developing countries.
- g. Whether designated terrorist organizations or criminal organizations operate within a country, especially in small and artisan mining areas.
- h. Whether there is ready access from a country to nearby competitive markets or processing operations. For instance, gold mined in Africa is more frequently refined in South Africa, the Middle East, or Europe rather than in the United States and a proposal to refine African gold in the United States would be unusual and higher risk.
- i. Whether appropriate AML/counter financing of terrorism laws, regulations, and other measures are applied and enforced in a country.
- j. The level of enforcement of laws addressing corruption or other significant organized criminal activity.
- k. Whether sanctions, embargoes, or similar measures have been directed against a country.

4.26.9.10.5.4
(11-12-2019)
Operational Risk

- (1) Operational risk is the risk that a business will fail to detect or prevent money laundering or terrorist financing as a result of inadequate internal processes or systems, or as a result of human failure. Assessment of operational risk includes:
 - a. Systems used to process transactions.
 - b. Frequency of employee turnover.
 - c. The recordkeeping system utilized by the company.
 - d. Business structure and business plan.
 - e. Involvement of senior management in BSA matters.
 - f. The company's relationship with its customers and suppliers.

4.26.9.10.5.5
(11-12-2019)
Monitoring Risk

- (1) The degree and nature of monitoring by a dealer will depend upon the risk assessment that the dealer has made.
- (2) Additional monitoring should be given to higher risk transactions and counterparties, and less monitoring given to transactions and counterparties that are below certain thresholds or criteria.
- (3) A risk may only become evident when a counterparty begins transactions, particularly if the transactions differ from those originally anticipated. The dealer should note and evaluate these changes in transactions.
- (4) The dealer should document its monitoring program and results of monitoring as well as periodically assess its monitoring program for adequacy.

4.26.9.10.6
(11-12-2019)
Records Commonly Found

- (1) Records most commonly found include:
 - a. Assay reports
 - b. Bank statements
 - c. Cash receipts journal
 - d. Cash register tape
 - e. Customer cards
 - f. Customer files
 - g. Customer invoices and receipts
 - h. Duplicate deposit slips

- i. Installment records
- j. Inventory control sheets
- k. Lay-away records
- l. Purchase order receipts
- m. Professional appraisals
- n. Sales journal
- o. Sales receipts

4.26.9.10.7
(11-12-2019)

Title 31 or Title 26 Exam

- (1) Examinations of dealers in precious metals, precious stones, or jewels should be started under Title 31 because they have an AML program requirement under Title 31 and Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, filing requirements under both Titles 26 and 31. This allows the examination to cover the determination of whether their AML program is adequate and to examine compliance with the Form 8300 filing requirements.
- (2) For example, IRS is conducting a Title 31 examination of a dealer that is required to have an AML program under 31 CFR 1027.210, *Anti-money laundering program for dealers in precious metals, precious stones, or jewels*. During the examination of the AML compliance program, the examiner identifies delinquent Form 8300 because of an inadequate AML program or a failure to implement the AML program. The failure to timely file a complete and correct Form 8300 is a violation of 31 CFR 1027.330, *Reports relating to currency in excess of \$10,000 received in a trade or business*. It is also a violation of 26 CFR 60501-1, *Returns relating to cash in excess of \$10,000 received in a trade or business*.
- (3) There is no prohibition against using information acquired in a Title 31 exam in a Title 26 exam.
- (4) When a dealer has a requirement under Title 31 for an AML compliance program and under Titles 26 and 31 to file a Form 8300, the BSA examiner must notify the entity up-front that it is subject to both Title 26 and Title 31 and the examination can cover both sections of the law.
- (5) The current Form 8300 Lead Sheet is designed so it can be used to determine compliance with Form 8300 requirements under either section of the law. The examination steps to determine an entity's compliance with the Form 8300 requirements remain the same no matter under which section of the law the examination is conducted.
- (6) There is no examination step that requires an examiner to review tax return information or IDRS to determine Form 8300 compliance. It is only at the conclusion of the Form 8300 examination, when processing the penalty case file under Title 26 that ERCS and IDRS need to be accessed.
- (7) If a Form 8300 Title 26 dealer case is received in the field and the BSA manager and examiner, prior to contacting the entity, concur that the examination should be initiated using Title 31 procedures, the case may be surveyed.
 - a. Survey the Form 8300 IRC 60501 case and return it to BSA Enterprise Computing Center.
 - b. A copy of the 1900 will be sent to the BSA ECS manager, who will forward the information to the BSA ECS Coordinator for evaluation. BSA ECS will record the survey. It will then evaluate the entity for a Title 31 examination using only sources available for Title 31 cases. BSA ECS

will select the case for Title 31 examination based on this evaluation only. If appropriate, BSA ECS will then assign the case as a Title 31 examination. If possible, the case should be assigned to a group different from the surveying group.

- c. If possible the BSA group manager should assign the Title 31 case file to an examiner different from the examiner involved in the surveyed case.
 - d. If it is impossible to reassign, the BSA examiner should wait a minimum of 30 days before contacting the entity so that there is a separation as complete as possible from the Title 26 case information.
- (8) The disclosure laws under IRC 6103, *Confidentiality and disclosure of returns and return information*, apply throughout the entire Title 26 examination process.
- a. If a Form 8300 examination is started under Title 26, the disclosure regulations under IRC 6103 apply and the information cannot be used in a Title 31 exam without securing a related statute determination. The examiner must secure a related statute determination, signed by the Territory Manager, prior to addressing any Title 31 issues.
 - b. For example, a retail jeweler is assigned for a Form 8300 examination under Title 26. During the examination, the examiner determines that the retailer, during the prior calendar or tax year, purchased more than \$50,000 in precious items from persons other than dealers or other retailers (such as members of the general public or foreign sources of supply). Because the examination has already been started, it is not possible to survey the Title 26 case. The Title 31 information can only be used if a related statute determination is made. See IRM 4.26.14, *Disclosure*, for the procedures for a related statute determination.
 - c. If an examination is opened under Title 26, the examiner cannot ask the entity any questions related to the BSA such as questions about their AML compliance program.

4.26.9.10.8
(11-12-2019)
**Title 31 Examination
Procedures**

- (1) An effective risk-based BSA examination consists of the following phases:
- a. Pre-Plan
 - b. Setting the scope and depth of the examination
 - c. Interview - On site visit to the dealer, walk through of the business, and interview of the appropriate personnel
 - d. Evaluation of the AML program to determine if it has been implemented and is effective
 - e. Examination of the books and records
 - f. Transaction testing
 - g. Developing conclusions and finalizing the examination
- (2) The techniques described in this section are intended as a guide and are not all-inclusive.
- (3) The Title 31 Lead Sheet Package and the Form 8300 Lead Sheet Package are available on the BSA SharePoint and should be used to guide the administrative aspects of the examination.

- (4) A dealer's AML program must be commensurate with their level of risk. The dealers should not necessarily take any single indicator as evidence of lower or higher risk. The risk assessment process should weigh several risk factors including:

- a. Geographic locations
- b. Customers
- c. Counterparties
- d. Suppliers
- e. Product
- f. Services
- g. Operational risk

4.26.9.10.8.1
(11-12-2019)
Pre-Plan

- (1) Prior to a Title 31 examination the examiner must:
- a. Review the FCQ system for any Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, filing, filed by the entity, and CTRs and SARs filed on the entity, its owners, and employees.
 - b. Review prior Title 31 examination results.
 - c. Check for previous Title 31 penalties.
- (2) The examiner must use the Lead Sheet packages for Title 31 and Form 8300 and the Primary Case Folder required records. These are available on the BSA SharePoint.
- a. Set up Form 4318, *Examination Workpapers Index*.
 - b. Begin the Form 9984, *Activity Record of Examining Officer*.
 - c. Set up Workpapers 105 – 125 from Planning to Close through GM Concurrence.
- (3) The examiner should become familiar with the common practices of the industry. Some useful associations are:
- a. The Jewelers Board of Trade provides a list of links to trade associations and organizations related to jewelers for terms and typical business organization. Listings include businesses with wide membership, such as the World Gold Council, as well as more local organizations, such as the New York Diamond Dealers Club.
 - b. The International Precious Metals Institute (IPMI) is the largest and most well-known association focused on precious metals in the world. IPMI does not appear to have any free publications. It does list sponsors and patrons, which at least show the names of major players both internationally and locally.
 - c. The American Gem Trade Association website includes information about retailers and dealers and free guides to trade practices such as "memo transactions".
 - d. The BSA SharePoint Title 31 Issues and Industries site also has background information and links to other internet sites.
- (4) The examiner should become familiar with the general business structure for retail stores and wholesalers. See IRM 4.26.12.9, *Other Retail Overview*, and IRM 4.26.12.11, *Wholesale Distributors Overview*. This will also help in determining if an entity meets the Title 31 definition of a retailer that is exempted from the dealer status under the BSA. Common business structure includes the following:

- a. Owner/Corporate Headquarters
- b. Store/Operations Manager
- c. Office Manager
- d. Sales Staff
- e. Bookkeeper
- f. Cashier

4.26.9.10.8.2
(11-12-2019)
**Determining Exam
Period**

- (1) 31 CFR 1027.210(a), *Anti-money laundering program requirement*, provides that a dealer is required to develop and implement an AML program not later than January 1, 2006, or six months after the date a dealer becomes subject to the requirements to have an AML program. For example:
 - a. An entity was not required to establish an AML program in 2015 based on its 2014 purchases and sales of covered goods. It will need to assess its 2015 business activities to determine if it must establish an AML program in 2016.
 - b. If the entity's covered goods purchases exceed \$50,000 and sales exceed \$50,000 anytime in 2014, they will become subject to 31 CFR 1027.100, *Definitions*, on January 1, 2015 and they will have until June 30, 2015 to implement their AML program.
 - c. The business will need to reassess at the end of each calendar or tax year if it will be required to have an AML program the following year.
- (2) Understanding certain terms will help determine the appropriate examination period.
 - a. Examination Period: This period is generally the most current 12 months and should be the same period cited on the Letter 1112, *Title 31 Violation Notification Letter*, if applicable.
 - b. Dealer Status Determination Period: The calendar or tax year(s) prior to the examination period. The business activities for this period may need to be reviewed to determine if a person purchased more than \$50,000 in covered goods and received more than \$50,000 in gross proceeds from sale of covered goods.
 - c. Because the examination period may include months from two different calendar or tax years (for example, for any 12- month period that is not January-December or October-September), determining dealer status may require examining records from two separate calendar or tax years.
- (3) When first contacting the business, the examiner must not initially define the examination period until a determination is made whether the entity is required to have an AML compliance program.
 - a. Mail Letter 4567, *Introduction Letter for PMSJ Dealers*, to the business.
- (4) If the entity states that it is a dealer subject to 31 CFR 1027.100 the examination period is usually the most current 12 months. Below are some examples to help determine the exam period:
 - a. The entity became subject to the BSA requirement to have an AML program on January 1, 2014 based on its 2013 purchases and sales of covered goods. It had until June 30, 2014 to implement the AML program. The exam starts in May 2015. The examination period is July 1, 2014 – May 30, 2015. The examination period starts in July 2014

because the entity had until July 1, 2014 to initiate the AML program. The exam period covers less than a 12-month period. In this example, select the most relevant six months to test the AML compliance program.

- b. An exam starts in February 2015 and the entity states it became a dealer in 2015 based on its 2014 purchases and sales of covered goods. It was not a dealer in 2014. The entity has until June 30, 2015 to have the AML program in place. The exam period is February 1, 2014 – January 31, 2015 and the entity was not required to have an AML program during this period. The examiner will close the case as a SAA, using Reason Code 100 Not an MSB – No examination conducted. The examiner will also flag the case for a follow-up examination in 2016 using the procedures set by BSA ECS for a follow-up examination.

- (5) If the entity states that it is **not** a dealer subject to 31 CFR 1027.100 then the dealer status determination period is the calendar or tax year(s) prior to the period that would have been the exam period. For example:

- a. An exam starts in March 2015 and the entity states it is not a dealer. The exam period would be March 1, 2014 – February 28, 2015. Review tax or calendar year 2013 records to determine the dealer status for 2014. Review tax or calendar year 2014 records to determine the dealer status for 2015.
- b. If the examiner determines the entity is a dealer for 2014 but not 2015, the entity's AML program should be reviewed for the months in 2014 that it was required to have the AML program. Select the most relevant six months in 2014 to test the AML compliance program.
- c. If the examiner determines the entity is a dealer for 2015 but not 2014, close the case as a SAA, using Reason Code 100 Not an MSB – No examination conducted. Also flag the case for a follow-up examination in 2016 using the procedures set by BSA ECS for a follow-up examination.

4.26.9.10.8.3 (11-12-2019) Initial Contact

- (1) Examiners will use Letter 4479, *PMSJ Appointment letter*, to make initial contact with the business. The examiner must give the business an appointment letter with the scheduled time and date for the Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, examination to the business.

Note: Do not use Letter 2277, *Form 8300 Appointment Letter*, as this is used when a Form 8300 examination is conducted under Title 26.

- (2) See IRM 4.26.9.10.8.2 for determining the exam period and for mailing Letter 4567, *Introduction Letter for PMSJ Dealers*, to the business.
- (3) Plan the initial contact using Workpaper 130 (of the appropriate package), *Initial Contact Check Sheet*, and record the information on it during the contact itself.
 - a. Set up Workpaper #135, *Initial Appointment Agenda*.
 - b. As an AML Compliance examination under Title 31, complete *AML Compliance Program Lead Sheet Title 31* (# 140) as well as, *Form 8300 Policy Procedures Internal Controls Lead Sheet* (# 140).
- (4) Prepare the initial Form 4564, *Information Document Request*, using the information recorded during the telephone conversation with the entity on

Workpaper #130, *Initial Entity Contact Check Sheet*. Include the IDR with the appointment letter and request these items up-front as applicable (this list is not all inclusive):

- a. Name(s), title(s), and contact information for dealer's BSA/AML compliance officer and the dealer IT manager.
- b. Company's history to ascertain a general understanding of the company.
- c. A copy of the AML compliance program in advance of the appointment. The BSA examiner should review copies of the AML program including but not limited to policies and procedures, BSA training monitoring, and reporting policies and procedures.
- d. Copy of the risk assessment.
- e. An organizational chart showing direct and indirect reporting lines.
- f. A list of acronyms used to describe their policies, procedures, computer systems, and departments along with their definitions.
- g. Copy of the independent review of their AML compliance program.
- h. Copies of all internal audits or external audits by regulators. The BSA examiner should note any inconsistencies reported and corrective actions recommended.
- i. Company's booklets/pamphlets (covered goods only).
- j. A download of computer records to be available at the initial appointment.
- k. Form 8300 records required under Title 31. Do not request evidence of compliance with the customer notice requirements that are only required in IRC 60501(e), *Statements to be furnished to persons with respect to whom information is required*, because this is a Title 31 exam.

- (5) The examiner may mail or hand-deliver the appointment letter and the IDR to the business.

4.26.9.10.8.4 (11-12-2019) Exam Scope Depth

- (1) Determining the scope of an examination is the process by which issues are selected that warrant examination. Base the scope of the examination on the facts and circumstances of each case. Consider factors such as inadequate records, poor internal control, and unusual currency flow. Select issues so that all items necessary for a substantially proper determination of the BSA requirements are considered. Exercise proper judgment throughout the examination process to expand or contract the scope as needed.
- (2) The depth of the examination is the extent to which an issue is developed or examined. The depth of the examination demonstrates the degree of intensity and thoroughness applied to decide the correctness of an item. Determining the depth of the examination will help estimate the time required to complete the examination. When determining the depth of the examination, consider the:
 - a. Risk assessment
 - b. AML program
 - c. Type of evidence/documents available
 - d. Complexity of transactions
 - e. Independent review
 - f. Training
- (3) The scope and depth of the BSA examination depend upon the facts and circumstances in each case. The scope and depth of a dealer examination should initially include six months of a 12-month examination period. The selected six months can include high volume periods, particularly regarding

“dealer” transactions, or a period related to certain known events. Consider that peak business activity periods may vary. The six months do not have to be contiguous.

- (4) To facilitate understanding the dealer’s risk profile and to establish the scope of the BSA examination, complete the following steps, in conjunction with the review of the dealer’s BSA/AML risk assessment:
 - a. Review prior examination reports, related workpapers, and management’s responses to previously identified BSA violations, deficiencies, and recommendations.
 - b. Review news articles concerning or pertaining to the dealer or its management.
 - c. Review internal or external independent reviews and workpapers for BSA compliance, as necessary, to determine the comprehensiveness and quality of audits, findings, and management responses and corrective actions. The independent reviewer’s scope, procedures, and qualifications provide valuable information on the adequacy of the AML compliance program.
 - d. Submit subsequent IDR to the dealer if necessary.
- (5) If after examining six months of records, it is determined that a dealer has implemented an effective AML compliance program designed to ensure BSA compliance, the transaction testing period can be limited to the six months examined. If no serious violations or deficiencies were detected during this period, the examination can be closed. If the dealer lacks an adequate compliance program or the examiner detects problems during the six-month review period, the examination period should be expanded appropriately.
- (6) If the dealer has been previously examined and only minor deficiencies were noted, a more limited scope examination should be considered. See IRM 4.26.6, *Bank Secrecy Act Examiner Responsibilities for BSA Examinations*, for more information on Scope and Depth.

4.26.9.10.8.5
(11-12-2019)
Interview

- (1) The examiner must conduct the examination at the place of business.
- (2) The examiner should interview both the owner and/or manager to obtain information on the operation of the business and the employee responsible for overseeing the AML program and filing of Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*. Record the initial interview on Workpaper 205 of either Lead Sheet.
- (3) The examiner should explain the examination process and specifically state that the examination is **NOT** an income tax examination.
- (4) Because the business is selected for a Title 31 examination and is also subject to the Form 8300 filing requirements under both Title 31 and Title 26, the BSA examiner must:
 - a. Advise the entity that the Form 8300 is a dual-purpose form required under both Title 31 and Title 26.
 - b. Also, advise that information acquired during the examination may be used to determine compliance with the related regulations under both titles.
 - c. Fully document this advice on Form 9984, *Examining Officer’s Activity Record*, as follows: “I advised XXX that the Form 8300 is a dual-purpose

form required under both Title 31 and the Internal Revenue Code. I further advised that information acquired during this examination may be used to determine compliance with the related regulations under both titles.”

- (5) Discuss the company’s compliance under Title 31, which should include the AML compliance program, management structure, BSA risk assessment, Form 8300 filings, and the level and extent of automated BSA/AML systems.
- (6) During the interview, the examiner should ascertain and/or verify:
 - a. The TIN of the business
 - b. The names and titles of officers or employees who handle cash transactions and are responsible for filing Form 8300
 - c. The owner/officer’s knowledge of the BSA as it relates to dealers of PMSJ
 - d. Who handles received cash, prepares bank deposit slips, and makes the bank deposits
 - e. The number and types of bank accounts
 - f. The type of records maintained on transactions required to be reported on Form 8300
 - g. Secure a copy of the AML program
 - h. Determine who has been designated as the compliance officer and the BSA knowledge of compliance officer
 - i. Training of employees on the BSA, the AML compliance program, and filing Form 8300
 - j. If an independent review was conducted and the results
 - k. The internal controls of the business for cash transactions
 - l. Whether the business has filed any Form 8300
 - m. Procedures used by the business to ensure that the information contained in the Form 8300 was complete and correct. For example, did the business verify the identity of the person from whom the cash was received by a driver’s license, passport, or other official document?
 - n. Procedure in place to ensure they are not buying covered goods from terrorist and/or criminal elements
 - o. Procedure to understand their distribution channels. This should include knowing both the seller and its customers
 - p. The entity’s membership in various types of trade associations
 - q. Related entities
- (7) The examiner needs to understand the company’s process and workflow and develop an adequate understanding of the processing environment – the process, related controls, and key roles and responsibilities. This is critical to performing the BSA examination. This understanding is achieved through two documentation techniques, process narratives and flow charts. These techniques help the examiner understand the dealer’s processes.
 - a. The objective of process narratives and flow diagrams is to generate an accurate representation of how work is performed and how transactions flow.
 - b. Typically, creating this type of documentation is a process that involves individuals at various levels of responsibility walking through processing steps and discussing related documents, responsibilities, and/or outputs.

- c. The examiner will need to pay close attention to the flow of payments (cash/cash equivalent), products (covered goods), and paper work.
- (8) Narrative and process flow tools allow the examiner to organize, describe, and graphically depict the results of:
 - a. Reviewing policy and procedure manuals
 - b. Discussing the process with key employees through inquiry
 - c. Performing a process walk through of sub-processes using samples
 - d. Considering key inputs and outputs to a process
 - e. Lines of responsibility for individual employees and departmental roles.
- (9) Condense the process information into manageable narratives and process flows that incorporate all the key steps, processing responsibilities, documents, and actions. Map key risks and controls on the process flow diagram to indicate when, by whom, and how controls mitigate risks.
- (10) Accurate, complete documentation of the company's process (as it pertains to covered goods) serves as a baseline for testing the risk assessment, internal controls, and effectiveness of the AML compliance program.
- (11) Do not ask about compliance with the customer notice requirements because this is not a requirement under Title 31 and this is a Title 31 exam.
- (12) The interview and inspection of records must be solely for the Title 31 BSA examination, which includes Form 8300 filings. No inquiries should be made as to the filing of other returns required by Title 26 or whether a specific item is reported on any such returns. The latter inquiries could constitute the opening of an income tax examination.
- (13) Refer to IRM 4.26.11, *Bank Secrecy Act, BSA Examiner Responsibilities for Form 8300 Examinations*, for additional questions relating to knowledge and intent.
- (14) The examiner should advise the trade or business that information from their records may be used for any tax matter permitted by the Internal Revenue Code.

4.26.9.10.8.6
(11-12-2019)
**Examining the AML
Program**

- (1) The examiner should follow the exam steps outlined in the *AML Compliance Program Lead Sheet Title 31* (#140) and the *Form 8300 Exam Lead Sheet* (#300).
- (2) Review the AML program to ensure it is commensurate with the dealer's risk and contains:
 - a. A system of internal controls to ensure ongoing compliance
 - b. Independent testing of the BSA compliance program
 - c. A designated person or persons responsible for managing BSA compliance (BSA compliance officer)
 - d. Training for appropriate personnel
 - e. Includes procedures for obtaining relevant customer and/or supplier information
- (3) Determine whether the dealer has adequately identified the risks within its operations and incorporated the risks into the AML compliance program. To mitigate these risks, the dealer should adopt policies, procedures, and processes that include:

- a. Identification of high-risk activities.
 - b. Mitigation strategies to manage high-risk activities.
 - c. Recordkeeping requirements.
- (4) Determine whether the AML compliance program includes policies, procedures, and processes that:
- a. Identify high-risk operations (goods, services, customers, suppliers, counterparties, and geographic locations); provide for periodic updates to the dealer's risk profile; and provide for an AML compliance program tailored to manage risks.
 - b. Identify a person or persons responsible for BSA/AML compliance.
 - c. Provide for program continuity despite changes in management or employee composition or structure.
 - d. Meet all regulatory requirements and recommendations for BSA compliance and provide for timely updates to implement changes in regulations or changes to the internal policies and procedures.
 - e. Implement risk-based policies for obtaining relevant customer and supplier information.
 - f. Identify reportable transactions and accurately file all required reports, Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*.
 - g. Provide sufficient controls and monitoring systems for the timely detection of high-risk activity and include procedures for dealing with high-risk activity.
 - h. Provide for adequate supervision of employees and appropriate persons that handle currency transactions, complete reports, monitor for suspicious activity, or engage in any other activity covered by the BSA and its implementing regulations.
 - i. Train appropriate personnel to be fully aware of their responsibilities under the BSA regulations and internal policy guidelines.
- (5) Determine whether the BSA/AML review is independent, such as performed by a person (or persons) who is not part of the dealer's BSA/AML compliance staff, not the compliance officer, or does not report to the BSA compliance officer. Evaluate the qualifications of the person(s) performing the independent review to assess whether the dealer can rely upon the findings and conclusions. Validate the reviewer's reports and workpapers to determine whether the dealer's independent review is comprehensive, accurate, adequate, and timely.
- (6) The independent review should address the following:
- a. The overall integrity and effectiveness of the AML compliance program, including policies, procedures, and processes.
 - b. BSA risk assessment.
 - c. BSA reporting and recordkeeping requirements.
 - d. Procedures for obtaining relevant customer-related information
 - e. Appropriate transaction testing, with emphasis on high-risk operations (goods, service, customers, and geographic locations).
 - f. Training adequacy, including its comprehensiveness, accuracy of materials, the training schedule, and attendance tracking.
 - g. The integrity and accuracy of management information systems (MIS) used in the AML compliance program.

- (7) Determine whether the independent review included a review of high-risk activity monitoring systems and an evaluation of the system's ability to identify unusual activity. Ensure through a validation of the reviewer's reports and workpapers that the dealer's independent review:
 - a. Reviews policies, procedures, and processes for monitoring high-risk activity.
 - b. Evaluates the system's methodology for establishing and applying expected activity or filtering criteria.
 - c. Evaluates the system's ability to generate monitoring reports.
 - d. Determines whether the system's filtering criteria are reasonable.
 - e. Determines whether previously identified deficiencies have been corrected.
- (8) Determine whether management has designated a person or persons responsible for the overall AML compliance program.
 - a. Determine whether the BSA compliance officer has the necessary authority and resources to execute all duties.
 - b. Assess the competency of the BSA compliance officer and his or her staff, as necessary.
 - c. Determine whether the BSA compliance area is sufficiently staffed for the dealer's overall risk level, size, and BSA compliance needs. In addition, ensure that no conflict of interest exists, and that staff is given adequate time to execute all duties.
- (9) Determine whether the following elements are adequately addressed in the training program and materials:
 - a. The importance the board of directors and/or senior management place on ongoing education, training, and compliance.
 - b. Comprehensiveness of training, considering specific risks of the covered products.
 - c. Training of appropriate personnel.
 - d. Frequency of training.
 - e. Documentation of attendance records and training materials.
 - f. Coverage of dealer policies, procedures, processes, and new rules and regulations.
 - g. Coverage of different forms of money laundering and terrorist financing as it relates to identification and examples of high-risk activity.
 - h. Penalties for noncompliance with internal policies and regulatory requirements.
 - i. As appropriate, conduct discussions with employees to assess their knowledge of BSA/AML policies and regulatory requirements.
- (10) After reviewing the dealer's AML program, document an evaluation of the program. Revisit the initial examination plan to determine whether any strengths or weaknesses identified during the interviews, walkthrough of the business, and review of the dealer's AML program warrant adjustments to the initial planned scope. Document and support any changes to the examination scope and then proceed to the additional examination procedures.

4.26.9.10.8.7
(11-12-2019)

**Examining for
Reportable Transactions**

- (1) The principal records will be a combination sales/cash receipts type journal. There may be information cards on preferred customers that may include names and addresses, items purchased, purchase prices, and methods of payment.
- (2) Examine the appropriate documents and accounting records to determine if:
 - a. Transactions occurred which involved the receipt of reportable cash in excess of \$10,000.
 - b. There are consecutive or related reportable transactions in excess of \$10,000.
 - c. Multiple items were purchased at the same time but recorded as separate purchases.
 - d. Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, was filed on such transactions.
- (3) Watch for payments in the form of sequentially numbered checks, multiple checks from the same account drawn on the same date, checks with no identified payer, payments drawn on a bank located in a foreign country or far from the payer.
- (4) Use of money orders and cashier's checks less than \$3,000 could be an indication of structuring. Watch for bulk amounts of sequentially numbered U.S. money orders and traveler's checks. If the money orders and traveler's checks were purchased for the maximum face value, and then used to purchase diamonds and gems at dealers located in foreign countries, check that the amounts match the invoices.
- (5) Cross reference customer cards for various purchases and form of payment. Look for matching items of jewelry that were agreed upon at the same time and purchased on different dates. Also, look for sales of large ticket items with accessories ordered and paid for later.
- (6) Identify multiple payments that are made in currency, or items defined as cash, on the same day or numerous days by customers. If this type of transaction occurs, review all available information to determine whether a Form 8300 was required.
- (7) Watch for manipulation of inventory items to conceal the sale of large ticket items.
- (8) A review of appraisals or assay reports may lead to incorrect receipts or large cash sales that were not recorded.
- (9) Review in-house financing where multiple payments may exceed \$10,000 during a 12-month period.
- (10) When recording potential cash transactions, it is important to note the:
 - a. Date funds were received
 - b. Amount
 - c. Date funds were deposited
 - d. Name of the transactors
 - e. Receipt number
 - f. Account number and account owner (if different from transactors)

- (11) For any transaction the examiner believes was reportable and a Form 8300 was not filed, the examiner should copy the receipts, contracts, and any other supporting documentation needed. The examiner should record the location of the original records pertaining to these transactions.
- (12) There may be a need, on a case-by-case basis, to interview the customer to obtain all the facts as required to develop the issues.
- (13) If a business uses a computerized system, the examiner must test the system to ensure its integrity before relying upon such records for the Form 8300 examination. For example, the examiner can run sample data through the system to see how the system performs.
- (14) Do not address the customer notification requirement of IRC 6050I(e), *Statements to be furnished to persons with respect to whom information is required*, because this is a Title 31 examination and there is no customer notification requirement under Title 31.

4.26.9.10.8.8

(11-12-2019)

Transaction Testing

- (1) The examiner must conduct transaction testing to ensure the AML has been effectively implemented. Use transaction testing to identify transactions that may be suspicious in nature, do not make business sense, or appear to be conducted in a manner to avoid the Form 8300 reporting requirements. Some examples include:
 - a. Purchasing covered goods from countries that are known for dealing in conflict products.
 - b. A single transaction structured as multiple transactions of less than \$10,000.
 - c. Transactions in excess of \$10,000 where cash and non-cash payments appear to be combined to avoid the filing requirements.
 - d. A pattern or series of transactions of less than \$10,000 conducted over a relatively short period by or for the same person.
- (2) Transaction testing includes the examination procedures detailed in the following paragraphs and the procedures discussed above.
- (3) Document the decision regarding the extent of transaction testing to conduct and the activities where it is to be performed, as well as the rationale for any changes to the scope of transaction testing that occur during the examination.
- (4) Perform transaction testing of the entity's sales and purchases, based on the risk assessment as well as prior examinations and independent reviews. This must be done by product and country. For purchases, inspect invoices to determine if the purchased product is obtained from a logical source such as diamonds from South Africa or emeralds from Colombia versus diamonds from a sanctioned location – one that is known for the sale of conflict diamonds.
- (5) Determine whether an activity is unusual or suspicious.
- (6) Inspect any certificates of the product's authenticity and country of origin.
- (7) For sales, determine where the product was sold to and if there are export documents that tie into those sales.
- (8) For both sales and purchases, determine if the invoice amounts make sense. For example, should a customer be able to buy or sell diamonds for \$1.00 per carat?

- (9) With the purchase of covered goods, determine if due diligence was conducted on the supplier. Was it documented? Were the governmental lists cross-checked? Was there a proper customer?
- (10) Depending on the initial findings, the examiner may need to expand the scope and/or depth of the review to include additional periods.
- (11) Based on examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with purchase and sale of covered goods.

4.26.9.10.8.9 (11-12-2019) **Red Flags**

- (1) PMSJ are easily transportable, highly concentrated forms of wealth, and easily converted to cash. As such they are highly attractive to money launderers and other criminals.
- (2) The business and/or the customer can be involved in potential money laundering schemes. The examiner must focus on both the business and the customers or suppliers during the examination.
- (3) The following lists of factors may be an indication of suspicious activity. Any of these “red flags” should be thoroughly researched and reviewed during an examination of a dealer in precious metals, stones or jewels.
- (4) Indicators of suspicious activity by the business include:
 - a. Failing to maintain complete records.
 - b. Failing to maintain accurate records.
 - c. Failing to record specific transactions.
 - d. Accepting third-party payments.
 - e. Failing to file Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, on reportable transactions.
 - f. Structuring a transaction by breaking one transaction into several to circumvent the reporting requirements.
 - g. Treating the purchase of related items as separate sales.
 - h. Purchases or sales that are not in conformity with standard industry practice or that are unusual for this type of business.
 - i. Willingness to trade or exchange items for less than retail value.
 - j. Purchases are inconsistent with past purchasing trends.
 - k. Third-party payments for items, such as the extent to which the business engages in transactions other than with established customers or sources of supply or other dealers subject to the regulations at 31 CFR 1027, *Rules for Dealers in Precious Metals, Precious Stones, or Jewels*.
 - l. Sales to nonexistent customers.
- (5) Indicators of suspicious activity by the customers or suppliers include:
 - a. Using multiple locations to conduct transactions.
 - b. Using several individuals at one or more locations to conduct a transaction.
 - c. Using aliases when conducting transactions.
 - d. Unwillingness by a customer or supplier to provide complete and accurate personal information, financial references, or business affiliations.

- e. Conducting numerous transactions at the same location at different times on the same day.
 - f. Unusual payment methods such as the use of large amounts of cash, multiple sequentially numbered money orders, traveler's checks or cashier's checks or payment from third parties.
 - g. Using a combination of currency and monetary instruments to conduct transactions.
 - h. Return of high-value items paid for in cash or monetary instruments to obtain a check refund.
 - i. Structuring of cash transactions to evade Form 8300 reporting requirements by making purchases at various locations.
 - j. Refusal to provide personal information for purposes of filing Form 8300 or other recordkeeping and reporting requirements.
 - k. Willingness to trade or exchange items for less than retail value.
 - l. Unusual purchases or sales for a customer or supplier or purchases are inconsistent with past purchasing trends.
 - m. Transactions on behalf of individuals/corporations located in jurisdictions with little or no AML regulation, countries with known drug, criminal or terrorist links and offshore entities in tax havens.
- (6) Evidence uncovered of potential money laundering should be referred to CI on a Form 2797, *Referral Report for Potential Fraud Cases*.

4.26.9.10.9
(11-12-2019)
**Finalizing the Title 31
Exam**

- (1) Determine compliance with the AML program requirement under 31 CFR 1027.210, *Anti-money laundering programs for dealers in precious metals, precious stones, or jewels*, as well as the Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, filing requirements under 31 CFR 1010.330, *Reports relating to currency in excess of \$10,000 received in a trade or business*. There is no examination of or conclusions regarding the IRC customer notification requirement which is not required under Title 31. Complete the workpaper #400, *BSA Violations Summary Form Title 31*.
- (2) Accumulate all pertinent findings from the examination performed. Evaluate the thoroughness and reliability of any risk assessment conducted by the dealer. Determine whether:
- a. The AML program is effectively monitored and supervised in relation to the dealer's risk profile as determined by the risk assessment.
 - b. The AML program is effective in mitigating the dealer's overall risk.
 - c. The board of directors and senior management are aware of BSA regulatory requirements; effectively oversee BSA/AML compliance; and commit, as necessary, to corrective actions (such as independent reviews and regulatory examinations).
 - d. Policies, procedures, and internal controls are adequate to ensure compliance with applicable laws and regulations and provide sufficient risk management to appropriately address high-risk operations (goods, services, customers, suppliers, counterparties, and geographic locations).
 - e. Independent testing (audit) is appropriate and adequately tests for compliance with required laws, regulations, and policies.
 - f. The designated person responsible for coordinating and monitoring day-to-day compliance is competent and has the necessary resources.
 - g. Personnel are sufficiently trained to adhere to legal, regulatory, and policy requirements.

- h. Reportable transactions have been identified and any required Form 8300 has been filed timely and accurately.
 - i. Information and communication policies, procedures, and processes are adequate and accurate.
- (3) Determine whether deficiencies or violations were previously identified by management, independent reviews, or in prior regulatory exam, or were only identified because of the current BSA examination.
- (4) Determine the underlying cause of any violations such as (the list is not all inclusive):
 - a. Management has not assessed, or has not accurately assessed, the dealer's AML risks.
 - b. Management is unaware of relevant issues.
 - c. Management is unwilling to create or enhance policies, procedures, and internal controls.
 - d. Management or employees disregard established policies, procedures, and internal controls.
 - e. Management or employees are unaware of or misunderstand regulatory requirements, policies, procedures, or internal controls.
 - f. High-risk operations (goods, services, customers, suppliers, counterparties, and geographic locations) have grown faster than the capabilities of the AML program.
 - g. Changes in internal policies, procedures, and internal controls are poorly communicated.
- (5) The examiner must hold a closing conference with the owner, corporate officer or general partner. Other employees, such as the BSA compliance officer and person responsible for filing Form 8300 may be asked to attend to assist in addressing specific items. The examiner must:
 - a. Review with the business deficiencies in the AML compliance program, and Form 8300 transactions not reported, or Form 8300 filed late, incomplete or inaccurate.
 - b. Advise the dealer of any recordkeeping deficiencies.
 - c. Identify actions needed to correct any outstanding deficiencies or violations, including the possibility of requiring the dealer to conduct a more detailed risk assessment.
 - d. Obtain an explanation for all issues discussed.
 - e. Review any additional documents or information provided by the dealer and determine whether any items should be removed from the list of violations.
 - f. Solicit an amended AML program if there is an AML program deficiency.
 - g. Ask the business to provide a written statement of the corrective actions they will undertake to address the issues noted.

4.26.9.10.10
(11-12-2019)
Closing

- (1) A dealer case can be closed under either Title 31 or Title 26 depending on the section under which the exam was conducted.
- (2) PMSJ dealers have requirements under Title 31 for an AML compliance program and under both Title 31 and Title 26 for filing Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*.

4.26.9.10.10.1
(11-12-2019)

**Closing a Non-Dealer
Case Examined Under
Title 31**

- (1) The examiner may determine that the business is not a dealer. See IRM 4.26.12, *Bank Secrecy Act, Examination Techniques for Form 8300 Industries*, for business activities that are not defined as a PMSJ dealer.
- (2) If the business is not a dealer and there are no Form 8300 reporting violations, the examiner should close the case as “No Issue” and send the Letter 4029, *Bank Secrecy Act No Change Letter*. In order not to mislead the business, ensure that the letter addresses only the Form 8300 compliance and insert in the “Recommendations are as follows:” section: “Form 8300 customer notification was not covered in this examination because it is not a requirement under the BSA”.
- (3) If the business is not a dealer and there are Form 8300 violations, follow the procedures for issuing Letter 1112, *Title 31 Violation Notification Letter*.
 - a. The failure to file a Form 8300 under 31 CFR 1010.330, *Reports relating to currency in excess of \$10,000 received in a trade or business*, will be cited on the Form 13726, *Summary of Examination Findings and Recommendations*. Form 13726 should contain a statement in the Explanation of Apparent Violations Regulations and Recommendations section: “Form 8300 customer notification is not covered by this examination because the customer notification is not required under the Bank Secrecy Act”.
 - b. No violations for an AML compliance program are cited because the business is not a dealer and therefore is not required to have an AML program.
- (4) If no referral to CI is warranted, the examiner should secure any delinquent Form 8300. See IRM 4.26.11, *Bank Secrecy Act, BSA Examiner Responsibilities for Form 8300 Examinations*, for detailed information.
- (5) Close the Title 31 case. The examiner should charge all examination time to the Title 31 case.

4.26.9.10.10.2
(11-12-2019)

**Closing a Dealer Case
Examined Under Title 31**

- (1) Complete the Title 31 case file, including all workpapers, Lead Sheets, and documentation to substantiate the AML program violations and the Title 31 Form 8300 reporting violations. Only one Title 31 case file needs to be completed.
- (2) If there are no Title 31 violations, issue Letter 4029, *Bank Secrecy Act No Change Letter*.
 - a. In order not to mislead the entity, insert in the “Recommendations are as follows:” section “Form 8300 customer notification is not covered in this examination because is not a requirement under the BSA”.
- (3) If there are Title 31 violations, the examiner must issue Letter 1112, *Title 31 Violation Notification Letter*.
 - a. If a Letter 1112 is issued, failure to file a Form 8300 under 31 CFR 1010.330, *Reports relating to currency in excess of \$10,000 received in a trade or business*, will be cited on the Form 13726, *Summary of Examination Findings and Recommendations*. Form 13726 should contain a statement in the Explanation of Apparent Violations Regulations and Recommendations section: “Form 8300 customer notification is not covered by this examination because the customer notification is not required under the Bank Secrecy Act”.

- b. Generally, if there is a Form 8300 violation under Title 31 there will be an AML program violation. If the business failed to file any required Form 8300 timely and correctly, there is a breakdown in the business's internal controls. If the AML program was effectively implemented and adequately monitored, there would not be a Form 8300 reporting violation.
 - c. If there are AML program violations of 31 CFR 1027.210, *Anti-money laundering programs for dealers in precious metals, precious stones, or jewels*, the examiner must state the exact nature of any program deficiencies (such as internal controls, training, independent review, and designated compliance officer) in the Letter 1112.
- (4) If it is determined that a referral should be made to FinCEN, follow the regular referral procedures and include the Title 31 Form 8300 issues (if applicable).
 - a. Record on Form 9984, *Examining Officer's Activity Record*, that a referral of the Title 31 case is being made for a Title 26 Form 8300 examination to address any applicable penalties and the customer notification requirement.
 - b. In the FinCEN referral, state: "Form 8300 is a dual-purpose form. A Form 8300 examination is a necessary part of a Title 31 examination to determine if an effective AML exists. XXX (the entity) was advised that the Form 8300 examination information could be used in a Title 26 Section IRC 6050I case on (date shown on Form 9984). The customer notification requirements of IRC 6050I(e) were not examined during the Title 31 examination."
- (5) If no referral to CI is warranted, the examiner should secure delinquent Form 8300. See IRM 4.26.11, *Bank Secrecy Act, BSA Examiner Responsibilities for Form 8300 Examinations*, for detailed information.
- (6) Close the Title 31 case. The examiner should charge all examination time up to this point to the Title 31 case.
- (7) Open the Title 26 Form 8300 case file if necessary to examine the customer notification issues or to assert a Form 8300 penalty.
 - a. See IRM 4.26.11 for establishing the case on ERCS.
 - b. Complete a Form 8300 administrative case file. See IRM 4.26.11. The examiner can use copies of Form 9984, *Memorandum of Interview*, Form 8300 Lead Sheet, and documentation supporting the Form 8300 violations from the Title 31 case file.
 - c. Inspect the Form 8300 customer notifications for completeness and accuracy.
 - d. Form a conclusion about the entity's compliance with the annual written statement notification requirements.
 - e. If applicable, complete a Form 8300 penalty case file using regular IRC 6721, *Failure to file correct information returns*, and IRC 6722, *Failure to furnish correct payee statements*, procedures. See IRM 4.26.11.
 - f. Charge time spent on the Title 26 Form 8300 exam to activity code 509.
- (8) For details regarding procedures for requesting Title 26 after completing examinations under Title 31, see IRM 4.26.8.
- (9) For details regarding case content, assembly, procedures, and a discussion of penalty considerations, see IRM 4.26.11.

4.26.9.11
(11-12-2019)
**Insurance Companies
Overview**

- (1) FinCEN issued regulations at 31 CFR Part 1025, *Rules for insurance companies*, on November 3, 2005 that require certain insurance companies to establish an AML compliance program and file SARs. The effective date is May 2, 2006.
- (2) The requirement to establish an AML program and file SARs applies only to insurance companies as defined in 31 CFR 1025.100(g), *Insurance company or insurer, offering covered products*, as defined in 31 CFR 1025.100(b), *Covered product*.
- (3) Insurance companies offer a variety of products aimed at transferring the financial risk of a certain event, from the insured to the insurer. These products include life insurance policies, annuity contracts, property and casualty insurance policies, and health insurance policies. These products are offered through several different distribution channels. Some insurance companies sell their products through direct marketing in which the insurance company sells a policy directly to the insured. Other companies employ agents, who may either be captive or independent. Captive agents generally represent only one insurer or one group of affiliated insurance companies; independent agents may represent a variety of insurance carriers.
- (4) The regulations at 31 CFR Part 1025 focus on those covered insurance products possessing features that make them susceptible to being used for money laundering or the financing of terrorism.
 - a. For example, life insurance policies that have a cash surrender value are potential money laundering vehicles. Cash value can be redeemed by a money launderer or can be used as a source of further investment of tainted funds for example, by taking out loans against such cash value.
 - b. Similarly, annuity contracts also pose a money laundering risk because they allow a money launderer to exchange illicit funds for an immediate or deferred income stream or to purchase a deferred annuity and obtain clean funds upon redemption.
 - c. These risks do not exist to the same degree in term life insurance products, group life insurance products, group annuities, or in insurance products offered by property and casualty insurers or by title or health insurers.

4.26.9.11.1
(11-12-2019)
Terminology

- (1) 31 CFR 1025.100, *Definitions*, contains a listing of key terms that relate to insurance companies. Understanding these terms will help understand the regulation and the insurance industry.
- (2) Some terms commonly used in this industry that have not been previously discussed in this IRM section are:
 - a. Actuary – A specialist with extensive training in the math of life insurance. An actuary performs the calculations needed to make sure that the company's products are mathematically sound. The actuary calculates mortality rates for life insurance or annuity policies and morbidity tables for accident and health policies.
 - b. Annuity contract – any agreement between the insurer and the contract owner whereby the insurer promises to pay out a fixed or variable income stream for a period.

- c. Application Form – It includes basic information such as the employer, health of the insured and general personal information. An Attending Physician's Statement may be required if there is a question about the insured's health.
- d. Beneficiary – Receiver of insurance benefit.
- e. Broker-dealer in securities – A broker or dealer in securities, registered or required to be registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934, except persons who register pursuant to section 15(b)(11) of the Securities Exchange Act of 1934.
- f. Equity Indexed Annuity – An annuity that guarantees a minimum fixed rate of interest credits but also provides higher credits if a specified common stock index rises sufficiently.
- g. Face Page of an Insurance Policy – The face page includes all the basic information about the insured and includes the promise to pay if specific events occur.
- h. Fixed Annuity – An annuity that provides a stated dollar benefit, regardless of the insurer's investment return.
- i. Gross Premium – Net premium plus loading equals the amount that the customer pays.
- j. Group annuity contract - A master contract providing annuities to a group of persons under a single contract.
- k. Group life insurance policy - Any life insurance policy under which a number of persons and their dependents, if appropriate, are insured under a single policy.
- l. Insurable Interest – Related to the policy owner and has two criteria: The individual (1) must be likely to benefit if the insured continues to live and (2) is likely to suffer a loss or detriment if the insured one dies. The insured is generally a relative of the policyholder or the policyholder themselves. The insured can also be in a business relationship with the policyholder.
- m. Health Insurance Policies and Disability Income Benefits - Insurance that protects against the risk of poor health. The health insurance helps pay hospital, surgical, doctor, and medical testing expenses. The disability portion can insure income continuance while the insured is disabled.
- n. Insured – Person whose life or health is covered.
- o. Insurance agent - A sales and/or service representative of an insurance company. The term "insurance agent" encompasses any person that sells, markets, distributes, or services an insurance company's covered products, including, but not limited to, a person who represents only one insurance company, a person who represents more than one insurance company, and a bank or broker-dealer in securities that sells any covered product of an insurance company.
- p. Insurance broker - A person who, by acting as the customer's representative arranges and/or services covered products on behalf of the customer.
- q. Insurance company or insurer - Any person engaged within the United States as a business in the issuing or underwriting of any covered product. The term "insurance company" or "insurer" does not include an insurance agent or insurance broker.
- r. Insurance Policy – A legally enforceable agreement between an insurance company and the purchaser of a policy. It is a contract.
- s. Law of Large Numbers – The greater the number of similar exposures (for example, insured lives) to a peril, the less the observed loss experience will deviate from the expected loss experience.

- t. Life Insurance – Protects against economic loss resulting from personal risks. Life insurance policies protect interested parties from the risk of premature death. It provides income to the beneficiary.
- u. Loading – Amount added to net premium to cover other expenses.
- v. Mortality Table – Used to compute mortality rates; it tells the insurers the rates at which insured people are expected to die.
- w. Net Premium – The amount needed just to pay claims, determined by the rate of mortality and investment income.
- x. Permanent life insurance policy - An agreement that contains a cash value or investment element and that obligates the insurer to indemnify or to confer a benefit upon the insured or beneficiary to the agreement contingent upon the death of the insured.
- y. Personal Risks – Premature death (life insurance); poor health (accident, disability, and health insurance) or, outliving resources (annuity).
- z. Policyholder – Purchaser of the policy.
- aa. Property and Casualty Insurance – Insurance that protects against property damage.
- ab. Reserves - Monies set aside by the insurance company to pay future benefits and are restricted by law to use for any other purpose. A portion of each premium payment goes into funding the reserves. Smaller portions are set aside in the earlier years of the policy because the risk is lower. If an event (death or injury) occurs in an earlier year, benefits are paid out of the general fund. This is the concept of risk distribution. The net amount of risk is the difference between the death benefit and the amount of reserve.
- ac. Risk Distribution – Insurer accepts risks from a large number of people and only a portion of them will suffer the loss within a given period. Risk distribution relies on the “law of large numbers”.
- ad. Risk Transfer – Purchase of insurance transfers the policyholder’s risk.
- ae. Underwriting – An analysis of risk; the study of information on insurance applications to determine how much risk an insurance applicant represents to the company. If the risk is within acceptable limits, the application is approved. If the risk is lower or higher than the average, an underwriter may approve at a lower or higher premium rate. If it is not within company limits, the company may deny the insurance. The goal is to write as many policies as possible while keeping risk loss within an acceptable range.
- af. Universal Life Policy – A type of life insurance policy characterized by flexible premiums, a shift of some of the investment risk to the policy owner even though the policy owner is not allowed to direct the investment portfolio, and a choice of death benefit designs.
- ag. Variable Annuity – An annuity with benefit payments that vary depending on the performance of selected blocks of the insurers invested assets.
- ah. Variable Life Policy – A type of life insurance policy in which the policy owner directs how the cash value will be invested, and thus bears the investment risk, and in which the death benefit is linked to the investment performance of the policy.
- ai. Variable Universal Life Policy – A type of life insurance policy that combines the premium flexibility features of universal life insurance with the policy owner-directed investment aspects of variable life insurance.
- aj. Whole Life Policy – A life insurance policy that provides death benefits upon the death of the insured, no matter when that occurs, if the policy is kept in force by the policy owner.

4.26.9.11.2
(11-12-2019)

Definition of Insurance Company and Covered Products

- (1) 31 CFR Part 1025, *Rules for insurance companies*, provides the BSA regulations and definitions for insurance companies.
- (2) The term “insurance company” or “insurer” means any person engaged within the United States as a business in the issuing or underwriting of any covered product. 31 CFR 1025.100(g), *Insurance company or insurer*.
 - a. The term “insurance company” or “insurer” does not include an insurance agent or insurance broker.
 - b. If an insurance company that is not presently issuing or underwriting a covered product should do so in the future, the insurance company would then become subject to the BSA regulations (but only to the extent of its business relating to covered products). Conversely, if an insurance company ceases issuing or underwriting covered products, the insurance company would no longer be subject to the BSA regulations.
- (3) Covered products are defined at 31 CFR 1025.100(b), *Covered product*, as:
 - a. A permanent life insurance policy, other than a group life insurance policy;
 - b. An annuity contract, other than a group annuity contract; and
 - c. Any other insurance product with cash value or investment features.
- (4) The definition of covered product encompasses any insurance product having the same kinds of features that make permanent life insurance and annuity products more at risk of being used for money laundering, such as, having a cash value or investment feature.
- (5) The following insurance products meet the definition of a covered product:
 - a. Whole Life Insurance
 - b. Universal Life Insurance
 - c. Variable Life Insurance
 - d. Variable Universal Life Insurance
 - e. Fixed Annuity
 - f. Equity Indexed Annuity
 - g. Variable Annuity

4.26.9.11.3
(11-12-2019)
BSA Law

- (1) Insurance companies as defined at 31 CFR 1025.100(g), *Insurance company or insurer*, must:
 - a. Create and maintain an AML program as required by 31 CFR 1025.210, *Anti-money laundering programs for insurance companies*.
 - b. File SARs as required by 31 CFR 1025.320, *Reports by insurance companies of suspicious transactions*, for suspicious transactions of \$5,000 or more.
- (2) See Guidance (Frequently Asked Questions) *Anti-Money Laundering Program and Suspicious Activity Reporting Requirements for Insurance Companies* (03/20/2008) at <https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-anti-money-laundering-program>.
- (3) Insurance companies are required to file FinCEN Form 114, *Report of Foreign Bank and Financial Accounts*.

- (4) Insurance companies must also file FinCEN Form 105, *Report of International Transportation of Currency or Monetary Instruments*.
 - a. All FinCEN Forms 105 must be filed with the customs officer in charge at any port of entry or departure.
 - b. If an examiner determines that an insurance company failed to file FinCEN Form 105 or meet the Currency or Monetary Instruments (CMIR) requirements, the examiner must make a referral to Customs through the BSA Policy Liaison to FinCEN.

4.26.9.11.3.1
(11-12-2019)
AML Program

- (1) Certain insurance companies must establish and implement a written, risk-based AML program reasonably designed to prevent the insurance company from being used to facilitate money laundering and the financing of terrorism.
- (2) At a minimum, the AML program shall:
 - a. Incorporate policies, procedures, and internal controls reasonably designed to assure compliance with the BSA and its implementing regulations,
 - b. Designate a compliance officer,
 - c. Provide for education or training of appropriate personnel, and
 - d. Provide for independent review to monitor and maintain the adequacy of the program.
- (3) The obligation to establish an AML program applies to an insurance company and not its agents or insurance brokers. However, an insurance company must integrate the company's agents and insurance brokers into its AML program.

4.26.9.11.3.1.1
(11-12-2019)
**Policies, Procedures,
and Internal Controls**

- (1) An insurance company's AML program must incorporate policies, procedures, and internal controls based upon the company's assessment of the money laundering and terrorist financing risks associated with its covered products.
- (2) The program must include policies, procedures, and internal controls to assist the insurance company in identifying transactions that may involve use of the company to facilitate money laundering or terrorist financing. The AML program must include provisions for making reasonable inquiries to determine whether a transaction involves money laundering or terrorist financing, and for refusing to consummate, withdrawing from, or terminating such transactions.
- (3) Internal controls are the insurance company's policies, procedures, and processes designed to detect, prevent, limit, and control money laundering and terrorist financing risks. Internal controls include policies, procedures, and processes for detecting and reporting required transactions and activity.
- (4) The level of the internal controls should be commensurate with the size, structure, risks, and complexity of the insurance company. Internal controls should provide for:
 - a. Effective risk assessment, including periodic updates to the insurance company's risk profile,
 - b. Development and implementation of policies, procedures, and internal controls to ensure compliance with all applicable BSA requirements and mitigation of risks identified by risk assessment,
 - c. Customer due diligence and verification of identity,
 - d. Filing of required reports,

- e. Creation and maintenance of required records,
- f. Responding to law enforcement requests, and
- g. Integration of automated data processing systems into BSA compliance.

4.26.9.11.3.1.2
(11-12-2019)
Compliance Officer

- (1) The insurance company must designate a qualified individual to serve as the BSA compliance officer.
- (2) The BSA compliance officer is responsible for coordinating and ensuring day-to-day BSA compliance and for assuring that:
 - a. The insurance company properly files reports, and creates and maintains records in accordance with the requirements of the BSA,
 - b. The AML program is updated as necessary to reflect current BSA requirements and related guidance, and
 - c. The insurance company provides appropriate training and education to applicable staff.
- (3) While the title of the individual responsible for overall BSA compliance is not important, his or her level of authority and responsibility within the insurance company is critical. The BSA compliance officer may delegate specific duties to other employees, but the officer is responsible for overall BSA compliance.
- (4) The BSA compliance officer should be fully knowledgeable about the BSA and all related regulations. The BSA compliance officer should also understand the insurance company's products, distribution channels, and locations of customers, as well as the potential money laundering and terrorist financing risks associated with those covered products.
- (5) The designation of a BSA compliance officer is not sufficient to meet the regulatory requirement if that person does not have the expertise, authority, or resources to satisfactorily complete the job.

4.26.9.11.3.1.3
(11-12-2019)
Training

- (1) Insurance companies must ensure that appropriate personnel are trained in applicable aspects of the BSA and their own responsibilities under the insurance company's AML program. The AML program must also provide for training in the detection of suspicious transactions to appropriate personnel because the regulations require insurance companies to file SARs.
- (2) At a minimum, the insurance company's training program must provide training for all personnel whose duties require knowledge of the BSA. The training should be tailored to the employee's specific responsibilities. An overview of the BSA requirements typically should also be given to new staff during employee orientation. Additionally, the insurance company must ensure that all appointed agents complete an adequate BSA training program.
- (3) Training should incorporate current developments and changes to the BSA and any related regulations. Changes to internal policies, procedures, processes, and monitoring systems should also be covered during training. Training should reinforce the importance that management places on compliance with the BSA and should ensure that all employees/agents understand their role in maintaining an effective AML program.

- (4) The scope and frequency of the training will depend on the insurance company's risk assessment, which should consider the insurance company's products, distribution channels, and geographic locations of customers. For some insurance companies, based on their risk assessments, annual training for certain employees/agents may not be necessary; for others, more frequent training may be warranted. Examples of money laundering activity and suspicious activity monitoring and reporting can and should be tailored to each individual audience.
- (5) Training and testing materials, the dates of training sessions, and attendance records should be maintained by the insurance company for the examiner to review.

4.26.9.11.3.1.4
(11-12-2019)

Independent Review

- (1) The AML program must provide for an independent review of the program to assess its effectiveness. An officer, employee, or group of employees may conduct the review, so long as none of the reviewers are the designated BSA compliance officer or report directly to the BSA compliance officer.
- (2) The primary purpose of the independent review is to determine the adequacy of the insurance company's AML program, including whether the company is operating in compliance with the requirements of the BSA and the insurance company's own policies and procedures.
- (3) The review should provide a fair and unbiased appraisal of each of the required elements of the insurance company's AML program, including its policies, procedures, internal controls, recordkeeping and reporting functions, and training.
- (4) The review should be based on the insurance company's risks, test the insurance company's risk assessment for reasonableness, and determine the adequacy of the risk mitigation strategies chosen by the insurance company.
- (5) The review should test internal controls and transaction systems and procedures to identify problems and weaknesses and, if necessary, recommend to management appropriate corrective actions. For example, if the program requires that an employee or category of employee should be trained once every six months, then the independent review should determine whether the training occurred and whether the training was adequate.
- (6) The review should include transaction testing to determine if all requirements of the insurance company's AML program have been implemented and if policies, procedures, processes, and internal controls are working appropriately.
- (7) Where applicable, the review should include the insurance company's policies, procedures, and processes for agent relationships, including how the insurance company maintains oversight over agents related to BSA compliance. This includes establishing new agent relationships, monitoring existing relationships, and handling non-compliance by agents, including termination of agent relationships where appropriate.
- (8) The review also should cover all AML program actions taken by, or defined as part of the responsibility of, the designated BSA compliance officer. These actions include, for example, the determination of the level of money laundering risk faced by the business, the frequency of BSA/AML training for

employees, and the adoption of procedures for implementation and oversight of program-related controls and transaction systems.

- (9) The review should be conducted on a periodic basis. The scope and frequency of the review will depend on the insurance company's risk assessment, which should take into account the insurance company's products, distribution channels, and geographic locations of customers. For some insurance companies, based on their risk assessment, an annual review may not be necessary; for others, more frequent review may be warranted.
- (10) The person or persons responsible for conducting the review should document the scope of the review, procedures performed, transaction testing completed, if any, findings of the review, and recommendations to management for corrective actions, if any. After the review, the reviewer or the designated BSA compliance officer should track deficiencies and weaknesses discovered during the review and document corrective actions taken by the insurance company. All the documentation should, as appropriate, be made accessible to government examiners and law enforcement personnel who have authority to examine such documents.

4.26.9.11.3.2 (11-12-2019) **Reporting Suspicious Activity**

- (1) An insurance company must file a SAR if a transaction is conducted or attempted by, at, or through an insurance company, **and** it involves or aggregates funds or other assets of at least \$5,000 **and** the insurance company knows, suspects, or has reason to suspect that the transaction (or pattern of transactions):
 - a. Involves funds derived from illegal activity, or is intended to hide or disguise funds or assets derived from illegal activity, as part of a plan to violate or evade any federal law or regulation, or to avoid any transaction reporting requirement under federal law or regulation,
 - b. Is designed, whether by structuring or other means, to evade any requirements of the BSA,
 - c. Serves no business or apparent lawful purpose, and the reporting company knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, or
 - d. Involves the use of an insurance company's products to facilitate criminal activity.
- (2) An insurance company is responsible for reporting suspicious transactions conducted through its insurance agents and insurance brokers. Accordingly, an insurance company must establish and implement policies and procedures reasonably designed to obtain customer-related information necessary to detect suspicious activity from all relevant sources, including from its insurance agents and insurance brokers, and must report suspicious activity based on such information.
- (3) Factors contributing to the decision to file a SAR include:
 - a. The size, frequency, and nature of the transaction,
 - b. The insurance company's experience with the customer and other individuals or entities associated with the transaction (if any), and
 - c. The norm for such transactions within the insurance company's line of business and geographic area.

- (4) It is important to note that a large transaction is not necessarily suspicious.
- (5) FinCEN's guidelines suggest that insurance companies should report continuing suspicious activity by filing a report at least every 90 days. This will notify law enforcement of the continuing nature of the activity, as well as remind the insurance company that it should continue to review the suspicious activity to determine whether other actions may be appropriate, such as management determining that it is necessary to terminate the relationship with the customer or employee that gives rise to the filing.
- (6) An insurance company may also voluntarily file a SAR on any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but the reporting of which is not required by this section. However, an insurance company is not required to file a SAR to report the submission to it of false or fraudulent information to obtain a policy or make a claim, unless the company has reason to believe that the false or fraudulent submission relates to money laundering or terrorist financing.

4.26.9.11.3.2.1
(11-12-2019)

Timing of a SAR Filing

- (1) A SAR must be filed no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR. Insurance companies may need to review a customer's transactions or account activity to determine whether to file a SAR. If no suspect is identified on the date of initial detection, an insurance company may delay filing a SAR for an additional 30 calendar days to identify a suspect, but in no case must reporting be delayed more than 60 calendar days after the date of the initial detection. The need for a review of customer activity or transactions does not necessarily indicate a need to file a SAR.
- (2) The phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with a customer's normal activity.
 - a. The insurance company's automated monitoring system may flag the transaction; however, this should not be considered initial detection of potential suspicious activity.
 - b. The time for filing a SAR starts when the insurance company, during its review or because of other factors, knows, suspects, or has reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity.
 - c. The review should be completed in a reasonable period. What constitutes a "reasonable period" will vary according to the facts and circumstances of the matter being reviewed and the effectiveness of the suspicious activity monitoring, reporting, and decision-making process of each insurance company.
- (3) For violations requiring immediate attention, in addition to filing a timely SAR, an insurance company should immediately notify, by telephone, an appropriate law enforcement authority. For violations involving suspected terrorist activities, the insurance company should contact FinCEN using its Financial Institutions Hotline (1-866-556-3974).

4.26.9.11.3.3
(11-12-2019)
Form 8300 Filing Requirement

- (1) For a detailed explanation of Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, see IRM 4.26.10, *Form 8300 History and Law*, and IRM 4.26.11, *BSA Examiner Responsibilities for Form 8300 Examinations*.
- (2) Insurance companies must file Form 8300 to report cash received as payment for insurance products if the cash received is in the form of currency (U.S. and foreign coin and paper money) more than \$10,000 in one transaction or two or more related transactions. The exception is when the insurance company receives certain monetary instruments, as explained below, and the insurance company knows that the instrument is being used in the transaction to avoid having to file Form 8300.
- (3) For transactions in which the recipient knows that a monetary instrument(s) is being used to avoid the filing of Form 8300 or for designated reporting transactions, the definition of cash for Form 8300 reporting purposes would also include the following monetary instruments when they aggregate to greater than \$10,000 within a 12-month period (not calendar year):
 - a. Cashier's check having a face amount of \$10,000 or less
 - b. Money order having a face amount of \$10,000 or less
 - c. Bank draft having a face amount of \$10,000 or less
 - d. Traveler's check having a face amount of \$10,000 or less
- (4) The sale of insurance policies, annuity contracts, or similar products offered by insurance companies is not a designated reporting transaction. However, if the insurance company knows that cash equivalents (that is, cashier's checks, money orders, traveler's checks and bank drafts all having a face amount of \$10,000 or less), or cash equivalents in combination with cash, are being used in an attempt to avoid the filing of Form 8300 which would be required if the payment was entirely in the form of currency, then the insurance company is required to file Form 8300.
 - a. For example, an insurance company receives \$11,000 in hundred-dollar bills as payment for an annuity contract. This transaction would be reported on Form 8300. If a customer paid \$10,000 in currency and gave a money order for \$1,000 as payment for an insurance policy, and the insurance company knew that the payment was being made in this fashion to avoid the filing of Form 8300 then a Form 8300 must be filed even though the transaction is not a designated reporting transaction.
 - b. In summary, if an insurance company does not accept cash, but accepts cash equivalents; generally, it is not necessary to file Form 8300 on payments for insurance policies and annuity contracts. An exception would be if the insurance company knew (not just suspected) that the monetary instrument(s) was used to avoid the filing of Form 8300 by the insurance company.
 - c. See the article *Guidance for the Insurance Industry on Filing Form 8300 at [guidance-for-the-insurance-industry-on-filing-form-8300](#)*.
- (5) Form 8300 is required by both Title 26 and Title 31. Under this dual reporting regime, the insurance company is only required to file one Form 8300 for a transaction subject to both IRC 6050I of Title 26 and section 31 USC 5331 of Title 31.

- (6) The regulations governing the filing of Form 8300 under 31 USC 5331 appear at 31 CFR 1010.330, *Reports relating to currency in excess of \$10,000 received in a trade or business*, and for insurance companies at 31 CFR 1025.330, *Reports relating to currency in excess of \$10,000 received in a trade or business*.
- (7) Under IRC 6050I(e), *Statements to be furnished to persons with respect to whom information is required*, any business filing a required Form 8300 must also furnish a written statement to each person identified on the Form 8300 by January 31 of the succeeding calendar year. This is not a requirement of 31 USC 5331 and **must not** be discussed during the Title 31 examination.

4.26.9.11.3.4

(11-12-2019)

Record Retention

- (1) Generally, records must be retained for five years
 - a. All records created for the AML program requirements must be retained for five years.
 - b. Copies of all filed Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, must be retained by the insurance company for five years from the date of the report.
 - c. Copies of all filed SARs and the original or record of any supporting documentation must be maintained for five years from the date of filing the SAR.
- (2) Failure to retain records is considered a record keeping violation.

4.26.9.11.4

(11-12-2019)

Risk Assessment

- (1) Each insurance company should identify and assess the money laundering risks that may be associated with its unique combination of products, services, customers and their geographic locations, distribution channels. Regardless of where risks arise, insurance companies must take reasonable steps to manage them.
- (2) If the insurance company does not have a written risk assessment, the examiner will generally need to conduct more in- depth interviews to determine the insurance company's risk profile.
- (3) The risk-based nature of the AML program requirement is designed to give an insurance company flexibility to tailor its AML program to specific circumstances. For example, the AML program for an insurance company that provides a wide range of covered products and has hundreds of independent agents and brokers would be structured differently from an AML program for an insurance company that offers small face value life policies, no annuity products, and has only captive agents.
- (4) The level and sophistication of analysis will vary from one insurance company to another because of the varying risks of products, distribution channels and customers. The detailed analysis is important because within any type of product, distribution channel, and category of customer, there are varying levels of risk. A detailed analysis will help the insurance company implement appropriate policies, procedures, and processes to mitigate risks.
- (5) An insurance company's risk categories will vary depending on the insurance company. The risk categories below are not exhaustive; however, they provide examples of risk categories the insurance company should consider when performing its risk assessment.

4.26.9.11.4.1
(11-12-2019)
Customer Risk

- (1) Although any customer could conceivably be engaged in money laundering or terrorist financing, certain customers may pose heightened risk because of the nature of their business, occupation, or transaction activity. In assessing customer risk, insurance companies should consider variables such as the type of covered product sought, and the geographic locations involved in the transaction.
- (2) Examples of customers who may pose a higher risk include:
 - a. Customers who seek to purchase a single-premium policy or annuity or to prepay premiums and borrow the maximum cash value or use the policy or annuity as collateral.
 - b. Customers who seek to cancel a life insurance policy during the free-look period or prior to maturity without regard to penalties.
 - c. Customers who demand policy loan or surrender value quickly without regard to penalties.

4.26.9.11.4.2
(11-12-2019)
Product Risk

- (1) Covered products that offer customers more anonymity or involve the handling of high amounts of currency or currency equivalents, may pose greater risk of money laundering or terrorist financing to an insurance company.
- (2) An effective AML program for an insurance company significantly engaged in such activities would include the training of employees to recognize indications of structuring as well as what to do when a potential customer pays (or attempts to pay) premiums with cash. For example:
 - a. All states require a free look period, generally between thirty and sixty days from the date the policy is delivered to the owner. During the free look period, the insurance company must issue a full refund if the customer wishes to cancel, no questions asked. If the customer can terminate the contract during the “free look” or “cooling off” period, he or she will not incur a cost. Cancellation of a policy during this period requires scrutiny, especially if the customer paid the premium in cash, with money orders, or by a wire transfer or the refund check is directed to an apparently unrelated third-party.
 - b. Depositing large sums of cash into an annuity and immediately withdrawing the funds may be a sign of money laundering. One method used for laundering through insurance policies – specifically those used as investment vehicles – is for the money launderer to make one or several overpayments of the policy premiums and then request that any reimbursement be paid to a third-party. The launderer thus continues to retain the policy as an investment product, while laundering funds through the reimbursement of the additional policy contributions.

4.26.9.11.4.3
(11-12-2019)
Geographic Risk

- (1) Identifying geographic locations that may pose a higher risk of money laundering or terrorist financing is essential to an insurance company’s risk assessment. Insurance companies should understand and evaluate the specific risks associated with doing business in, processing transactions for customers from, or facilitating transactions involving certain geographic locations.

- (2) Geographic risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorist financing risks. High-risk geographic locations can be either international or domestic.
- (3) There is no universally agreed definition that prescribes whether a country or geographic area represents a higher risk.

4.26.9.11.4.4
(11-12-2019)

Distribution Channel Risk

- (1) The methods that an insurance company uses to distribute its covered products to its customers should be evaluated when assessing a company's risk. Covered products can be distributed by captive agents, independent agents, banks, and/or broker-dealers.
- (2) One of the major risk exposures of an insurance company is that one of its agents will engage in transactions that put the insurance company at risk for money laundering or other financial crimes.
- (3) A company should categorize the risk involved in each distribution channel it utilizes in selling its covered products.
- (4) The insurance company should have procedures in place to identify those agents that conduct transactions that appear to lack commercial justification or otherwise cannot be supported by verifiable documentation.
- (5) Once high-risk agents are identified, the insurance company should implement procedures to ensure that the transactions those agents conduct are legitimate. In addition, the insurance company should implement procedures for handling non-compliance by its branches/agents (such as agent contract termination).
- (6) Covered products sold through independent agents may pose a greater risk of money laundering than products sold through banks and broker-dealers because banks and broker-dealers are required to have their own AML programs in place.

4.26.9.11.4.5
(11-12-2019)

Operational Risk

- (1) Operational risk is the risk that an insurance company will fail to detect or prevent money laundering or terrorist financing because of inadequate internal processes or systems, or as a result of human failure. Evaluation of operational risk includes:
 - a. The insurance company's systems used to process transactions that utilize transaction dollar limits,
 - b. The frequency of employee and insurance agent turnover,
 - c. The recordkeeping system utilized by the insurance company,
 - d. The covered products issued or underwritten,
 - e. The insurance company's business structure and product distribution channels,
 - f. The involvement of senior management in BSA matters, and
 - g. The insurance company working relationship with insurance agents.
- (2) Management should consider the staffing resources and the level of training necessary to promote adherence with policies, procedures, and processes. For those insurance companies that have taken on a higher-risk BSA/AML profile, management should address this in the risk assessment and provide a more robust program that specifically monitors and controls the higher risks that management and the board have accepted.

4.26.9.11.5
(11-12-2019)
Records Commonly Found

- (1) Other than the AML program and filed BSA reports, records most commonly found include:
 - a. Applications for covered products
 - b. Insurance policies
 - c. Insurance contracts

4.26.9.11.6
(11-12-2019)
Title 31 or Title 26 Exam

- (1) Examinations of insurance companies must be started under Title 31 because they have an AML program requirement under Title 31 and Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, filing requirements under both Titles 26 and 31. This allows the examination to cover the determination of whether their AML program is adequate and to examine compliance with the Form 8300 filing requirements.
- (2) For example, IRS is conducting a Title 31 examination of an insurance company that is required to have an AML program under 31 CFR 1025.210, *Anti-money laundering programs for insurance companies*. During the examination of the AML compliance program, the examiner identifies delinquent Form(s) 8300 because of an inadequate AML program or a failure to implement the AML program. The failure to timely file a complete and correct Form 8300 is a violation of 31 CFR 1027.330, *Reports relating to currency in excess of \$10,000 received in a trade or business*. It is also a violation of 26 CFR 60501-1, *Returns relating to cash received in trade or business, etc.*
- (3) There is no prohibition against using information acquired in a Title 31 exam in a Title 26 exam.
- (4) When an insurance company has a requirement under Title 31 for an AML compliance program and under Titles 26 and 31 to file a Form 8300, the BSA examiner must notify the company, up-front, that it is subject to both Title 26 and Title 31 and the examination may cover both sections of the law.
- (5) The current Form 8300 Lead Sheet is designed so it can be used to determine compliance with Form 8300 requirements under either section of the law. The examination steps to determine a company's compliance with the Form 8300 requirements remain the same no matter under which section of the law the examination is conducted.
- (6) There is no examination step that requires an examiner to review tax return information or IDRS to determine Form 8300 compliance. It is only at the end of the Form 8300 examination, when processing the penalty case file under Title 26 that ERCS and IDRS need to be accessed.
- (7) If an insurance company case is assigned as a Form 8300 Title 26 exam and the BSA group manager and examiner, prior to contacting the company, determine the examination should be initiated under Title 31, the case may be surveyed.
 - a. Survey the case and return it to BSA Exam Case Selection (ECS).
 - b. BSA ECS will record the survey. It will then evaluate the company for a Title 31 examination using only sources available for Title 31 cases. BSA ECS will select the case for Title 31 examination based on this evaluation

- only. If appropriate, BSA ECS will then assign the case as a Title 31 examination. If possible, the case should be assigned to a group different from the surveying group.
- c. If possible the BSA group manager should assign the Title 31 case file to an examiner different from the examiner involved in the surveyed case.
 - d. If it is impossible to reassign, the BSA examiner should wait a minimum of 30 days before contacting the company so that there is a separation as complete as possible from the Title 26 case information.
- (8) For a Title 26 Form 8300 examination, BSA ECS uses tax return information to identify entities subject to Form 8300 filing requirements, and to build and grade the cases. The disclosure laws under IRC 6103, *Confidentiality and disclosure of returns and return information*, apply throughout the entire Title 26 examination process.
- a. If a Form 8300 examination is started under Title 26 the disclosure rules under IRC 6103 apply and the information cannot be used in a Title 31 exam without securing a related statute determination. The examiner must secure a related statute determination, signed by the Territory Manager, prior to addressing any Title 31 issues.
 - b. For example, an insurance company is assigned for a Form 8300 examination under Title 26. During the examination, the examiner determines that the company underwrites, and issues covered products. Because the examination has already been started, it is not possible to survey the Title 26 case. The Title 31 information can only be used if a related statute determination is made. See IRM 4.26.14, *Bank Secrecy Act, Disclosure*, for the procedures for a related statute determination.
 - c. If an examination is opened under Title 26 the examiner cannot ask the company any questions related to the BSA such as questions about their AML compliance program.

4.26.9.11.7
(11-12-2019)
**Title 31 Examination
Procedures**

- (1) An effective risk-based BSA examination consists of the following phases:
- a. Pre-Plan
 - b. Setting the scope and depth of the examination
 - c. Interview - Onsite, walk through of the business, and interview of the appropriate personnel
 - d. Evaluation of the AML program to determine if it has been implemented and is effective
 - e. Examination of the books and records
 - f. Transaction testing
 - g. Developing conclusions and finalizing the examination
- (2) The techniques described in this section are intended as a guide and are not all-inclusive.
- (3) The Title 31 Lead Sheet Package and the Form 8300 Lead Sheet Package are available on the BSA SharePoint and should be used to guide the administrative aspects of the examination.
- (4) An insurance company's AML program must be commensurate with their level of risk. The company should not necessarily take any single indicator as evidence of lower or higher risk. The risk assessment process should weigh several risk factors including:

- a. Geographic locations
- b. Customers
- c. Product
- d. Services
- e. Distribution Channels
- f. Operational risk

4.26.9.11.7.1
(11-12-2019)

Pre-Plan

- (1) Prior to a Title 31 examination the examiner must:
 - a. Review the FinCEN Query system for any Form 8300 filed by the company, and CTRs and SARs filed on the company, its owners, and employees.
 - b. Review prior Title 31 examination results.
 - c. Check for previous Title 31 penalties.
- (2) The examiner must use the Lead Sheet packages for Title 31 and Form 8300 and the Primary Case Folder required records. These are available on the BSA SharePoint.
 - a. Set up Form 4318, *Examination Workpapers Index*.
 - b. Begin the Form 9984, *Examining Officer's Activity Record*.
 - c. Set up Workpapers 105 – 125 from Planning to Close through GM Concurrence.
- (3) Due to the nature and complexity of insurance companies' systems and the volume of records, the BSA examiner will use a CAS in conducting most (if not all) insurance exams. Depending on the size of the company, the volume of the transactions, and the complexities involved, the audit team may include one or more BSA examiners, a CAS, and support personnel.
 - a. BSA examiners should request a CAS in time for the CAS to be present at the initial interview as this will help to ensure that the exam runs expeditiously. To request a CAS, visit <https://srs.web.irs.gov/>.
- (4) The examiner should become familiar with the common practices of the insurance industry. Below are some associations and research tools the examiner should be aware of:
 - a. National Association of Insurance Commissioners (NAICS) - <https://www.naic.org/>
 - b. International Association of Insurance Supervisors (IAIS)- <http://www.iaisweb.org/home>
 - c. Office of Foreign Assets Control (OFAC) - <https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx>
 - d. Criminal Investigation - <https://www.irs.gov/compliance/criminal-investigation/criminal-enforcement>
 - e. Fraud- <https://www.irs.gov/compliance/criminal-investigation/types-of-fraudulent-activities-general-fraud>
 - f. Internal Revenue Bulletins (IRB) - <https://www.irs.gov/irb>
 - g. Financial Crimes Enforcement Network - <https://www.fincen.gov/>
 - h. Code of Federal Regulations (CFR) <https://archive.opm.gov/fedregis/>
 - i. The BSA SharePoint Title 31 Issues and Industries site may have background information and links to other internet sites

- (5) It is important to have a comprehensive understanding of the different divisions of the insurance company that is under examination. There are several common divisions of insurance companies that are involved in the issuance of a covered product.
- (6) Insurance companies generally separate their different divisions in several ways by either function or by product. For example, if an insurance company differentiates the major divisions by the work that division performs, the divisions are separated by function. However, if the insurance company delegates certain responsibilities to the departments that handle the administration of certain products, the insurance company separates the divisions by line of business.
- (7) Examiners will need to determine how the following functional areas are covered by the AML program:
 - a. Underwriting Department
 - b. Actuarial Department
 - c. Customer Service
 - d. Claims Administration
 - e. Annuity Administration
 - f. Accounting Department
 - g. Information Technology
 - h. Legal Department
 - i. Compliance Department
 - j. Operations Department
 - k. Marketing Department
 - l. Audit Department
 - m. Risk Management
 - n. Finance Department

4.26.9.11.7.2
(11-12-2019)
Initial Contact

- (1) It is the examiners responsibility to identify the contact person and to inform the company of the upcoming BSA examination. Insurance companies are not sent Letter 1052, *Bank Secrecy Act Requirements Notification Letter*, or an equivalent.
- (2) Because most insurance companies are designated as LB&I cases, the BSA examiner must inform the BSA Exam Group Manager of the date of the pre-audit conference (as far as possible in advance of the opening conference). The BSA Exam Group Manager will submit a request to the BSA ECS Title 31 Program Analyst to identify the LB&I case manager assigned to the case and provide the contact information to the BSA Exam Group Manager. The BSA Exam Group Manager will reach out to the LB&I case manager to discuss the logistics on conducting the Title 31 exam.
- (3) All initial taxpayer contacts must be made by mail to combat phone scams, phishing, and identity theft.
- (4) Use Letter 4155, *Insurance Appointment Letter*, for examinations selected for Title 31 examination.
- (5) After mailing the initial contact letter, and there is no response, the BSA examiners should wait two weeks before calling.

- (6) The purpose of the initial phone contact, with the insurance company, is to set up an opening conference meeting. The initial contact is usually made with one of the officers of the company and/or the compliance officer.
 - a. Making the contact by telephone allows the examiner to schedule the appointment at a mutually agreed upon time and place.
 - b. At this time, the examiner should briefly explain the purpose of the BSA examination as well as the examination process.
 - c. The examiner should confirm the type of covered products sold and the type of books/records that are maintained to prepare a more appropriate initial information document request.
 - d. The examiner should also determine the person(s) to be present at the opening conference.
- (7) Once the examiner has set the date for the opening conference, he/she should confirm the appointment using the official appointment letter which will state the current or revised date, time, and place of the meeting.
 - a. Use Letter 4155, *Insurance Appointment letter*, for examinations selected for Title 31 examination.
 - b. **Do not use** Letter 2277 as this is used when a Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, examination is being performed under Title 26.
- (8) Plan the initial contact using Workpaper #130 (of the appropriate package), *Initial Contact Check Sheet*, and record the information on it during the contact itself.
 - a. Set up Workpaper #135, *Initial Appointment Agenda*.
 - b. As an AML Compliance examination under Title 31, complete *AML Compliance Program Lead Sheet Title 31* (#140) as well as, *Form 8300 Policy Procedures Internal Controls Lead Sheet* (# 140).
- (9) Prepare the initial Form 4564, *Information Document Request*, using the information recorded during the telephone conversation with the company on Workpaper #130, *Initial Entity Contact Check Sheet*. Include the IDR with the appointment letter. At a minimum, the first document request should be issued by the end of the opening conference. Request these items up-front as applicable (this list is not all inclusive):
 - a. Name(s), title(s), and contact information for the BSA/AML compliance officer and the Information Technology (IT) manager.
 - b. A copy of the AML compliance program in advance of the appointment. The BSA examiner should review copies of the AML program including but not limited to policies and procedures, BSA training, monitoring, and reporting policies and procedures.
 - c. Copy of the risk assessment.
 - d. An organizational chart showing direct and indirect reporting lines.
 - e. A list of acronyms used to describe their policies, procedures, computer systems, and departments along with their definitions.
 - f. Copy of the independent review of their AML compliance program.
 - g. Copies of all internal audits or external audits by regulators. The BSA examiner should note any inconsistencies reported and corrective actions recommended.
 - h. Company's booklets/pamphlets (covered goods only).

- i. A download of computer records to be available at the initial appointment.
- j. Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, records required under Title 31. Do not request evidence of compliance with the customer notice requirements that are only required in IRC 6050I(e), *Statements to be furnished to persons with respect to whom information is required*, because this is a Title 31 exam.

- (10) The examiner may mail or hand-deliver the appointment letter and the IDR to the business.

4.26.9.11.7.3
(11-12-2019)

Exam Scope and Depth

- (1) Determining the scope of an examination is the process by which issues are selected that warrant examination. Base the scope of the examination on the facts and circumstances of each case. Consider factors such as inadequate records, poor internal control, and unusual currency flow. Select issues so that all items necessary for a substantially proper determination of the BSA requirements are considered. Exercise proper judgment throughout the examination process to expand or contract the scope as needed.
- (2) The depth of the examination is the extent to which an issue is developed or examined. The depth of the examination demonstrates the degree of intensity and thoroughness applied to decide as to the correctness of an item. Determining the depth of the examination will help estimate the time required to complete the examination. When determining the depth of the examination, consider the:
 - a. Risk assessment
 - b. AML program
 - c. Type of evidence/documents available
 - d. Complexity of transactions
 - e. Independent review
 - f. Training
- (3) The scope and depth of the BSA examination depend upon the facts and circumstances in each case. The scope and depth of an insurance company examination should initially include six months of a 12-month examination period. The six months do not have to be contiguous.
- (4) To facilitate understanding the insurance company's risk profile and to establish the scope of the BSA examination, complete the following steps, in conjunction with the review of the company's BSA/AML risk assessment:
 - a. Review prior examination reports, related workpapers, and management's responses to previously identified BSA violations, deficiencies, and recommendations.
 - b. Review news articles concerning or pertaining to the company and its management.
 - c. Review internal or external independent reviews and workpapers for BSA compliance, as necessary, to determine the comprehensiveness and quality of audits, findings, and management responses and corrective actions. The independent reviewer's scope, procedures, and qualifications provide valuable information on the adequacy of the AML compliance program.
 - d. Submit subsequent IDRs to the company if necessary.
- (5) If after examining six months of records, it is determined that the insurance company has implemented an effective AML compliance program designed to

ensure BSA compliance, the transaction testing period can be limited to the six months examined. If no serious violations or deficiencies were detected during this period, the examination can be closed. If the insurance company lacks an adequate compliance program or the examiner detects problems during the six-month review period, the examination period should be expanded appropriately.

- (6) If the insurance company has been previously examined and only minor deficiencies were noted, a more limited scope examination should be considered. See IRM 4.26.6, *Bank Secrecy Act Examiner Responsibilities*, for more information on Scope and Depth.

4.26.9.11.7.4 (11-12-2019) Interview

- (1) The examiner must conduct the examination at the place of business.
- (2) The examiner should interview managers, employees, and insurance agents who:
 - a. Handle day-to-day transactions,
 - b. Have direct contact with receiving and handling premium payments,
 - c. Are responsible for handling policy loan requests or policy liquidation requests,
 - d. Are responsible for filing Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, and SARs,
 - e. Review day-to-day BSA compliance, or
 - f. Are responsible for implementing or supervising the AML program.
- (3) Record the initial interviews on Workpaper 205 of either Lead Sheet.
- (4) The examiner should explain the examination process and specifically state that the examination is NOT an income tax examination.
- (5) Because the business is selected for a Title 31 examination and is also subject to the Form 8300 filing requirements under both Title 31 and Title 26, the BSA examiner must:
 - a. Advise the company that the Form 8300 is a dual-purpose form required under both Title 31 and Title 26.
 - b. Also, advise that information acquired during the Title 31 examination may be used to determine compliance with the related rules under Title 26.
 - c. Fully document this advice on Form 9984, *Examining Officer's Activity Record*, as follows: "I advised XXX that the Form 8300 is a dual-purpose form required under both Title 31 and the IRC. I further advised that information acquired during this examination may be used to determine compliance with the related rules under both titles."
- (6) Discuss the company's compliance under Title 31, which should include the AML compliance program, management structure, BSA risk assessment, Form 8300 filings, and the level and extent of automated BSA/AML systems.
- (7) During the interview, the examiner should ascertain and/or verify:
 - a. The TIN of the business,
 - b. The names and titles of officers or employees who handle cash transactions and are responsible for filing Form 8300,

- c. The owner/officer's knowledge of the BSA as it relates to insurance companies,
 - d. Who handles received cash, prepares bank deposit slips, and makes the bank deposits,
 - e. The number and types of bank accounts used,
 - f. The type of records maintained on transactions required to be reported on Form 8300,
 - g. Secure a copy of the AML program,
 - h. Determine who has been designated as the compliance officer and the BSA knowledge of compliance officer,
 - i. Training of employees on the BSA, the AML compliance program, and filing Form 8300,
 - j. If an independent review was conducted secure a copy and the results,
 - k. The internal controls of the company for cash transactions,
 - l. Whether the company has filed any Form 8300,
 - m. Procedures used by the company to ensure that the information contained in the Form 8300 was complete and correct, (For example, did the company verify the identity of the person from whom the cash was received by a driver's license, passport, or other official document)
 - n. The company's membership in various types of trade associations, and
 - o. Related entities.
- (8) The examiner needs to understand the company's process and workflow and develop an adequate understanding of the processing environment – the process, related controls, and key roles and responsibilities. This is critical to performing the BSA examination. This understanding is achieved through two documentation techniques - process narratives and flow charts. These techniques help the examiner understand the insurance company's processes.
- a. The objective of process narratives and flow diagrams is to generate an accurate representation of how work is performed and how transactions flow.
 - b. Typically, creating this type of documentation involves individuals at various levels of responsibility walking through processing steps and discussing related documents, responsibilities, and/or outputs.
 - c. The examiner will need to pay close attention to the flow of payments (cash/cash equivalent), products (covered goods), monitoring of the company's agents, and paper work.
- (9) Narrative and process flow tools allow the examiner to organize, describe, and graphically depict the results of:
- a. Reviewing policy and procedure manuals,
 - b. Discussing the process with key employees through inquiry,
 - c. Performing a process walk through of sub-processes using samples,
 - d. Considering key inputs and outputs to a process, and
 - e. Lines of responsibility for individual employees and departmental roles.
- (10) Condense the process information into manageable narratives and process flows that incorporate all the key steps, processing responsibilities, documents, and actions. Map key risks and controls on the process flow diagram to indicate when, by whom, and how controls mitigate risks.
- (11) Accurate, complete documentation of the company's process (as it pertains to covered goods) serves as a baseline for testing the risk assessment, internal controls, and effectiveness of the AML compliance program.

- (12) Do not ask about compliance with the customer notice requirements because this is not a requirement under Title 31 and this is a Title 31 exam.
- (13) The interview and inspection of records must be solely for the Title 31 BSA examination, which includes Form 8300 filing requirements under Title 31. No inquiries should be made as to the filing of other returns required by Title 26 or whether a specific item is reported on any such returns. The latter inquiries could constitute the opening of an income tax examination.
- (14) Refer to IRM 4.26.11, *BSA Examiner Responsibilities for Form 8300 Examinations*, for additional questions relating to knowledge and intent.
- (15) The examiner should advise the company that information from their records may be used for any tax matter permitted by the Internal Revenue Code.

4.26.9.11.7.5 (11-12-2019) **Assessing Risk**

- (1) Develop an initial examination scope and plan commensurate with the preliminary BSA/AML risk profile.
 - a. The scope and planning process ensure the examiner is aware of the insurance company's AML program, compliance history, and risk profile (for example, products, distribution channels, customers, geographic locations, operations).
 - b. While the examination plan may change at any time because of on-site findings, the initial risk assessment assists the examiner in establishing a reasonable scope/depth for the BSA examination.
- (2) Review the insurance company's risk assessment.
 - a. Determine whether the insurance company has addressed all risk-related issues, including introduction of any new products, customers, agent relationships, other operational risks, distribution channels, and geographic locations of customers.
 - b. Determine whether the insurance company's process for periodically reviewing and updating its BSA/AML risk assessment is adequate.
 - c. If the insurance company has not developed a risk assessment, or if the risk assessment is inadequate, complete a preliminary risk assessment.
- (3) The examiner should consider any differences between their and the insurance company's risk assessment.
- (4) The examiner should focus the examination on the aspects of the insurance company that are the highest risk.

4.26.9.11.7.6 (11-12-2019) **Examining the AML Program**

- (1) The examiner should follow the exam steps outlined in the *AML Compliance Program Lead Sheet Title 31* (#140) and the *Form 8300 Exam Lead Sheet* (#300).
- (2) Review the AML program to ensure it is commensurate with the company's risk and contains:
 - a. A system of internal controls to ensure ongoing compliance
 - b. Independent testing of the BSA compliance program
 - c. A designated person or persons responsible for managing BSA compliance (BSA compliance officer)

- d. Training for appropriate personnel
 - e. Includes procedures for monitoring their insurance agents
- (3) Determine whether the insurance company has adequately identified the risks within its operations and incorporated the risks into the AML compliance program. To mitigate these risks, the company should adopt policies, procedures, and processes that include:
- a. Identification of high-risk activities.
 - b. Mitigation strategies to manage high-risk activities.
 - c. Recordkeeping requirements.
- (4) Determine whether the AML compliance program includes policies, procedures, and processes that:
- a. Identify high-risk operations (covered products, customers, distribution channels, and geographic locations); provide for periodic updates to the company's risk profile; and provide for an AML compliance program tailored to manage risks.
 - b. Identify a person or persons responsible for BSA/AML compliance.
 - c. Provide for program continuity despite changes in management or employee composition or structure.
 - d. Meet all regulatory requirements and recommendations for BSA compliance and provide for timely updates to implement changes in regulations or changes to the internal policies and procedures.
 - e. Implement risk-based policies for obtaining relevant customer information.
 - f. Monitor the insurance agents.
 - g. Identify and monitor for suspicious activity that reasonably relates to the insurance company's products, distribution channels, and customer activities.
 - h. Identify reportable transactions and accurately file all required reports, Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*.
 - i. Provide sufficient controls and monitoring systems for the timely detection of high-risk activity and include procedures for dealing with high-risk activity.
 - j. Provide for adequate supervision of employees and appropriate persons that handle currency transactions, complete reports, monitor for suspicious activity, or engage in any other activity covered by the BSA and its implementing regulations.
 - k. Train appropriate personnel to be fully aware of their responsibilities under the BSA regulations and internal policy guidelines.
- (5) Identify and document the transaction cycle of the products of the insurance company through discussion and observation. This process should answer the Who, What, Where, and Why of the insurance company's activities so the examiner can evaluate the appropriateness of risk-based internal controls, policies, and procedures implemented by the insurance company.
- (6) Identify, document, analyze, and evaluate the day-to-day system of monitoring transactions for BSA reporting requirements. Determine whether monitoring systems are appropriate based on the risks of the insurance company.
- (7) Review the insurance company's policies and procedures for monitoring/oversight of the activities of its appointed agents. Ensure that the insurance company has appropriately monitored transactions of agents which are identi-

fied as having the highest risk. The insurance company is ultimately responsible for the compliance of all its appointed agents.

- (8) Determine whether the BSA/AML review is independent, such as performed by a person (or persons) who is not part of the company's BSA/AML compliance staff, not the compliance officer, or does not report to the BSA compliance officer. Evaluate the qualifications of the person(s) performing the independent review to assess whether the company can rely upon the findings and conclusions. Validate the reviewer's reports and workpapers to determine whether the company's independent review is comprehensive, accurate, adequate, and timely.
- (9) The independent review should address the following:
 - a. The overall integrity and effectiveness of the AML compliance program, including policies, procedures, and processes.
 - b. BSA risk assessment.
 - c. BSA reporting and recordkeeping requirements.
 - d. Agent oversight.
 - e. Procedures for obtaining relevant customer-related information
 - f. Appropriate transaction testing, with emphasis on high-risk operations (goods, service, customers, and geographic locations).
 - g. Training adequacy, including its comprehensiveness, accuracy of materials, the training schedule, and attendance tracking.
 - h. The integrity and accuracy of management information systems (MIS) used in the AML compliance program.
- (10) Determine whether the independent review included a review of high-risk activity monitoring systems and an evaluation of the system's ability to identify unusual activity. Ensure through a validation of the reviewer's reports and workpapers that the independent review:
 - a. Reviewed policies, procedures, and processes for monitoring high-risk activity.
 - b. Evaluated the system's methodology for establishing and applying expected activity or filtering criteria.
 - c. Included a review of suspicious activity monitoring systems and an evaluation of the system's ability to identify unusual activity.
 - d. Evaluated the system's ability to generate monitoring reports.
 - e. Determined whether the system's filtering criteria are reasonable.
 - f. Determined whether previously identified deficiencies have been corrected.
- (11) Determine whether management has designated a person or persons responsible for the overall AML compliance program.
 - a. Determine whether the BSA compliance officer has the necessary authority and resources to execute all duties.
 - b. Assess the competency of the BSA compliance officer and his or her staff, as necessary.
 - c. Determine whether the BSA compliance area is sufficiently staffed for the company's overall risk level, size, and BSA compliance needs. In addition, ensure that no conflict of interest exists, and that staff is given adequate time to execute all duties.

- (12) Determine whether the following elements are adequately addressed in the training program and materials:
 - a. The importance the board of directors and/or senior management place on ongoing education, training, and compliance.
 - b. Comprehensiveness of training, considering specific risks of the covered products.
 - c. Training of appropriate personnel.
 - d. Frequency of training.
 - e. Documentation of attendance records and training materials.
 - f. Coverage of the company's policies, procedures, processes, and new rules and regulations.
 - g. Coverage of different forms of money laundering and terrorist financing as it relates to identification and examples of high-risk activity.
 - h. Penalties for noncompliance with internal policies and regulatory requirements.
 - i. As appropriate, conduct discussions with employees and agents to assess their knowledge of BSA/AML policies and regulatory requirements.
- (13) After reviewing the company's AML program, document an evaluation of the program. Revisit the initial examination plan to determine whether any strengths or weaknesses identified during the interviews, walkthrough of the business, and review of the company's AML program warrant adjustments to the initial planned scope. Document and support any changes to the examination scope and then proceed to the additional examination procedures.

4.26.9.11.7.7
(11-12-2019)
**Examining for
Suspicious Activity
Monitoring and
Reporting**

- (1) The focus of the examination should be evaluating an insurance company's overall policies, procedures, and processes to identify, monitor, research, and report suspicious activity.
- (2) Policies, procedures, and internal controls should identify the person(s) responsible for the identification, research, and reporting of suspicious activities. Appropriate policies, procedures, and processes should be in place to monitor and identify unusual activity.
 - a. Monitoring systems typically include some combination of employee/agent identification, manual systems, and automated systems. The insurance company should ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities, considering the insurance company's overall risk profile and the volume of business. After thorough research and analysis, decisions to file or not to file a SAR should be documented.
 - b. The monitoring process may involve review of daily reports, reports that cover a period (such as rolling 30-day reports, monthly reports), or both types of reports.
 - c. The type and frequency of reviews and resulting reports should be commensurate with the insurance company's risk profile and should appropriately cover its high-risk transactions, services, customers, and distribution channels.
 - d. The insurance company should have policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity, which may include senior management of the insurance company. Upon identification of unusual activity, additional research is typically conducted.

- e. The insurance company will generally have to make two decisions once it becomes aware of unusual activity related to a transaction: (1) Whether to file a SAR, and (2) Regardless of whether a SAR is filed, whether to monitor the customer going forward.
 - f. The insurance company could decide after reviewing all information that the transaction does not warrant reporting. Notwithstanding that decision, the insurance company could decide that it is appropriate to monitor the customer for the same or similar transactions in the future. The insurance company could plan to revisit the question of whether to file a SAR if the customer conducts such transactions in the future. Alternatively, the insurance company could make the decision that it will file a SAR if such transactions continue without a reasonable explanation.
 - g. Insurance companies are encouraged to document SAR decisions. Thorough documentation provides a record of the SAR decision-making process, including final decisions not to file a SAR. However, due to the variety of systems used to identify, track, and report suspicious activity, as well as the fact that each suspicious activity reporting decision will be based on unique facts and circumstances, this documentation may not always look the same.
 - h. It is the responsibility of the insurance company to determine the sufficiency and adequacy of its documentation for the SAR decision-making process.
- (3) Review the insurance company's policies, procedures, and processes for identifying, researching, and reporting suspicious activity. Determine whether they include the following:
- a. Lines of communication for the referral of unusual activity to appropriate personnel,
 - b. Designation of individual(s) responsible for identifying, researching, and reporting suspicious activities,
 - c. Monitoring systems used to identify unusual activity,
 - d. Procedures to ensure the timely generation of, review of, and response to reports used to identify unusual activities,
 - e. Procedures for documenting decisions not to file a SAR,
- Note:** There is no affirmative requirement to document decisions not to file SARs, so an insurance company should not be automatically criticized or cited for failing to have such documentation. The lack of documentation, however, may make it far more difficult to determine the decision process for not filing a SAR.
- f. Procedures for determining whether to refuse services to customers for attempting a suspicious transaction or engaging in continuous suspicious activity,
 - g. Procedures for completing, filing, and retaining SARs and their supporting documentation, and
 - h. Procedures for reporting SARs to senior management.
- (4) Evaluate the insurance company's policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity.
- a. Determine whether policies, procedures, and processes require appropriate research when monitoring and reporting unusual activity.

- b. The decision to file a SAR is an inherently subjective judgment. Focus on whether the insurance company has an effective suspicious activity reporting decision-making process, not on decisions about whether to file individual SARs.
 - c. Review individual SAR filing decisions to test the effectiveness of the suspicious activity monitoring, reporting, and decision-making process. In those instances where the insurance company has an adequate, established suspicious activity reporting decision-making process, followed existing policies, procedures, and processes, and determined not to file a SAR, the insurance company should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.
- (5) Review SAR activity. Have there been significant changes in the volume or nature of SARs filed? Investigate the reason(s) for these change(s).
 - a. If there is a significant historical change in the number and/or nature of SARs filed, interview responsible personnel to determine whether the changes are appropriate. Determine whether management is aware of trends identified.
 - b. Review the nature of SARs filed.
 - c. Determine whether management has a process to monitor the number and nature of SARs filed and the ability to strengthen controls and processes when necessary, based on this information.
- (6) Based on a risk assessment, prior examination reports, policies, procedures, internal controls, and the insurance company's preliminary examination findings, sample the SARs. Review the quality of SAR data to assess the following:
 - a. SARs contain accurate information
 - b. SARs were filed within the required timeframe
 - c. SARs were filed (verification of filing through the FinCEN Query)
- (7) Sample specific customer transactions to review the suspicious activity monitoring reports and decisions to file or not file a SAR.
- (8) Based on the risks, consider reviewing all covered products offered by the insurance company to determine if transactions are being structured by using a variety of products.
- (9) Transaction testing of suspicious activity monitoring systems and reporting processes is intended to determine whether the insurance company's policies, procedures, and processes are adequate and effectively implemented.
 - a. Transaction testing of suspicious activity monitoring systems and reporting processes should be based on the risks identified during the review of the insurance company's risk assessment as well as the policies, procedures, and internal controls implemented by the insurance company to mitigate risks, identify suspicious activity, and report suspicious activity.
 - b. The examiner must document the factors used to select samples and maintain a list of the transactions sampled.
 - c. Review the selected transactions for unusual activity. If the examiner identifies unusual activity, review customer information for indications that

- the activity is typical for the customer (in other words, the sort of activity in which a policyholder is normally expected to engage).
- d. From the results of the sample, determine whether the insurance company's manual or automated suspicious activity monitoring system effectively detects unusual or suspicious activity.
 - e. Identify the underlying cause of any deficiencies in the monitoring systems (such as inappropriate filters, insufficient risk assessment, or inadequate decision-making).
- (10) For transactions identified as unusual, discuss the transactions with management and appropriate personnel involved in the transaction where applicable.
- a. Determine whether the personnel demonstrate knowledge of the customer and the unusual transactions.
 - b. After examining the available facts, determine whether management knows of a reasonable explanation for the transactions or if an apparent reporting deficiency exists.
 - c. Based on the response, consider expanding the scope of the examination.
- (11) Based on examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with monitoring, detecting, and reporting suspicious activity.

4.26.9.11.7.8
(11-12-2019)
**Examining for
Reportable Form 8300
Transactions**

- (1) Examine the appropriate documents and accounting records to determine if:
- a. Transactions occurred which involved the receipt of reportable cash in excess of \$10,000.
 - b. There are consecutive or related reportable transactions in excess of \$10,000.
 - c. Multiple covered products were purchased at the same time but recorded as separate purchases.
 - d. Any Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, were filed on such transactions.
- (2) Watch for payments in the form of sequentially numbered checks, multiple checks from the same account drawn on the same date, checks with no identified payer, payments drawn on a bank located in a foreign country or far from the payer.
- (3) Use of money orders and cashier's checks less than \$3,000 could be an indication of structuring. Watch for bulk amounts of sequentially numbered U.S. money orders and traveler's checks.
- (4) For any transaction the examiner believes was reportable and a Form 8300 was not filed, the examiner should copy the receipts, contracts, and any other supporting documentation needed. The examiner should record the location of the original records pertaining to these transactions.
- (5) For any transaction the examiner believes was reportable and a Form 8300 was not filed, the examiner should copy the receipts, contracts, and any other supporting documentation needed. The examiner should record the location of the original records pertaining to these transactions.

- (6) There may be a need, on a case-by-case basis, to interview the customer to obtain all the facts as required to develop the issues.
- (7) If a business uses a computerized system, the examiner must test the system to ensure its integrity before relying upon such records for the Form 8300 examination. For example, the examiner can run sample data through the system to see how the system performs.
- (8) Do not address the customer notification requirement of IRC 6050I(e), *Statements to be furnished to persons with respect to whom information is required*, because this is a Title 31 examination and there is no customer notification requirement under Title 31.

4.26.9.11.7.9

(11-12-2019)

Transaction Testing

- (1) The examiner must conduct transaction testing to ensure the AML has been effectively implemented. Transaction testing is another important factor in forming conclusions about the integrity of the insurance company's overall controls and risk management processes.
- (2) Perform transaction testing, using a sample of transactions, to evaluate the adequacy of the insurance company's compliance with regulatory requirements, to determine the effectiveness of its policies, procedures, and processes, and to evaluate suspicious activity monitoring systems.
- (3) Transaction testing should be risk-based. The extent of transaction testing and activities conducted is based on various factors, including the examiner's judgment of risks, controls, and the adequacy of the independent testing.
- (4) Once on-site, the scope of the transaction testing can be adjusted to address any issues or concerns identified during the pre-planning, the interviews, and walk through of the company.
- (5) Testing should be sufficient to assess the degree of risk exposure in a function or activity.
 - a. When risk management processes or internal controls are considered inappropriate, such as when there is an inadequate segregation of duties or when onsite testing determines that necessary processes are inadequate or absent, perform additional transaction testing.
 - b. Additionally, the examiner should perform substantial on-site transaction testing if it appears an insurance company's management is being less than candid, has provided false or misleading information, or has omitted material information.
- (6) If the insurance company uses a computerized system, the examiner must test the system to ensure its integrity before relying on it. The examiner, with the assistance of a CAS if needed, can run a sample of transactions through the system to determine how it handles transactions and if the filtering criteria identify reportable or potentially suspicious transactions.
- (7) Use transaction testing to identify transactions that may be suspicious in nature, do not make business sense, or appear to be conducted in a manner to avoid the Form 8300 reporting requirements. Some examples include:
 - a. Borrowing against the cash surrender value of permanent life insurance policies.
 - b. Selling units in investment-linked products (such as annuities).

- c. Using insurance proceeds from an early policy surrender to purchase other financial assets.
 - d. Buying policies that allow the transfer of beneficial interests without the knowledge and consent of the issuer (such as secondhand endowment and bearer insurance policies).
 - e. Purchasing insurance products through unusual methods such as currency or currency equivalents.
 - f. Buying products with insurance termination features without concern for the product's investment performance.
 - g. A single transaction structured as multiple transactions of less than \$10,000.
 - h. Transactions in excess of \$10,000 where cash and non-cash payments appear to be combined to avoid the filing requirements.
 - i. A pattern or series of transactions of less than \$10,000 conducted over a relatively short period by or for the same person.
- (8) Document the decision regarding the extent of transaction testing to conduct and the activities where it is to be performed, as well as the rationale for any changes to the scope of transaction testing that occur during the examination.
- (9) Determine whether an activity is unusual or suspicious.
- (10) Depending on the initial findings, the examiner may need to expand the scope and/or depth of the review to include additional periods.
- (11) Based on examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes.

4.26.9.11.7.10
(11-12-2019)
**Verifying Agent
Monitoring**

- (1) The BSA examination must include a review of how the insurance company monitors and trains its agents.
- (2) The BSA insurance regulations apply only to insurance companies; there are no independent obligations for brokers and insurance agents.
- a. However, the insurance company is responsible for the conduct and effectiveness of its AML compliance program, which includes insurance agent and broker activities.
 - b. Insurers must integrate agents and brokers into their AML programs and ensure they are sufficiently trained.
- (3) Insurance companies offer covered products through appointed agents. One of the major risk exposures of an insurance company is that one of its agents will engage in transactions that put the insurance company at risk for money laundering or other financial crimes.
- a. To reduce this risk, the insurance company should have procedures in place to identify those agents that conduct transactions that appear to lack commercial justification or otherwise cannot be supported by verifiable documentation.
 - b. Once high-risk agents are identified, the insurance company should implement procedures to ensure that the transactions those agents conduct are legitimate. In addition, the insurance company should implement procedures for handling non-compliance by its brokers/agents (such as agent contract termination).

- (4) An insurance company must monitor the activity of its agents. The list of what insurance companies should be monitoring their agents for is not all inclusive.
- a. Compliance with relevant customer-related information requirements,
 - b. Compliance with any payment policies and procedures (such as, restrictions on cash, cash equivalents, or third-party payments),
 - c. Compliance with Form 8300 requirements,
 - d. Identification and referral of suspicious customer payments or actions,
 - e. Identification of suspicious agent payments,
 - f. Accessibility of customer and payment records,
 - g. Participation in and the adequacy of training;
 - h. Quality of any Form 8300 filed,
 - i. Unusual amount of SAR or Form 8300 filings on customers of agent, and
 - j. Sudden increase in writing large policies, increase in customers of agent remitting structured payments, or increase of customers of agent cancelling policy after free look or requesting loans.
- (5) There are various ways that an insurance company can monitor its agents. These include, but are not limited to:
- a. Reviewing the quality of customer applications.
 - b. Reviewing the forms of payment received with the initial application.
 - c. Following up on customer complaints.
 - d. Monitoring cancellations of policies during the free look period.
 - e. Monitoring early surrenders of annuities.
 - f. Monitoring customers who purchase single premium policies and annuities and almost immediately withdraw the cash value.
 - g. Monitoring customers who prepay premiums and borrow the maximum cash value.
 - h. Reviewing SARs and Form 8300 filed on customers of the agents.
 - i. Visiting agents: Are these required? Do the agents expect visitations by the principal insurance company? Are the visits done on a risk basis?
- (6) Where applicable, the independent review should include the insurance company's policies, procedures, and processes for agent relationships, including how the insurance company maintains oversight over agents related to BSA compliance. This includes establishing new agent relationships, monitoring existing relationships, and handling noncompliance by agents, including termination of agent relationships where appropriate.
- (7) The examiner must test the insurance company's policies, procedures, and internal controls to ensure that the insurance agents and brokers are fully integrated into the company's AML compliance program. This is a third-party check of transactions conducted on behalf of the insurance company that is under a Title 31 examination. Two samples need to be conducted:
- a. Select a sample of high-risk transactions for the insurance company and follow the transactions to the agent level. This includes interviewing the insurance agent directly related to these high-risk transactions and reviewing the agent's records associated with the transaction.
 - b. Select a sample of agents based on the insurance company's risk assessment of its insurance sales activities, covered products, and distribution channels, as well as prior examination and audit reports. With other data/criteria such as transactions that are at high-risk, agent's sales volume, agent's policy redemptions, FinCEN Query filings by or on an agent, a CAS should be able to help select the sample of agents. The

CAS can provide a list of agents in an electronic format (Excel or Access). The CAS should also be able to determine the number of agents to select in a statistically valid sample.

- (8) When selecting a sample of agents, avoid contacting banks and broker-dealers. This can be accomplished by requesting agent IDs in electronic format of all banks and broker-dealers. This data can be compared to transaction data to remove this group from the sample. If an examiner discovers AML issues that relate to a bank or broker-dealer during a BSA examination at the insurance company level, refer the issue to the BSA Liaison to FinCEN. FinCEN can then coordinate a referral with the appropriate federal bank regulator or the Securities and Exchange Commission.
- (9) For the samples selected, use the FinCEN Query system to obtain a download of any filings on or by agents of the insurance company.
- (10) Interview the agents in the sample to determine:
 - a. Agent's knowledge of the insurance company's AML policies, procedures, and internal controls.
 - b. Does the agent know the process for reporting suspicious activity?
 - c. Training received by the agent on the insurance company's AML policies, procedures, and internal controls. What form was the training? What did the training consist of? Who gave the training? When did the agent participate in the training?
- (11) Sample transactions of covered products for the agent at the agent level. This is the only way to know that the agent followed the insurance company's policies, procedures, and internal controls.
 - a. Is the agent identifying suspicious transactions and reporting those to the insurance company? Did the agent provide the necessary information to the insurance company?
 - b. Does the agent receive cash or cash equivalents from customers? If so, how is a cash transaction recorded and reported to the insurance company? Based on the cash received, is the agent required to file Form 8300? Was any required Form 8300 filed correctly and timely?
 - c. Does the agent make customer payments with a check drawn on the agent's own account, a cashier's check, or money orders?
 - d. How does the agent handle customers who frequently cancel policies during the free look period or surrender annuities early?
 - e. Compare transaction data at the agent level with the insurance company's records.
 - f. Review account opening documentation and ongoing due diligence information.
 - g. Determine whether activity is unusual or suspicious.
- (12) Based on the procedures completed, including transaction testing, form a conclusion about the adequacy of the AML policies, procedures, and processes associated with insurance sales.
- (13) Any BSA deficiencies or violations found at the agent level such as a breakdown in identifying and/or reporting suspicious activity or lack of training, are BSA violations at the insurance company level. The insurance agent

cannot be cited for AML program violations because insurance agents are not required to have an AML compliance program.

4.26.9.11.7.11
(11-12-2019)

Red Flags

- (1) A January 2010 FinCEN study of insurance companies, Insurance Industry Suspicious Activity Reporting, reveals that the most commonly cited suspicious activity involved the use of multiple cash equivalents for premium and or loan payments. Filing narratives also frequently discussed subjects paying premiums in an unusual manner – often by submitting cash and/or cash equivalents with checks – with instrument values below the BSA threshold. Although most subjects had a direct relationship to a policy such as the owner or beneficiary, “gatekeepers” such as accountants, trustees, or attorneys were also frequently mentioned.
- (2) The examples below standing alone are not, in and of themselves, indicative of suspicious activity but would need to be investigated further to determine the facts and circumstances in each case. These examples are not exhaustive.
- (3) Indicators of suspicious activity by the business include:
 - a. Failing to maintain complete records.
 - b. Failing to maintain accurate records.
 - c. Failing to record specific transaction.
 - d. Accepting third-party payment.
 - e. Failing to file a SAR or Form 8300, *Report of Cash Payments Over \$10,000 Received in a Trade or Business*, on a reportable transaction.
 - f. Structuring a transaction by breaking one transaction into several to circumvent the reporting requirements.
 - g. Treating the purchase of related items as separate sales.
 - h. Sales that are not in conformity with standard industry practice or that are unusual for this type of business.
 - i. Sales to nonexistent customers.
- (4) Indicators of suspicious activity by the customers include:
 - a. Customer exhibits an unusual concern regarding the insurance company’s compliance with government reporting requirements, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities or furnishes unusual or suspect identification or business documents.
 - b. A customer wishes to engage in transactions that lack business sense, apparent investment strategy, or are inconsistent with the customer’s stated plans.
 - c. A customer has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
 - d. A customer appears to be acting as the agent for another entity but declines, evades, or is reluctant, without legitimate commercial reasons, to provide any information in response to questions about that entity.
 - e. A customer insists on dealing only in cash equivalents or asks for exceptions to the insurance company’s policies relating to the acceptance of cash and cash equivalents.
 - f. Surrender of single premium policies during the free look period.
 - g. Evidence of structuring (an attempt by a customer to spread deposits of currency or cash equivalents on a single day, over several days or in a number of accounts).
 - h. Large cash payments.

- i. The purchase of a life insurance policy or annuity beyond a person's means, especially if the beneficiary has no clear relationship to the owner, insured or annuitant.
- j. A potential customer has several policies (for covered products) with different insurance carriers.
- k. Directions to send proceeds to third parties, especially if outside the U.S. or inside the U.S. if the owner is outside the U.S.
- l. Customers who ask for exceptions to the insurance company's policies.
- m. Potential customers who are unconcerned with suitability of the insurance product.
- n. Customer demands loan quickly and threatens a lawsuit if the insurance company does not comply with these time frames.
- o. Inconsistent application information.
- p. The purchase of an insurance product inconsistent with the customer's needs; unusual payment methods, such as cash, cash equivalents (when such a usage of cash or cash equivalents is, in fact, unusual), or structured monetary instruments.
- q. Early termination of a product, especially at a cost to the customer, or where payment is made by, or the refund check is directed to, an apparently unrelated third-party.
- r. The transfer of the benefit of a product to an apparently unrelated third-party.
- s. A customer who shows little concern for the investment performance of a product, but much concern about the early termination features of the product.
- t. A customer who is reluctant to provide identifying information when purchasing a product, or who provides minimal or seemingly fictitious information.
- u. A customer who authorized third parties to withdraw money from the cash value of their policies or were frequently cashing out their policies early.
- v. Suspicious loans taken out against an annuity contract.
- w. Life insurance premiums paid by unrelated third parties.
- x. Use of an insurance policy as collateral.
- y. Policy owner or customer is from or maintains accounts or policies in a jurisdiction whose government has been identified by the State Department as a sponsor of international terrorism or has been designated by the Financial Action Task Force as non-cooperative with anti-money laundering principles.
- z. Customers change owners, beneficiary, or third-party payees shortly after purchasing the policy.
 - aa. Excessive name and address changes.
 - ab. Customers frequently cancel policies during the free look period or surrender annuities or policies early.
 - ac. Customers frequently borrow maximum against policy early.
 - ad. Customers' initial payments frequently consist of cash, cash equivalents, multiple checks, third-party checks, or wire transfers or payments from a jurisdiction not logical for the customer (such as a tax haven).
 - ae. Excessive contracts issued for a client.
 - af. Excessive wire transfers; free look request, and loans.
 - ag. Customer address was determined to be a Specially Designated National address.
 - ah. Customers have frequent withdrawals of applications during the under-writing process.

- ai. Customers have frequent changes of information after application submission (owner, premium amount, or addresses).
- aj. Customers' information on application appears inconsistent and/or unusual for the sort of transaction applied for (for example, seemingly unconnected relationship of third-party payees, or owner).
- ak. Number of withdrawals or amount exceeds what is considered "the norm".
- al. Currency activity exceeds profile.
- am. Wire activity exceeds profile.
- an. Surrender occurred with suspiciously large penalty.
- ao. Withdrawal occurred after recent contract add or change.
- ap. Withdrawal occurred after recent address change.
- aq. Withdrawal was made to individual/company not having existing relationship.
- ar. Termination of policy after deposit considered excessive.
- as. Deposit was made from individual/company not having existing relationship.
- at. Withdrawal made after deposit considered excessive.
- au. Customer secured a loan too soon after new policy issue.
- av. Loan payoff followed by request for new loan.
- aw. Single withdrawal amount exceeds limit.
- ax. Deposit from/withdrawal to an OFAC sanctioned country.

(5) Indicators of suspicious activity by the agents include agents:

- a. Who do not comply with company policies, such as customer information requirements or payment policies.
- b. Who submit applications that include false, inconsistent, or suspicious information.
- c. Whose customers' initial payments frequently consist of cash, cash equivalents, multiple checks, third-party checks, or wire transfers or payments from jurisdictions not logical for the customer (such as tax havens).
- d. Who make customer payments with a check drawn on the agent's own account.
- e. Whose customers frequently cancel policies during the free look period or surrender annuities early.
- f. Whose customers change the owners shortly after purchasing the policy.
- g. Whose customers frequently conduct suspicious transactions.
- h. Who demonstrate a lavish lifestyle beyond their means; do not take vacations; show a dramatic increase in sales; or transact a disproportionate amount of single premium business.

(6) Evidence uncovered of potential money laundering should be considered for a referral to CI on Form 2797, *Referral Report for Potential Fraud Cases*.

4.26.9.11.7.12
(11-12-2019)
**Examining
Recordkeeping
Compliance**

- (1) Any documents the insurance company maintains that are relevant to the BSA examination can be requested and reviewed.
- (2) Determine if the insurance company is maintaining adequate records and document any recordkeeping violations. Examination procedures should be performed based on the risks identified.
- (3) If the examiner determines that records are inadequate, were destroyed, or not maintained:

- a. Expand the scope of the BSA examination and
 - b. Document all problem areas and findings in the workpapers.
- (4) Confirm that all required BSA reports are kept for five years.
- (5) If apparent BSA violations are detected, interview the responsible person or employee who conducted the unrecorded transaction(s). Based on the responses, consider expanding the scope of the examination.

4.26.9.11.7.13
(11-12-2019)
Finalizing the Title 31 Exam

- (1) Determine compliance with the AML program requirement under 31 CFR 1025.210, *Anti-money laundering programs for insurance companies*, suspicious activity reporting at 31 CFR 1025.320, *Reports by insurance companies of suspicious transactions*, and the Form 8300 filing requirements under 31 CFR 1010.330, *Reports relating to currency in excess of \$10,000 received in a trade or business*. There is no examination of or conclusions regarding the IRC customer notification requirement which is not required under Title 31. Complete the workpaper BSA Violations Summary Form Title 31.
- (2) Accumulate all pertinent findings from the examination performed. Evaluate the thoroughness and reliability of any risk assessment conducted by the insurance company. Determine whether:
- a. The AML program is effectively monitored and supervised in relation to the company's risk profile as determined by the risk assessment.
 - b. The AML program is effective in mitigating the company's overall risk.
 - c. The board of directors and senior management are aware of BSA regulatory requirements; effectively oversee BSA/AML compliance; and commit, as necessary, to corrective actions (such as independent reviews and regulatory examinations).
 - d. Policies, procedures, and internal controls are adequate to ensure compliance with applicable laws and regulations and provide sufficient risk management to appropriately address high-risk operations (covered products, customers, distribution channels, and geographic locations).
 - e. Independent testing (audit) is appropriate and adequately tests for compliance with required laws, regulations, and policies.
 - f. The designated person responsible for coordinating and monitoring day-to-day compliance is competent and has the necessary resources.
 - g. Personnel are sufficiently trained to adhere to legal, regulatory, and policy requirements.
 - h. Reportable transactions have been identified and any required SAR and Form 8300 have been filed timely and accurately.
 - i. Information and communication policies, procedures, and processes are adequate.
- (3) Determine whether deficiencies or violations were previously identified by management, independent reviews, or in a prior regulatory exam, or were only identified because of the current BSA examination.
- (4) Determine the underlying cause of any violations such as (the list is not all inclusive):
- a. Management has not assessed, or has not accurately assessed, the company's AML risks.
 - b. Management is unaware of relevant issues.

- c. Management is unwilling to create or enhance policies, procedures, and internal controls.
 - d. Management or employees disregard established policies, procedures, and internal controls.
 - e. Management or employees are unaware of or misunderstand regulatory requirements, policies, procedures, or internal controls.
 - f. High-risk operations have grown faster than the capabilities of the AML program.
 - g. Changes in internal policies, procedures, and internal controls are poorly communicated.
- (5) The examiner must hold a closing conference with the corporate officer or compliance officer. Other employees may be asked to attend to assist in addressing specific items. The examiner must:
- a. Review with the company deficiencies in the AML compliance program, suspicious transaction not reported, SARs not filed timely or correctly, and Form 8300 transactions not reported, or Forms 8300 filed late, incomplete or inaccurate.
 - b. Advise the company of any recordkeeping deficiencies.
 - c. Identify actions needed to correct any outstanding deficiencies or violations, including the possibility of requiring the company to conduct a more detailed risk assessment.
 - d. Obtain an explanation for all issues discussed.
 - e. Review any additional documents or information provided by the company and determine whether any items should be removed from the list of violations.
 - f. Ask the company to provide a written statement of the corrective actions they will undertake to address the issues noted.

4.26.9.11.8
(11-12-2019)

**Closing a Case
Examined Under Title 31**

- (1) An insurance company case is examined under Title 31.
- (2) Complete the Title 31 case file, including all workpapers, Lead Sheets, and documentation to substantiate the AML program violations, SAR violations, and the Title 31 Form 8300 reporting violations.
- (3) If there are no Title 31 violations, issue Letter 4029, *Bank Secrecy Act No Change Letter*.
 - a. In order not to mislead the company, insert in the "Recommendations are as follows" section "Form 8300 customer notification is not covered in this examination because is not a requirement under the BSA."
- (4) If there are Title 31 violations, the examiner must issue Letter 1112, *Title 31 Violation Notification Letter*.
 - a. If a Letter 1112 is issued, failure to file a Form 8300 under 31 CFR 1010.330, *Reports relating to currency in excess of \$10,000 received in a trade or business*, will be cited on the Form 13726, *Summary of Examination Findings and Recommendations*. Form 13726 should contain a statement in the Explanation of Apparent Violations Regulations and Recommendations section: "Form 8300 customer notification is not covered by this examination because the customer notification is not required under the Bank Secrecy Act".
 - b. Generally, if there is a Form 8300 violation under Title 31, there will be an AML program violation. If the company failed to file any required SAR

- or Form 8300 timely and correctly, there is a breakdown in the company's internal controls. If the AML program was effectively implemented and adequately monitored, there would not be a suspicious activity or Form 8300 reporting violation.
- c. If there are AML program violations of 31 CFR 1025.210, *Anti-money laundering programs for insurance companies*, the examiner must state the exact nature of any program deficiencies (such as internal controls, training, independent review, and designated compliance officer) in the Letter 1112.
- (5) If it is determined that a referral should be made to FinCEN, follow the regular referral procedures and include the Title 31 Form 8300 issues (if applicable).
 - a. Record on Form 9984, *Examining Officer's Activity Record*, that a referral of the Title 31 case is being made for a Title 26 Form 8300 examination to address any applicable penalties and the customer notification requirement.
 - (6) If no referral to CI is warranted, the examiner should secure delinquent Form 8300 and have the company file any delinquent SARs electronically.
 - (7) Close the Title 31 case. The examiner should charge all examination time up to this point to the Title 31 case.
 - (8) Open the Title 26 Form 8300 case file if necessary to examine the customer notification issues or to assert a Form 8300 penalty.
 - a. See IRM 4.26.11, *Bank Secrecy Act, BSA Examiner Responsibilities for Form 8300 Examinations*, for establishing the case on ERCS, case content, assembly, procedures, and a discussion of penalty considerations.
 - b. Complete a Form 8300 administrative case file. The examiner can use copies of Form 9984, the Memorandum of Interview, Form 8300 Lead Sheet, and documentation supporting the Form 8300 violations from the Title 31 case file.
 - c. Inspect the Form 8300 customer notifications for completeness and accuracy.
 - d. Form a conclusion about the company's compliance with the end-of-year statement notification requirements
 - e. If applicable, complete a Form 8300 penalty case file using regular IRC 6721, *Failure to file correct information returns*, and IRC 6722, *Failure to furnish correct payee statements*, procedures. See IRM 4.26.11.
 - f. Charge time spent on the Title 26 Form 8300 exam to activity code 509.

Note: For complete details regarding procedures for requesting Title 26 after completing examinations under Title 31, see IRM 4.26.8, *Special Procedures*.

4.26.9.12
(11-12-2019)
**Prepaid Access
Overview**

- (1) On July 26, 2011, the Financial Crimes Enforcement Network (FinCEN), which is a Treasury bureau that collects and analyzes financial transaction information to combat money laundering, terrorist financing, and other financial crimes, announced its final rule addressing regulatory gaps resulting from the “proliferation of prepaid innovations ... and their increasing use as an accepted payment method”. (<https://www.fincen.gov/news/news-releases/fincen-issues-prepaid-access-final-rule>)
- (2) The final rule amended the BSA regulations (31 CFR Part 1010, *General provisions*, and 31 CFR Part 1022, *Rules for money services businesses*) applicable to MSBs. The final rule is available at <https://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf>. The amended regulations:
 - a. Renamed “stored value” as “prepaid access” to more accurately describe the activity involved in prepaid programs, and
 - b. Superseded the terms, “issuer” and “redeemer” of stored value with “providers” and “Sellers” of prepaid access.
- (3) Prepaid access:
 - a. Is a financial service providing purchasers convenient access to a financial system. Issuers benefit significantly from the features available on the prepaid access device, for example, the magnetic stripe, which allows tracking of specific details, including goods and services purchased, available balances, and demographic information.
 - b. Has natural features, including its transportability and a potential for carrying high dollar amounts. These features also increase the risk of its use in money laundering or other criminal activity. Therefore, as a type of payment system, an appropriate level of regulation is required to prevent its misuse.

4.26.9.12.1
(11-12-2019)
Prepaid Access Defined

- (1) Prepaid access is access to funds or the value of funds paid in advance and retrievable or transferable at some future point through an electronic device or vehicle such as a card, code, electronic serial number, mobile identification number, or personal ID number. (31 CFR 1010.100(ww), *Prepaid access*)
- (2) The above definition is intentionally non-technology specific to cover future advances in technology.

4.26.9.12.2
(11-12-2019)
**Prepaid Access
Terminology**

- (1) Prepaid access terminology creates a standard way to communicate within the industry. Understanding industry terms ensures comprehension of the type of products sold and the services offered by a prepaid access program. The terminology discussed is used by the industry and not necessarily defined as such in the BSA regulations.
 - a. Acquirer - A company or financial institution that contracts with merchants to accept payment cards (including prepaid cards) as payment.
 - b. Automated Clearing House (ACH) - An electronic payment network, used typically to process batch debit and credit transfers between financial institutions. ACH transactions function like electronic checks that are settled (paid) within one or two business days, using procedures like paper check settlement. Some prepaid cards (for example, payroll cards and government-funded prepaid cards) are loaded via ACH transactions.

- c. Card Brand - Typically, American Express, Discover, MasterCard, Visa, or the ATM/Electronic Funds Transfer (EFT) networks, collectively, the “Card Brands” (also referred to as Brand or Card Organization/ Association). The Card Brands provide the underlying infrastructure for network branded prepaid cards and some restricted access network prepaid cards.
- d. Card-to-Card Transfer - A transaction that moves funds directly from one prepaid card account to another. For example, card-to-card transfers may be offered with remittance cards or payroll card products, where a family member may provide a prepaid card to another family member, such as a parent, spouse or child, and transfer funds from one prepaid card to the prepaid card held by the family member.
- e. Electronic Funds Transfer (EFT) Network - Networks—such as New York Currency Exchange (NYCE), Star, Pulse, Interlink and Maestro—that provide switching and support services for online or ATM and/or point of sale (POS) purchase transactions.
- f. J-Hook - Looped end hook used by retailers in stores to display merchandise including prepaid cards.
- g. Load refers to adding funds or added funds to a prepaid access device to establish an available balance. Reload is a transaction placing additional funds onto an already active prepaid access device. The terms often are used interchangeably.
- h. Loads and reloads made through a depository institution include, but are not limited to, Automated Clearing House (ACH) transfers from a bank account, cash or other deposit at a bank, or a check drawn on a bank and payable to the prepaid access provider (Provider).
- i. Loads and reloads from non-depository sources include, but are not limited to, retail store transactions (for example, by cash, check, or credit card), wire transfers originating at an MSB, or checks payable to a party other than the prepaid access Provider.
- j. Load Fee - A fee charged when a prepaid card is loaded or reloaded with money.
- k. Load Limit - The maximum number of times a prepaid card may be loaded with funds or the maximum value that may be loaded to a prepaid card.
- l. Load Network - A network of retail business locations that have established a secure electronic facility with a prepaid card issuer to accept cash, cash equivalent, and credit and/or debit transactions to add value to a prepaid card.
- m. Network Branded Prepaid Card - A prepaid card displaying the logo of a card brand (for example, American Express, Discover, MasterCard, Visa, NYCE, Pulse, Star) that can be used at unrelated merchants to pay for goods and services and for ATM cash access.
- n. Network Branded Prepaid Card Association (NBPCA) - A nonprofit trade association. See <https://www.nbpca.org/>.
- o. Pooled Account - Single account used by an issuer to hold funds associated with its prepaid cards. Balances for each prepaid card account are maintained in the system of record (generally by the Processor).
- p. Provider – The prepaid program participant that agrees to serve as the principal conduit for access to information. See IRM 4.26.9.12.4.
- q. Reissue - The creation and issuance of a new prepaid card with the same card number and expiration date as the previous card.
- r. Remittance Card - A prepaid card that facilitates transfers of funds by consumers, usually to friends/family in their home countries.

- s. Seller – A retailer engaged in the sale of prepaid access, that receives funds or the value of funds in exchange for an initial loading or subsequent loading of prepaid access under certain conditions. See IRM 4.26.9.12.5.
 - t. Unbanked/Underbanked Consumers - Individuals who have no or limited access to financial services at banks and other mainstream financial institutions. There are between 20 to 80 million un/under-banked individuals in the U.S.
 - u. Value Chain - The entities that play a role in making prepaid products available might include the issuer/issuing bank, program manager, processor, and distributor.
 - v. Agent - An entity that acts as a processor, a third-party, or both, for a prepaid card issuer, providing payment-related services, directly or indirectly. Performs services such as:
 - Storing, processing or transmitting cardholder, transaction data or account numbers,
 - Conducting cardholder solicitation, card application processing services, or customer service,
 - Conducting merchant solicitation, sales, customer service, merchant transaction solicitation, or merchant training,
 - Performing transaction-related or back office-related functions; providing ATM and/or point-of-transaction deployment or operational support, and
 - Soliciting other entities to sell, distribute, activate, or load prepaid cards on behalf of an issuer.
- (2) Some entities fill more than one link in the value chain. The roles and responsibilities associated with each are dictated by programs

4.26.9.12.3
(11-12-2019)

Prepaid Access Program

- (1) A prepaid access program is an arrangement under which one “person” (entity), or more persons acting together, provides prepaid access. (31 CFR 1010.100(ff)(4)(iii), *Prepaid program*)
- (2) Prepaid access arrangements can vary greatly and include travel programs, university campus programs, public transportation programs, and many others. All programs offer specific features and characteristics targeted to different groups of people and activities.
- (3) Participants in a prepaid program may include, but are not limited to, retailers, issuing banks, prepaid program managers, prepaid card networks, payments processors, and other service providers.
- (4) FinCEN issued FIN-2016-G002, Frequently Asked Questions (FAQs) regarding Prepaid Access, on March 24, 2016, indicating the FAQs “are in addition to, and supplement the FAQs entitled Final Rule – Definitions and Other Regulations Relating to Prepaid Access, which were issued on November 2, 2011”. The FAQs posting are available at <https://www.fincen.gov/sites/default/files/shared/FIN-2016-G002.pdf> and http://www.fincen.gov/news_room/nr/pdf/20111102.pdf, respectively.

4.26.9.12.3.1
(11-12-2019)

Prepaid Access Program Inclusions

- (1) Prepaid programs covered under the regulations include:
 - a. Closed loop prepaid access, and
 - b. Open loop prepaid access.
- (2) Closed loop prepaid access of greater than \$2,000 in value on any single day:

- a. Is defined as prepaid access to funds or the value of funds that can be used only for goods and services in transactions involving a defined merchant or location (or set of locations), such as affiliated retailers or retail chains, a college campus, or a subway system. 31 CFR 1010.100(kkk), *Closed loop prepaid access*.
 - b. Excludes transfers of value to third parties and cash withdrawals.
- (3) Open loop prepaid access is often referred to in the industry as “general purpose reloadable (GPR) cards”. Open loop prepaid access of greater than \$1,000 value on any single day:
- a. Can be of any value with thresholds established per device.
 - b. Have no requirement to aggregate purchases on separate (distinct) prepaid devices procured within a single day.
 - c. Are used for employment benefits and provide for international use. (IRM 4.26.9.12.3.2.3)
 - d. Features transfers between or among users per 31 CFR 1010.100 (ff)(4)(iii)(D)(i)(ii) referred throughout this IRM as person-to-person (P-to-P) transfers that allow customers to move value freely from their account to other cardholders.
 - e. Allows loading of additional funds from non-depository sources.

4.26.9.12.3.2
(11-12-2019)
**Prepaid Program
Exclusions**

- (1) There are various prepaid arrangements that do not fall under the definition of a prepaid access program. They do not warrant inclusion under the regulations due to low vulnerability and low risk of being used, knowingly or unknowingly, for money laundering, terrorist financing, or other illicit activities. Accordingly, these arrangements are not required to register with FinCEN as an MSB.

4.26.9.12.3.2.1
(11-12-2019)
**Closed Loop Prepaid
Access Exclusions**

- (1) Excluded under the regulations are closed loop prepaid access devices when:
- a. The value of each closed loop prepaid access device or vehicle is \$2,000 or less in any one day. (31 CFR 1010.100(ff)(4)(iii)(A))
Example: If a closed loop prepaid access device has a value of \$1,500, and the holder spends \$1,000 and subsequently reloads \$600 before the end of the day, this prepaid access would fall within the definition of a prepaid program because \$2,100 (\$1,500 beginning balance plus \$600 reload) has been associated with the prepaid access within a single day.
 - b. For sole payment of government benefits, such as those issued by Federal, state, local, and tribal governments; and U.S. territories and Insular Possessions. (31 CFR 1010.100(ff)(4)(iii)(B))
 - c. For sole disbursement of health/dependent care, such as pre-tax flexible spending arrangements or Health Reimbursement Arrangements (HRAs). (31 CFR 1010.100(ff)(4)(iii)(C))

Note: These arrangements are pre-funded by employee and/or employer contributions to an account maintained by the payor. Maximum annual dollar limits are established for these accounts, and the funds can only be accessed as reimbursement for defined, qualifying expenses.

4.26.9.12.3.2.2
(11-12-2019)

**Open Loop Prepaid
Access Exclusions**

- (1) Excluded are open loop prepaid access in the amount of \$1,000 or less, on any single day, and without the capability of:
 - a. Transmitting funds/value internationally. (31 CFR 1010.100(ff)(4)(iii)(D)(2)(i))
 - b. Transferring value P-to-P within a prepaid program. (31 CFR 1010.100(ff)(4)(iii)(D)(2)(ii))
 - c. Loading additional funds or the value of funds from non-depository sources. (31 CFR 1010.100(ff)(4)(iii)(D)(2)(iii))

4.26.9.12.3.2.3
(11-12-2019)

**Employment-Related
Limited Exclusions**

- (1) Employment benefits, incentives, bonuses, wages, or salaries enjoy limited exclusion as a type of prepaid program. Exclusion applies only when:
 - a. It does not permit transmission of funds or value internationally.
 - b. It does not permit P-to-P transfers within a prepaid program.
 - c. It does not permit reloads of additional funds or the value of funds from non-depository sources.
 - d. The employer, and not the employee, can add to the value to the prepaid access.

4.26.9.12.4
(11-12-2019)

Prepaid Access Provider

- (1) The Provider is the prepaid program participant that serves as the principal conduit for access to information by fellow program participants. One participant in each prepaid program is designated as the Provider.
- (2) A Provider of the prepaid access program can be determined in one of two ways under 31 CFR 1010.100(ff)(4)(i):
 - The program participants can determine the Provider.
 - The program participant with principal oversight and control over the program will, by default, be the Provider when not determined by the program participants.
- (3) Five factors determine the Provider of a prepaid access program in the event no program participant agrees to be, nor registers as the Provider. (31 CFR 1010.100(ff)(4)(ii))
- (4) Based on the facts and circumstances of each prepaid access program, determining the Provider is a matter of establishing the participant exhibiting principal oversight and control. Activities include:
 - Organizing the prepaid access program,
 - Setting and determining compliance with program terms and conditions,
 - Determining program participants, such as the issuing bank, payment processor, or distributor,
 - Controlling or directing parties to initiate, freeze or terminate prepaid access, and
 - Engaging in other activities evidencing oversight and control.
- (5) The Provider is subject to IRS's regulatory oversight and examination authority for compliance with its BSA obligations.
 - If the prepaid access is sold under an exempted arrangement, such as when a bank is the Prepaid Access Program Manager and the program is not subject to IRS's delegated authority to examine MSBs for BSA compliance.

4.26.9.12.5
(11-12-2019)
**Prepaid Access Seller
Defined**

- (1) A Prepaid Access Seller is any person receiving funds or the value of funds in exchange for initial or subsequent loading of prepaid access. (31 CFR 1010.100(ff)(7))
- (2) The Prepaid Access Seller is the party with the greatest face-to-face contact with the purchaser and is the most valuable resource for capturing information at the POS. Typically, sales of prepaid access products occur at general-purpose retailers engaged in a full spectrum product line, such as pharmacies, convenience stores, supermarkets, discount stores, and other similar retailers.
- (3) Determination as a Prepaid Access Seller is based on meeting one of two conditions.
 - It sells prepaid access that can be used prior to the verification of the customer's identification by the program participant, (31 CFR 1010.100(ff)(7)(i)) or
 - It sells prepaid access (including closed loop prepaid access) to funds that exceed \$10,000 to any person during any one day and has not implemented policies and procedures reasonably adapted to prevent such a sale. (31 CFR 1010.100(ff)(7)(ii))

Note: Reasonable adaptation is based on the regulations, and facts and circumstances; there are no standard policies and procedures established to prevent sales or prepaid access exceeding \$10,000 in value to any person during any one day.
- (4) To **not** be considered a Prepaid Access Seller under the regulations, the retailer must implement policies and procedures reasonably adapted to prevent the sale of prepaid access that exceeds \$10,000 in value to any person during any one day and must not sell prepaid access offered under a prepaid program that can be used before verification of the customer's identification.
 - a. Reasonably adapted policies and procedures are risk-based and appropriate to the Seller's customer base, location, and its typical volume of prepaid access sales, among other considerations.
- (5) The sale of prepaid access in an amount exceeding \$10,000 should raise automatically a "red flag" with a retailer, regardless of whether the purchase is by cash or some other form of payment. High-dollar prepaid access transactions pose inherent money laundering risks.
 - a. The sale of over \$10,000 in prepaid access to one person in any one day does not, in and of itself, mean the Seller's policies and procedures are not reasonably adapted to prevent such sales. Determining whether a program is "reasonably adapted" depends on the facts and circumstances of the occurrence(s).
 - b. See IRM 4.26.9.12.9.5.3.2 for more details.
- (6) An entity reloading prepaid access from a non-depository source is a "Seller", subject to the regulations, if it:
 - a. Reloads in excess of \$10,000 for any person on any given day.
 - b. Does not have policies and procedures reasonably adapted to prevent such reloading for any person on any given day.

- c. Reloads funds onto a prepaid access device that is part of a prepaid program not subject to initial customer verification.

Example: A retailer sells a closed loop prepaid access product that can be loaded for more than \$2,000 on any one day. The customer can use the product without providing ID-verifying information. The retailer is a seller under 31 CFR 1010.100(ff)(7)(i) because:

- (7) The phrase “can be used before verification of customer ID” refers only to use of features of a prepaid access product that qualifies as a prepaid program under the regulations.

Example: A retailer sells a closed loop prepaid access product that can be loaded for more than \$2,000 on any one day. The customer can use the product without providing ID-verifying information. The retailer is a Seller under 31 CFR 1010.100(ff)(7)(i) because the prepaid access product qualifies as a prepaid access program; and the prepaid access product can be used before verification of the customer’s ID. This definition stands regardless of whether the retailer implemented policies and procedures to prevent the sale of prepaid access exceeding \$10,000 to any one person during any one day. 31 CFR 1010.100(ff)(7)(ii).

Example: A retailer sells an open loop prepaid access product that allows initial funds to be loaded below \$1,000 and can be used for purchases before any customer ID verification. The prepaid access product does not have features for international use, P-to-P transfers, or loads from non-depository sources. The retailer has not implemented policies and procedures reasonably adapted to prevent the sale of prepaid access that exceeds \$10,000 to any person during any one day. In this example, the retailer: is not a Seller of prepaid access under 31 CFR 1010.100(ff)(7)(i) because the features of the prepaid product in this example do not qualify as a prepaid program or is a Seller of prepaid access under 31 CFR 1010.100(ff)(7)(ii) because the retailer did not have policies and procedures reasonably adapted to prevent the sale of prepaid access that exceeds \$10,000 to any person during any one day.

4.26.9.12.6
(11-12-2019)
**Prepaid Access Provider
Regulatory
Requirements**

- (1) The regulations require Prepaid Access Providers to:
 - a. Register with FinCEN, and file electronically FinCEN Form 107, *Registration of Money Services Business*.
 - b. Maintain an agent listing and provide it upon initial and biannual renewal registrations.
- (2) MSB registration requirements, other than the above, apply to Prepaid Access Program Providers and participants, see FinCEN’s Fact Sheet on MSB Registration Rule at <https://www.fincen.gov/fact-sheet-msb-registration-rule> and BSA Requirements for MSBs at <https://www.fincen.gov/bsa-requirements-msbs>.

4.26.9.12.6.1
(11-12-2019)
**Provider Requirement to
Register with FinCEN**

- (1) The Prepaid Access Provider must:

- a. Prepare and maintain a list of Agents upon registration and must be revised each January 1 for the immediately preceding 12-month period. Upon request, the list must be made available to FinCEN and any other appropriate law enforcement agency. (31 CFR 1022.380(d)(1), *In general*)
 - b. Identify each prepaid program for which it is the Provider, in the MSB Registration form, items 38 to 43. (31 CFR 1022.380(a)(1), *In general*)
 - c. Retain a copy of FinCEN Form 107, *Registration of Money Services Business*.
 - d. Renew the registration each two calendar-year period following the initial registration.
- (2) The Prepaid Access Provider is also required to re-register the prepaid access program if it experiences:
- a. A change in ownership or control that requires the business to re-register under State law,
 - b. A transfer of more than 10 percent of the voting power or equity interests (other than an MSB that must report such transfers to the Securities and Exchange Commission), or
 - c. An increase of more than 50 percent in the number of its agents during any registration period.
- (3) Only the Provider is required to register. (31 CFR 1022.380, *Registration of money services businesses*)

4.26.9.12.6.1.1
(11-12-2019)

Who Is Not Required to Register

- (1) Participants in a prepaid access arrangement, other than the Provider, are not required to register.
- (2) Participants in an excluded prepaid access program are also not required to register. See IRM 4.26.9.12.3.2 for the programs excluded from the BSA requirements.
- (3) Prepaid Access Sellers are not required to register. (31 CFR 1022.380(a)(1), *In general*) A Seller of prepaid access, as defined in 31 CFR 1010.100(ff)(7), *Seller of prepaid access*, is any person that receives funds or the value of funds in exchange for an initial loading or subsequent loading of prepaid access if that person:
- a. Offers products under a prepaid access program, that can be used before customer ID verification under 31 CFR 1022.210(d)(1)(iv), or
 - b. Sells prepaid access (including closed loop prepaid access) to funds exceeding \$10,000 to any person during any one day and has not implemented policies and procedures reasonably tailored to prevent such sales.
- (4) 31 CFR 1010.100(ff)(8)(i), *Limitation*, specifies that the term, "MSB", does not include a bank or foreign bank. Therefore, a bank cannot be a Provider of prepaid access subject to the requirements, including the registration requirement.
- a. A bank can be the Prepaid Access Program Manager, but not the Provider. IRS does not have delegated examination authority under Title 31 to examine banks.

4.26.9.12.6.2
(11-12-2019)
Agent Listing

(1) The Participants, other than the Provider, in a prepaid access arrangement that meet the definition of a prepaid program, are considered Agents of the Prepaid Access Provider.

4.26.9.12.6.3
(11-12-2019)
Prepaid Access Provider and Program Participant Requirements

(1) Providers and program participants of prepaid access, as MSBs, are required to:

- Maintain an anti-money laundering (AML) program.
- Prepare and maintain an Agent list.
- File currency transaction reports (CTRs).
- File suspicious activity reports (SARs).
- Collect and retain customer and transaction information.

4.26.9.12.6.3.1
(11-12-2019)
AML Program

(1) The Prepaid Access AML program requirements for Providers and Sellers are the same as MSB requirements.

(2) Providers and Sellers of prepaid access are required to develop, implement, and maintain an effective AML program. 31 CFR 1022.210(a), *Anti-money laundering programs for money service businesses*. The AML program must be reasonably effective in ensuring compliance with the regulations. By filing the proper reports and maintaining the required records, the MSB mitigates the risk of being used to facilitate money laundering or other illicit activities, such as terrorist financing.

(3) The AML program is based on the unique character of the business. Its requirements should be commensurate with risk types (for example, location, size, customer, prepaid product features, volume of the service) and risk levels.

(4) The AML program must be in writing and must:

- a. Incorporate policies, procedures, and internal controls reasonably designed to assure compliance with BSA regulations. (31 CFR 1022.210(d)(1))
- b. Designate a person to assure day-to-day compliance with the program and other requirements of the regulation. (31 CFR 1022.210(d)(2))
- c. Provide education and/or training of personnel regarding their responsibilities under the program. (31 CFR 1022.210(d)(3))
- d. Provide for independent review to monitor and maintain the program. (31 CFR 1022.210(d)(4))

(5) The AML program must also include provisions for complying with the following requirements:

- a. Verifying customer ID. (31 CFR 1022.210(d)(1)(i)(A))
- b. Filing reports. (31 CFR 1022.210(d)(1)(i)(B))
- c. Creating and retaining records. (31 CFR 1022.210(d)(1)(i)(C))
- d. Responding to law enforcement requests. (31 CFR 1022.210(d)(1)(i)(D))

(6) Prepaid Access Providers and Sellers with automated data processing systems should incorporate compliance procedures within their automated systems.

(7) Each MSB and its Agents are responsible for establishing, implementing, and maintaining an AML program required by 31 CFR 1022.210(a). By agreement,

responsibility for the development of the policies, procedures, and internal controls required by the regulation can be allocated between Prepaid Access Program participants.

- (8) There are two additional AML program requirements for Providers and Sellers of prepaid access under 31 CFR 1022.210(d)(1)(iv):
 - a. The identity of a person who obtains prepaid access under a prepaid program must be verified.
 - b. Procedures must be established to verify the identification of a person who obtains prepaid access to funds that exceed \$10,000 during any one day and that comply with reporting requirements.

4.26.9.12.6.3.2
(11-12-2019)

Customer Identification Requirements

- (1) 31 CFR 1022.210(d)(1)(iv) requires Prepaid Access Providers and Sellers to establish and maintain procedures to verify the identity of a person who obtains prepaid access, and obtain customer identifying information. The AML program, if effectively designed, implemented, and maintained, can be vital in mitigating the various risks involved in P-to-P transactions, especially as they relate to the placement stage of money laundering. See IRM 4.26.1.1.2, *Definition of Money Laundering*, for more details on the placement stage.
- (2) Providers and Sellers of prepaid access are required to, and are responsible for, establishing procedures to:
 - a. Verify the identity of a person who purchases prepaid access under a prepaid program, and
 - b. Obtain the following identifying information on the person purchasing the prepaid access - name, date of birth, address, and ID number.
- (3) Unlike Providers, Sellers are retailers that sell a variety of products (such as, convenience stores and pharmacies). Therefore, Sellers generally have the best opportunity to collect customer identifying information at the POS due to their face-to-face contact with customers.
- (4) For Sellers, the focus is on prepaid access that poses increased money laundering risks, such as those that do not require verification of customer identification before use or that have the potential for carrying high-dollar amounts.

4.26.9.12.6.3.3
(11-12-2019)

Suspicious Activity Reports

- (1) 31 CFR 1022.210(d)(1)(iv) requires Sellers of prepaid access to establish procedures to verify the ID of a person who purchases prepaid access to funds that exceed \$10,000, in a single transaction, or in aggregate, during any one day. For such transactions, the Seller must also obtain identifying information on the person who made the purchase including name, date of birth, address, and ID number.
- (2) Providers and Sellers of prepaid access, as MSBs, are required to file Currency Transaction Reports (CTRs). 31 CFR 1010.311, *Filing obligations for reports of transactions in currency*.
 - a. A CTR is filed for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through or to a prepaid access Provider or Seller, involving a transaction in currency of more than \$10,000.

- b. Multiple currency transactions are treated as a single transaction if the Seller has knowledge that the transactions are by or on behalf of any person and result in either cash in or cash out totaling more than \$10,000 during any one business day. 31 CFR 1010.313(b), *Multiple transactions*. See IRC 4.26.13, *Structuring*.
 - c. A CTR is filed within 15 calendar days following the day the reportable transaction occurred. 31 CFR 1010.306(a)(1), *Filing of reports*. The CTR must be filed electronically with FinCEN
- (3) Prepaid Access Providers and Sellers must ensure effective procedures that monitor transactions for suspicious activity. Providers and Sellers are required to file electronically Suspicious Activity Reports (SARs) with FinCEN when the transactions are:
- a. Conducted or attempted by, at or through an MSB and involves funds, including aggregated funds, or other assets of at least \$2,000, and the MSB knows, suspects, or has reason to suspect that the transaction, or pattern of transactions is suspicious.
- (4) A Provider or Seller may also file a SAR on transactions it believes are relevant to the possible violation of any law or regulation but whose reporting is not required by 31 CFR 1022.320(a)(1), *General*.

4.26.9.12.6.3.4
(11-12-2019)
**Recordkeeping
Requirements**

- (1) 31 CFR 1022.420, *Additional records to be maintained by providers and sellers of prepaid access*, was added to require each Prepaid Access Provider to maintain for five years, access to records relating to Provider and Seller transactions including:
- a. Providers of prepaid access are required to maintain access to records for five years related to transactions conducted in the ordinary course of business that would be needed to reconstruct prepaid access activities.
 - b. Providers must retain customer identification information for five years from the date of prepaid access last use.
 - c. Sellers must retain customer identification information for five years from the date the prepaid access was sold.

4.26.9.12.6.3.4.1
(11-12-2019)
**Records Commonly
Found**

- (1) Providers maintain various types of reports and records including information derived from transactions and tasks performed by a cardholder, from time of purchase to expiration.
- (2) Various payment systems and mechanisms are used to move illicit funds and facilitate criminal activities. The information collected by the Provider can be extremely useful in the examination, providing transactional information and cardholder ID information.
- (3) These reports and records contain the necessary information for supporting analyses and for following the money trail. Such reports and records include:
- a. Load volumes (by cash, ACH, ATM, credit/debit cash)
 - b. Cash out transactions
 - c. Credits back to the Prepaid Card Account
 - d. Multiple withdrawals per account
 - e. International transactions
 - f. Duplicate card sales
 - g. Chargebacks and reversals of loads due to fraudulent transactions

- (4) The provider collects various types of data from the cardholder, required for activating the prepaid card, such as the cardholder's:
 - a. Name (Last, First, Middle Initial)
 - b. Date of Birth
 - c. The ID Number
 - d. Address (Street, City, State, ZIP Code)
 - e. Phone Number (Home and or cell phone number)

4.26.9.12.6.3.5
(11-12-2019)
**Additional Prepaid
Access Requirements**

- (1) Providers and Sellers of prepaid access must also file:
 - a. *Report of Foreign Bank and Financial Accounts (FBAR)*, FinCEN Form 114, and
 - b. *Report of International Transportation of Currency and Monetary Instruments (CMIR)*, FinCEN Form 105.

4.26.9.12.7
(11-12-2019)
Risk Factors

- (1) Prepaid card programs are extremely diverse in the range of products and services offered and the customer bases served. In evaluating the risk profile of a prepaid access program, Providers and Sellers should consider the program's specific features and functionalities. No single indicator is necessarily determinative of lower or higher BSA/AML risk.
- (2) To implement a risk-based AML program, it is essential that Providers and Sellers understand the money laundering and terrorist financing risks posed by the prepaid products they offer. Providers and Sellers should identify and assess their risks and develop procedures that mitigate those risks.
- (3) Some entities fill more than one link in the value chain. The roles and responsibilities associated with each are not necessarily hard and fast.
- (4) Analysis of these features and other factors, such as volume and materiality, assists in determining the potential money laundering risks and, consequently, the AML risk management processes and internal controls that can be applied to the prepaid program.
- (5) Prepaid Access Program features and functionalities that could increase the money laundering risk include, but are not limited to:
 - a. The anonymity of the cardholder
 - b. Fictitious cardholder information
 - c. Cash access of the card (especially internationally)
 - d. The volume of funds that can be transacted on the card
 - e. Type and frequency of card loads and transactions
 - f. Card value limits
 - g. Geographic location of card activity
 - h. Relationships with parties in the card program
 - i. Distribution channels
 - j. The nature of funding sources

4.26.9.12.7.1
(11-12-2019)
**Knowledge about
Customers**

- (1) The risk posed by non-face-to-face relationships and anonymity (not identifying the customer) can occur with prepaid cards, mobile payment services, and Internet-based payment services.

- (2) Factors increasing risk include:
 - a. Lack of relevant information about the cardholder or about parties involved with cards.
 - b. Non-customer (anonymous cardholder).
- (3) Factors decreasing risk include:
 - a. The collection, availability, and verification of information related to cardholders may reduce risk by allowing for due diligence and screening against government lists, among other “know your customer” controls.
 - b. Similarly, the established relationship between a card program’s issuer and the program’s acquirer or distributor (for example, a commercial loan relationship with a corporate customer providing payroll or benefits cards to their employees), provides comfort as to the purpose, users, and use of the cards.
 - c. The customer has an existing relationship with the Prepaid Access Provider/Seller.
 - d. If a non-customer, cardholder ID data is verified.
 - e. There are limits on loads and spending.
 - f. Transactions are monitored.
 - g. There are prohibitions on cash access and reloading.

4.26.9.12.7.2
(11-12-2019)
Intended Users

- (1) Risk is increased when prepaid access allows multiple users.
- (2) Risk is decreased when Prepaid Access Programs:
 - Feature cards that limit the use of a prepaid card program by restricting (or complicating) the process of transferring value to third-party beneficiaries.
 - Restrict who can use a card to extract value, such as use of a PIN, or embossing the cardholder’s name and/or photograph on the card, or that limit the card use to a specific individual.

4.26.9.12.7.3
(11-12-2019)
Number of Prepaid Cards per Person

- (1) Risk is increased when prepaid access permits an individual to carry multiple cards simultaneously, whether by design or through lack of sufficient identifying information to make such a determination.
- (2) Risk is decreased when there are limitations on the number of cards that can be held by one individual. Risk is managed by enforced monitoring of identifiers (for example, tax ID numbers or other government identifiers), which makes it difficult for a single individual to handle a large volume of cards, and to process large amounts of value.

4.26.9.12.7.4
(11-12-2019)
Card Expiration

- (1) Prepaid programs offering cards with a predetermined and limited lifespan (for example, one year after issuance) are potentially less appealing to money launderers due to the requirement that the cards must be used relatively quickly, rather than retained for later aggregation or conversion.

4.26.9.12.7.5
(11-12-2019)
Geographic Area

- (1) The extent to which a prepaid access product can be used globally for making payments or transferring funds is important to consider when determining risk. Some programs, such as travel cards, are designed specifically for cross-border use but have strict limits on use within specific jurisdictions.

- (2) Open-loop prepaid access cards often allow customers to make payments at domestic and foreign POSs through global payment networks. The cards are accepted as a means of payment everywhere a Network Branded Prepaid Card is accepted. Providers may be based in one country and sell their product internationally through Agents or the Internet. These cards can then be used to purchase goods and services, or to access cash, internationally. Some prepaid card programs also allow cardholders to transfer funds P-to-P.
- (3) The global use of some prepaid cards to make payments, access cash, and transfer funds are features that make this product attractive for money laundering and terrorist financing. The compact physical size of prepaid cards makes the cards potentially vulnerable to misuse by criminals who use the cards, instead of cash, to make cross-border transportations of value or to transport a discreet number of prepaid cards loaded with high fund values.
- (4) Risk increases when:
 - a. No geographical restrictions or limitations exist and, therefore, allow for use in any jurisdiction.
 - b. Cards can be used in jurisdictions considered to be at higher risk for money laundering or terrorist financing, or have minimal or non-existent anti-money laundering laws.
 - c. Mobile payment services and Internet-based payment services that can be used to transfer funds globally or within a wide geographical area, with many counter-parties, are more attractive to criminals than purely domestic business models. In addition, Providers located in one jurisdiction may offer these services to customers located in another jurisdiction where they may be subject to less stringent AML obligations, oversight, or controls.
- (5) Risk decreases when geographic restrictions are placed on the use of a prepaid card, for example, the ability to limit the use of the card to jurisdictions.

4.26.9.12.7.6
(11-12-2019)
**Load and Reload
Frequency**

- (1) Depending on the type of prepaid card or device, and the issuer's terms and conditions, a load or reload may be made in a variety of ways such as cash, ACH/direct deposit, bank account transfer, reload device, or transfer from debit/credit card.
- (2) Factors that increase risk include:
 - a. Unrestricted frequent reloads.
 - b. Loads and reloads in high dollar amounts.
- (3) Factors that decrease risk include:
 - a. Single loads only (non-reloadable).
 - b. Limitations on the use of the card to one or a limited number of merchants, or the inability to use the prepaid card for higher risk activities (for example, card use restricted to targeted merchant types).
 - c. Limits or prohibitions on amounts of loads or the number of loads/reloads within a specific timeframe (velocity or speed of fund use).

- d. If unrestricted reloads with high limits, source of funds data is required in addition to cardholder ID verification, enhanced due diligence on cardholders, enhanced transaction monitoring, and caps on ATM withdrawals.

4.26.9.12.7.7
(11-12-2019)

Source of Funding

- (1) Depending on the type of prepaid card or device and the issuer's terms and conditions, funds may be added in a variety of ways such as cash, ACH load/direct deposit, bank account transfer, transfer from debit/credit card, or reload device.
- (2) How a prepaid card is funded presents varying degrees of money laundering risk, due largely to the relative degree of control a financial institution has in determining and constraining the source of the funds used to load value onto cards.
- (3) Factors that increase risk include:
 - a. The ability to add value to a prepaid card using cash increases due to difficulties in determining the legitimacy of the source of the cash. Cash poses the highest potential risk because cash is anonymous and provides no transaction history. Loading value onto a prepaid card using cash increases the risk that such a card program will be subjected to criminal abuse.
 - b. Unknown sources of funding of the prepaid card, such as with cash. Anonymous funding methods, obscuring the source of the funds, creates a higher risk.
 - c. Other monetary instruments that provide anonymity as to the source or owner of the funds, or by means of a funds transfer from an unknown third-party, for example, third-party wire or check.
- (4) Factors that decrease risk include:
 - a. A known source of funds, such as a transfer from an existing financial institution account of the purchaser or receiving funds from a known, trusted source, such as a government agency or an employer (for an employee's compensation or for other benefits from the employer).
 - b. Review and controls are in place for locations where the funding can be done.
 - c. Card value cannot be funded with cash.
 - d. Cash loading is limited to a specific amount, where identification is requested at the time of loading, or where other mitigating safeguards are employed. See IRM 4.26.9.12.8.
 - e. Require customer identification if the cash exceeds a predetermined cash load limit either for an individual account or for one or a series of transactions in a day.
 - f. Limits on person to person transfers.
 - g. If funding methods include cash or third-party wire/check, verify the cardholder's identity. Setting limits on loads and spending, monitoring transactions, and prohibiting cash access and reloading mitigate risk.

4.26.9.12.7.8
(11-12-2019)

Funding by Value Transfer

- (1) Prepaid card programs carry increased money laundering risk when the cards can be loaded online by value transfer from another card (prepaid, debit, or credit) due to the relative ease of transferring funds electronically and the lack of face-to-face contact.

- (2) Card programs increase their risk when card holders are allowed to value transfer between unrelated cardholders or they are allowed to transfer with other prepaid access programs.
- (3) Card programs decrease risk when no value can be loaded from another card and value transfers between unrelated cardholders are not allowed.

4.26.9.12.7.9
(11-12-2019)
Value Limits

- (1) Potential card value can be controlled by card program features such as:
 - a. Imposing a maximum amount of funds that can be loaded onto a card in any instance.
 - b. Imposing a maximum amount of total value that can be held on the card at any given time (ceiling/card limit).
 - c. Limits on aggregate card values.
 - d. The number of times, or total value with which a card can be reloaded in each period. These features may be applied to a single transaction or in aggregate.
- (2) In general, lower load capacity results in lower potential money laundering risk, due to the necessity of using more cards to launder a given amount of funds.

4.26.9.12.7.10
(11-12-2019)
**Cash Withdrawal via
Automated Teller
Machine (ATM)/Cash
Redemption**

- (1) Mobile and Internet payment services are increasingly connected with prepaid cards, which indirectly allow access to cash withdrawals. Access to cash through the ATM network increases risk level. Some prepaid cards allow funding in one country/area and cash withdrawals in another.
- (2) Cash access from a prepaid card presents unique challenges to assessing risks. In some instances, merchants' POSs may be used to withdraw cash by overpaying for merchandise and receiving the overpaid amount in cash.
- (3) Features that increase risk include:
 - a. Cash access from a prepaid card, such as through ATM withdrawals or other access points, increase the potential that the card will be used for money laundering purposes, as does the ability to redeem the card value for cash. Note, however, that for some prepaid card programs (for example, a card issued through a government benefits program or employer payroll program), withdrawing cash via an ATM could be considered entirely consistent with anticipated card use.
 - b. Merchants' POS may be used to withdraw cash by overpaying for merchandise and receiving the overpaid amount in cash (cash back).
- (4) Features that decrease risk include:
 - a. Inability to withdraw cash from an ATM or receive cash back at the POS.
 - b. Maximum dollar thresholds on ATM withdrawals or cash back at the POS and on the number of withdrawals/cash back within a specific period (velocity or speed of fund use).

4.26.9.12.7.11
(11-12-2019)

Intended Scope of Card Use

- (1) Prepaid access programs can be designed to limit use to a specific merchant or shopping establishment (for example, a shopping mall) - a closed loop card program. Some open loop card programs are designed to offer broader access to the full range of merchants capable of accepting that type of branded card - an open loop card program. Other open loop card programs may restrict use by merchant industry types (for example, not accepted for purchases related to casino activities).
- (2) A feature that increases risk is:
 - a. Card programs that have no restrictions on nature and/or place of use or transaction/velocity limits on card use.
- (3) Features that decrease risk include:
 - a. Limitations on the use of the card to one or a limited number of merchants.
 - b. The inability to use the prepaid card for higher risk activities for example, card use restricted to targeted merchant types.
 - c. Transaction/velocity limits on card use.

4.26.9.12.7.12
(11-12-2019)

Third-Party Relationships

- (1) A third-party relationship is any business arrangement between the Provider and another entity, by contract or otherwise.
- (2) A Provider's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in compliance with the BSA.
- (3) Prepaid access programs may involve several parties to perform services and execute payments such as the Provider, issuer, payment network, distributor, and Seller.
 - a. The interactions of these parties generate risk due to the potential of segmentation and loss of customer and transaction information.
 - b. This risk may be compounded if important services are outsourced to potentially unregulated third parties without clear lines of accountability and oversight, or that are located abroad.
 - c. This is concerning when it is not clearly established which entities are subject to AML obligations, who is responsible for complying with such obligations, and what country (among those involved in the transaction process) is responsible for regulating and supervising AML compliance measures.
- (4) Providers often use third parties for cash acceptance and withdrawals, and to establish new customer relationships. Use of and reliance on unaffiliated third parties for establishing customer relationships and reloading raises risk levels, particularly if the collected information is not shared with the entity responsible for AML requirements.
- (5) A Provider, responsible for all aspects of the customer relationship (such as registration, cash-in/cash-out, and transactions), can lower the risk. Of relevance is a strong AML program with management, control and oversight of the third-party network.
- (6) Factors that increase risk include non-face-to-face transactions such as:

- a. Direct Mail
- b. Internet sales
- c. Telephone sales
- d. Services offered through third-party unregulated entities (such as retailers)

(7) Factors that decrease risk:

- a. Sold via face-to-face
- b. Collection and verification of cardholder information
- c. Monitored transactions are monitored
- d. Limits on loads/spending and ATM transactions
- e. Short prepaid card expiration dates

4.26.9.12.8
(11-12-2019)
Risk Mitigation

- (1) Transaction monitoring and suspicious activity reporting is essential. Its importance is greater where obtaining reliable information on the customer may be difficult.
- (2) As part of their system of internal controls, Providers and Sellers must establish a means for monitoring, identifying, and reporting suspicious activity related to prepaid access programs. Procedures to obtain regular card transaction information from processors or other third parties must be established.
- (3) Monitoring systems should identify foreign card activity, bulk purchases made by one individual, and multiple purchases made by related parties. In addition, procedures should include monitoring for unusual activity patterns, such as cash card loads followed immediately by withdrawals of the full amount from another location.
- (4) Many prepaid card programs monitor activity to detect suspicious activity, such as:
 - a. Loads and reloads
 - b. Purchases and withdrawals
 - c. Inactive and dormant accounts
 - d. Multiple accounts or prepaid card products held by an individual or group
 - e. Use of Social Security Number (SSN) - Review transactions using the same SSN for abnormal activity during rolling periods – daily, weekly, monthly, and quarterly
 - f. International ATM and debit transactions
 - g. Cardholder P-to-P transactions
 - h. Non-financial transactions (email, address, PIN changes done in conjunction with certain financial transactions, and others)
 - i. Location-level monitoring of retail partner card sale and load activity, for example, peer groups of retail partners by geographic area (for example, city, zip code, and others)

4.26.9.12.9
(11-12-2019)
Examination Procedures

- (1) The objective of conducting an examination of a Prepaid Access Provider/Seller is to confirm that an AML Program has been developed and implemented, is administered appropriately, and to assess the adequacy of its policies, procedures and practices in ensuring compliance with the required BSA regulations.

4.26.9.12.9.1
(11-12-2019)
Pre-Plan

- (2) The Title 31 MSB Lead Sheet Package is available on the BSA SharePoint and should be used to guide the administrative actions of a Prepaid Access examination.
- (3) The examination must be conducted at the prepaid Provider's/Seller's business location.
- (1) Due to the nature and complexity of prepaid access and the volume of records, the BSA examiner will need to recruit the assistance of a Computer Audit Specialist (CAS) in conducting most, if not all, prepaid access examinations. Depending on the volume of the transactions, and the complexities involved, the audit team may include one or more BSA examiners, a CAS, and support personnel.
- (2) Contact the CAS early in the examination planning. The CAS should be present at the initial interview (if possible, have the CAS attend the opening conference to facilitate the examination's expeditious progress). To request a CAS, visit <https://srs.web.irs.gov/>.
- (3) Guidance for workpaper #105, *Administrative Plan to Close Lead Sheet*, is available at IRM 4.26.6.5.3, *Examination Process*, and on the BSA SharePoint. The workpaper is used as a guide for the examination planning phase.
- (4) Guidance for workpaper #110, *Preplan Analysis*, is available at IRM 4.26.6.5.1, *Preplan*, and on the BSA SharePoint. The preplan is the initial administrative step in conducting an examination. Details follow on creating forms that organize the examination administrative file and analyzing available information to develop the examination plan.
- (5) The examiner adjusts the audit preplan to include information gained from the interview and the random sample.

4.26.9.12.9.2
(11-12-2019)
Initial Contact

- (1) **ALL** initial taxpayer contacts must be made by mail to combat phone scams, phishing, and identity theft.
- (2) Examiners will use Letter 4313, *Bank Secrecy Act Money Services Business Examination Appointment*, to notify the MSB of its selection for examination and will not make initial contact by telephone. After mailing the contact letter and allowing sufficient time for the taxpayer to respond (14 calendar days from mailing the letter), employees can then initiate contact by telephone with the taxpayer as needed.
- (3) When a valid Form 2848, *Power of Attorney and Declaration of Representative*, or Form 8821, *Tax Information Authorization*, is on file for the taxpayer, the initial contact letter will be mailed to the taxpayer and a copy of that letter will be mailed to the representative with Letter 937, *Transmittal Letter for Power of Attorney*.
- (4) Publications sent to the taxpayer should always agree with the enclosures listed on the taxpayer's cover letter to avoid confusion. However, blank forms and publications available on <https://www.irs.gov/> should not be included when sending copies of letters and the information document requests with Letter 937 to representatives and appointees.
- (5) This guidance is consistent with the instructions for Form 2848 and Form 8821.

4.26.9.12.9.3
(11-12-2019)
Scope and Depth

- (1) The scope and depth of each Title 31 examination will depend on the facts and circumstances of each case.
- (2) Depending on initial findings, the examiner may expand the scope and/or depth of the review to include additional periods.

4.26.9.12.9.4
(11-12-2019)
Interviews

- (1) Thorough interviews are essential to a quality BSA examination. Interview questions should be tailored to the party interviewed and the levels of responsibility. Document all responses to the interview questions in the case file.
- (2) Familiarity with the prepaid industry terminology and operations will optimize the benefits of the interview. Ask the interviewee probing questions to gain a clear understanding of the prepaid operations.
- (3) Conduct interviews from the “top down”. Upper management and the BSA compliance officer should be the first interviewed, as they should have institutional knowledge of the Provider’s/Seller’s background and commitment to BSA compliance.
- (4) Interviews may be conducted with supervisory personnel with managerial oversight for employees responsible for reviewing and monitoring prepaid transactions and filing BSA reports.
- (5) Conduct interviews with the staff responsible for loading, reloading, activating, and monitoring the prepaid products; and for filing BSA reports to gain insights with daily processes.
- (6) Conduct the interviews and examination at the provider’s business location. Ensure that a tour of the business is conducted to confirm and clarify information obtained during the interview. Being on-site will help to ensure a thorough understanding of the business activities and environment in which the Provider/Seller operates.
- (7) There may be a need, on a case-by-case basis, to interview the customer to obtain all the facts as required to develop the issues.

4.26.9.12.9.5
(11-12-2019)
The AML Compliance Program

- (1) The required elements of an AML compliance program for a Prepaid Provider/Seller are:
 - a. A written system of policies, procedures, and internal controls to ensure ongoing compliance, commensurate with the Provider’s/Seller’s BSA/AML risk profile with clearly defined roles and responsibilities with appropriate separation of administrative and reviewer responsibilities.
 - b. Designated BSA Compliance Officer(s) responsible for managing BSA compliance.
 - c. Training for appropriate personnel.
 - d. Independent testing of BSA compliance.

4.26.9.12.9.5.1
(11-12-2019)
Examining the AML Compliance Program

- (1) The examiner reviews the Provider’s/Seller’s management-approved, written AML Compliance Program to:
 - a. Ensure it contains the required elements.
 - b. Gain a clear understanding of the policies, procedures and processes designed to ensure BSA compliance.

- c. Ensure that there are internal controls are in place to prevent, detect, and limit the risks of a prepaid product being used to launder money or facilitate terrorist financing.
 - d. Ensure its effective administration.
- (2) The examiner determines whether the AML program policies, procedures, and processes are adequate and effective by:
 - a. Identifying higher-risk operations (products, services, customers, third parties, and geographic locations).
 - b. Reviewing the provider's risk assessment and procedures for updating that assessment.
 - c. Reviewing risk-based customer due diligence policies, procedures, and processes.
 - d. Reviewing policies and procedures that mitigate effectively the identified risks.
 - e. Reviewing the Provider's notes and corporate minutes for updates regarding compliance initiatives, identified compliance issues and deficiencies, and corrective actions taken.
 - f. Ensuring one or more persons are assigned responsibility for BSA/AML compliance.
 - g. Determining continuity if there are changes in management, employee composition, or organizational structure.
 - h. Determining if the Provider meets all regulatory recordkeeping and reporting requirements, implements recommendations for BSA compliance, and provides timely updates in response to regulatory changes.
 - i. Determining if third parties, such as the Sellers, are adhering to the Provider's policies, transaction thresholds, and any other guidelines; and whether third-party risk is managed effectively through policies and procedures that guide the Provider's evaluation, selection, and oversight of the third-party's (processors, Sellers and distributors) activities.
 - j. Performing transaction testing to document the effectiveness of the Provider's internal controls.

4.26.9.12.9.5.2
(11-12-2019)

Examination Techniques

- (1) The examiner should follow the examination steps outlined in the *AML Compliance Program Lead Sheet Title 31 (# 140)*, available on the BSA SharePoint.
- (2) To perform an effective BSA examination, it's critical to develop an adequate understanding of the provider's processes. This can be achieved by documenting the process in a narrative or flow chart. Process narratives and flowcharts generated should be an accurate representation of how the work is performed and how transactions flow.
- (3) Document the prepaid products, activation of the prepaid products, verification of customer, the types of payment accepted, the process for loads and reloads, limits, and monitoring. The purpose of understanding and documenting the provider's processes and workflow will allow you to organize, describe, and depict graphically the results of:
 - a. Reviewing the policies and procedures.
 - b. Discussing the process with key employees.
 - c. Performing a process walk through of the provider's operation and business activities, using samples, and other similar items.
 - d. Identifying key inputs and outputs of the prepaid access activities.

- e. Identifying lines of responsibility for individual employees and departmental roles at each step of the process.
 - f. Identifying key records and documents associated with each processing step.
 - g. Identifying key risks and controls and when, whom, and how risks are mitigated.
- (4) An accurate and complete documentation of the company's process as it pertains to prepaid access serves as a baseline for testing risk assessment, internal controls, monitoring, and overall effectiveness of the AML Compliance Program.

4.26.9.12.9.5.3
(11-12-2019)
Examining for Suspicious Activity Monitoring and Reporting

- (1) The examiner should be alert to identify suspicious transactions that do not make business sense and appear to be performed in a manner to avoid the SAR and CTR reporting requirements.

4.26.9.12.9.5.3.1
(11-12-2019)
Transaction Testing

- (1) The examiner reviews the AML Compliance Program policies, procedures, and processes prior to any transaction testing.
- (2) If a business uses a computerized system, the examiner must perform testing to ensure its integrity before relying upon such records.
- (3) See IRM 4.26.6.5.1.3, *BSA Examination Techniques*, for guidance on reviewing downloads of records, and addressing instances when records require a combination of manual examination and computer auditing techniques.
- (4) When violations are found, the BSA examiner should document the facts and circumstances with respect to the violation and advise Prepaid Access management of findings and solicit an explanation as to why each violation occurred.
- (5) See IRM 4.26.13, *Structuring*, if structured transactions are detected.

4.26.9.12.9.5.3.2
(11-12-2019)
Red Flags

- (1) Red flags can indicate suspicious activity where a product's actual use deviates from its intended use or does not make economic sense. Red flags should therefore be tailored to the product's features. For example, cash withdrawals in foreign jurisdictions will be expected where the product is a prepaid travel card, but unusual where the product is marketed to minors.
- (2) The examples below are indicative of suspicious activity but would need further investigation of the facts and circumstances in each case to confirm suspicions. These examples are not exhaustive.
- (3) Suspicious activity indicators related to customer ID include:
- a. Discrepancies between the information submitted by the customer and information detected by monitoring systems.
 - b. A customer who presents unusual or suspicious identification documents that the financial institution cannot readily verify.
 - c. A customer uses different tax identification numbers with variations of his or her name.

- d. A customer who is reluctant or unwilling to provide the needed information for a mandatory report.
 - e. A customer who is reluctant or unwilling to have the report filed.
 - f. A customer who is reluctant or unwilling to proceed with a transaction after being informed of a required report filing.
- (4) Suspicious activity indicators related to customer actions include:
- a. A cardholder that coerces or attempts to coerce an employee not to comply with required recordkeeping or file reporting forms.
 - b. A customer with an excessive number of cards (based on program parameters).
 - c. Individuals who hold an unusual volume of prepaid access accounts with the same provider.
 - d. A customer who requests a shipment of cards outside of the U.S.
 - e. A customer who has a U.S. mailing address but an Internet Protocol (IP) address in high-risk foreign country.
- (5) Suspicious activity indicators related to transactions include:
- a. Prepaid access account used only for withdrawals, and not for POS or online purchases.
 - b. Atypical use of the payment product (including unexpected and frequent cross-border access or transactions).
 - c. Multiple withdrawals conducted at different ATMs (sometimes located in various geographic areas or countries different from jurisdiction where prepaid access account was funded).
 - d. Multiple transactions slightly below reportable thresholds.
 - e. Large number of failed authorizations.
 - f. Transactions posted to the card account without corresponding authorizations.
 - g. Transactions occurring in more than one state or country on the same day.
 - h. Repetitive transactions occurring at the same time for the same amount each day or each week.
 - i. Transactions consistently occurring outside of the cardholder's residential area.
 - j. Repeated transactions outside of the cardholder's normal activity.
 - k. Unexplainable transactions with seemingly no logical purpose.
 - l. Multiple value loads on the same day at different load locations.
 - m. Numerous cash loading, just under the reporting threshold, of the same prepaid card(s), conducted by the same individual(s) on several occasions (for example, structured loading of prepaid cards).
 - n. High-dollar deposits followed by numerous small withdrawals.
 - o. Wire transfers originating by dealers in foreign exchange to Prepaid Access Providers. The wires are in large, round amounts and sent through several other dealers in foreign exchange. Their economic purpose is not evident.
- (6) Suspicious activity indicators related to source of funds include:
- a. Large and diverse sources of funds (for example, bank transfers, credit card, and cash funding from different locations) used to fund the same prepaid access account(s).
 - b. Multiple bank accounts located in various cities used to fund the same prepaid access account.

- c. Loading or funding of account always done by third parties.
- d. Multiple third-party funding activities of a prepaid access account followed by the immediate transfer of funds to unrelated bank account(s) or P-to-P transfers.
- e. Multiple loading or funding of the same accounts, followed by ATM withdrawals shortly afterwards, over a short period.

(7) Indicators of suspicious activity by the Prepaid Access Company include:

- a. Large number of bank accounts held by the same Prepaid Access Company (sometimes in different countries) apparently used as flow-through accounts (may be indicative of layering activity).
- b. A Prepaid Card Company located in one country but holding accounts in other countries (unexplained business rationale, which could be suspicious).
- c. Back and forth movement of funds between bank accounts held by different prepaid cards companies located in different countries (may be indicative of layering activity if it does not fit the business model).
- d. The volume and frequency of cash transactions (sometimes structured below reporting threshold) conducted by the owner of a prepaid card company, which does not make economic sense.

4.26.9.12.10
(11-12-2019)

Pre-Paid Access and Tax Refund Fraud

- (1) One rapidly growing trend is the misuse of prepaid cards by criminals engaged in income tax refund fraud. Because prepaid cards can be designed to allow consumers to receive direct deposits on prepaid cards, these cards are ideal vehicles to receive refunds derived from fraudulent tax returns filed by criminals.
- (2) A form of tax refund fraud occurs when a criminal files a false tax return using another person's identifying information (identity theft). The submitted refund return is processed by the IRS or state revenue office and a tax refund is issued in the name of the taxpayer. The refund is transferred electronically to the purported taxpayer per the payment instructions submitted with the tax return, which specify the bank routing number and account number to which the prepaid card will credit. Once the refund posts to the prepaid card, the criminal controlling the card can access the funds via ATM withdrawals, cash advances, and purchases. A criminal may attempt to use the same prepaid card to facilitate multiple fraudulent tax refund attempts.

4.26.9.12.10.1
(11-12-2019)

Prepaid Access Red Flags for Tax Refund Fraud

- (1) Below are several red flags the examiner should be aware of and that will assist with identifying potentially fraudulent tax refunds.
 - a. Multiple direct deposit tax refunds, from the U.S. Department of the Treasury or state or local revenue offices that are directed to different individuals and made to a prepaid access account held in the name of a single account holder.
 - b. An individual opening multiple prepaid card accounts in different names, using valid Taxpayer Identification Numbers (TINs) and respective names, and having the cards mailed to the same address. Shortly after card activation, ACH credits representing tax refunds from Treasury, state or local revenue offices, occur, followed quickly by ATM cash withdrawals and/or POS purchases.

- c. Multiple prepaid cards, which receive tax refunds as the primary or sole source of funds and that are associated with the same physical address, telephone number, e-mail address, or Internet Protocol (IP) address.
- d. Individuals involved in criminal activity may also contact the customer service departments requesting a change of address/contact information for the permanent prepaid card shortly after opening on-line a temporary prepaid card account.
- e. Individuals using accounts where most of the transactions are ACH federal tax refunds or refund anticipation loans.
- f. Suspicious account openings requested on behalf of individuals who are not present, with the fraudulent individual named as owner of the prepaid card, especially if the source of funds is limited to direct deposit of tax refund proceeds. (This may indicate exploitation of elderly, minor, imprisoned, disabled, or recently deceased individuals).
- g. Account holders attempting to load tax refund checks via remote image or deposit capture.
- h. Inconsistent data supplied during application, for example, providing a Texas phone number but a Michigan address.
- i. Tax refunds deposited to accounts with recently added secondary card-holders.
- j. Multiple prepaid cards mailed to the same physical location or general geographic vicinity (for example, same street address but different apartment numbers).
- k. Unrelated accounts linked by suspicious and unusual email formats (for example, abcdefg@hotmail.com; bcdefgh@hotmail.com, and other similar accounts) or other similar data elements, such as similar refund amounts.
- l. Timing of tax refund, particularly if the refund is received outside the traditional tax season (typically January through May).
- m. The freezing or closure of an account due to suspicious activity involving either Treasury tax refund checks or ACH Treasury deposits.
- n. Third-party employees may also facilitate tax refund fraud by conducting transactions inconsistent with normal activity, such as opening multiple prepaid access accounts that receive a large quantity of Treasury refunds.
- o. Employees who do not follow proper identification procedures or who accept apparent fraudulent identification when opening a prepaid access account.

- (2) See also FinCEN advisory FIN-2013-A001, Update on Tax Refund Fraud and Related Identity Theft, issued February 26, 2013 and is available at <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2013-a001>

4.26.9.12.10.2
(11-12-2019)

**Detecting and Stopping
Fraudulent Tax Refunds**

- (1) Fraudulent tax refund activity can be detected by prepaid card providers who should file a SAR, potentially containing information useful to an investigation.
- (2) There are some ways prepaid access providers can assist in identifying and preventing fraudulent tax refunds in connection with their prepaid program, which includes:
 - a. Know the Customer. The provider should properly authenticate an applicant's identity. This is a critical step in mitigating the risk of identity theft and preventing tax refund fraud. The provider should ensure they have a written customer identification program, which includes reasonable procedures to allow them to verify the identity of each applicant, particularly before cash access is enabled on the account. See IRM 4.26.9.12.7.1.

- b. Monitor Accounts. Account monitoring, both at the time of account opening and on an ongoing basis, is essential to identifying and preventing tax refund fraud. Effective monitoring includes establishing account parameters. For example, number of reloads or dollar limits for associated accounts. Establish triggers to assist in identifying any red flags or suspicious activity that suggests an account is being used to facilitate identity theft or fraudulent refunds.
- c. Follow-up on suspicious transactions. The Provider can attempt to contact the account holder to confirm account opening and discuss suspected fraudulent activity. The Provider can also block or return direct deposits or other transactions that exceed account parameters or appear to be fraudulent.
- d. File SARs.

4.26.9.12.11
(11-12-2019)
**Verifying Seller
Monitoring**

- (1) When considering a new retail partner, a provider evaluates several categories with respect to the retailer. The initial screening process will help determine if the retailer is qualified to become a seller. After the initial screening, if the provider determines that an acceptable partner has been identified, it may continue to evaluate factors such as financial risk, OFAC check, due diligence checks, and credit and reputational risks. The issuing banks of the provider's prepaid cards may also be involved in this process.
- (2) A provider may monitor the relationships with the sellers by setting various transaction thresholds. Various categories can be used to ascertain suspicious activity, such as the number of cards sold, number and amount of loads to cards, cash withdrawals, and total activity for a given retail partner location.

4.26.9.12.12
(11-12-2019)
Finalizing the Exam

- (1) Determine compliance with the AML program requirement under 31 CFR 1022.210, *Anti-money laundering programs for money service businesses*.
- (2) Accumulate all pertinent findings from the examination performed. Evaluate the thoroughness and reliability of any risk assessment conducted by the prepaid provider. Determine whether:
 - a. The AML program is effectively monitored and supervised in relation to the prepaid provider's risk profile as determined by the risk assessment.
 - b. The AML program is effective in mitigating the prepaid provider's overall risk.
 - c. The board of directors and senior management are aware of BSA regulatory requirements; effectively oversee BSA/AML compliance; and commit, as necessary, to corrective actions (such as, independent reviews and regulatory examinations).
 - d. Policies, procedures, and internal controls are adequate to ensure compliance with applicable laws and regulations and provide sufficient risk management to appropriately address high-risk operations (goods, services, customers, suppliers, counterparties, and geographic locations).
 - e. Independent testing (audit) is appropriate and adequately tests for compliance with required laws, regulations, and policies.
 - f. The designated person responsible for coordinating and monitoring day-to-day compliance is competent and has the necessary resources.
 - g. Personnel are sufficiently trained to adhere to legal, regulatory, and policy requirements.

- h. Reportable transactions have been identified and required forms have been filed timely and accurately.
 - i. Information and communication policies, procedures, and processes are adequate and accurate.
- (3) Determine whether deficiencies or violations were previously identified by management, independent reviews, or in a prior regulatory exam, or were only identified because of the current BSA examination.
- (4) Determine the underlying cause of any violations such as (the list is not all inclusive):
 - a. Management has not assessed, or has not accurately assessed, the prepaid provider's AML risks.
 - b. Management is unaware of relevant issues.
 - c. Management is unwilling to create or enhance policies, procedures, and internal controls.
 - d. Management or employees disregard established policies, procedures, and internal controls.
 - e. Management or employees are unaware of or misunderstand regulatory requirements, policies, procedures, or internal controls.
 - f. High-risk operations (goods, services, customers, suppliers, counterparties, and geographic locations) have grown faster than the capabilities of the AML program.
 - g. Changes in internal policies, procedures, and internal controls are poorly communicated.
- (5) The examiner must hold a closing conference with the owner, corporate officer or general partner. Other employees, such as the BSA compliance officer and person responsible for filing required BSA forms may be asked to attend to assist in addressing specific items. The examiner must:
 - a. Review with the business deficiencies in the AML compliance program.
 - b. Advise the prepaid provider of any recordkeeping deficiencies.
 - c. Identify actions needed to correct any outstanding deficiencies or violations, including the possibility of requiring the prepaid provider to conduct a more detailed risk assessment.
 - d. Obtain an explanation for all issues discussed.
 - e. Review any additional documents or information provided by the prepaid provider and determine whether any items should be removed from the list of violations.
 - f. Solicit an amended AML program if there is an AML program deficiency.
 - g. Ask the business to provide a written statement of the corrective actions they will undertake to address the issues noted.

4.26.9.12.13
(11-12-2019)
Closing a Case

- (1) Complete the workpaper BSA Violations Summary Form Title 31.
- (2) The examiner should hold a closing conference with the owner, corporate officer, or general partner. Other employees, such as the BSA compliance officer and person responsible for filing reports may be asked to attend to assist in addressing specific items.
 - a. The examiner should first review with the business issues (or problems) with the compliance program, the transaction(s) not reported, or CTRs and SARs filed incompletely or incorrectly.
 - b. Obtain an explanation for all issues discussed.

- c. Ask the business to provide a written statement of the corrective actions they will undertake to address the issues noted.

- (3) If there are no Title 31 violations, issue Letter 4029, *Bank Secrecy Act No Change Letter*.
- (4) If the Title 31 violations do not meet the standards for a FinCEN referral, the examiner should issue Letter 1112, *Title 31 Violation Notification Letter*.

Note: Do not use Letter 1112, Form 13726, *Summary of Examination Findings and Recommendations*, or Form 13727, *Acceptance Statement*, from the IRS Forms Repository because those three documents are not linked. Use the versions on the BSA SharePoint site.

- (5) If it is determined that a referral should be made to FinCEN, follow the regular referral procedures. See IRM 4.26.8.6, *Form 5104, Report of Apparent Violation of Financial Recordkeeping and Reporting Regulations*.
- (6) Close the Title 31 case, through the group manager to BSA Examination, CTR Operations, which maintains Title 31 closed cases.
- (7) For details regarding case content, assembly and procedures see IRC 4.26.6, *Bank Secrecy Act Examiner Responsibilities*.

4.26.9.13 (11-12-2019) Virtual Currency Overview

- (1) Virtual Currency is a growing segment of the US financial system. It has grown from a fringe payment system to a platform with a daily transaction volume in the billions. The ability to quickly send thousands of dollars across the world at minimal cost, while remaining anonymous or pseudonymous, places virtual currency at a high risk of being used in money laundering, fraud, or terrorist financing.
- (2) Virtual currency allows customers to pay for real goods and services as they would with government-issued currency; however, the anonymity of virtual currency transactions continues to present risks to tax administration and law enforcement. One of the factors that give virtual currency value and appeal is the ability to exchange virtual currency for government issued currencies through virtual currency exchangers.
- (3) Virtual currency is a unique financial product that has disruptive and often complicated elements. It allows large amounts of value to be transferred quickly in person to person transactions, even though they may be on opposite sides of the world. Often, these transactions are conducted with little to no oversight or monitoring.
- (4) Virtual currency is an electronic medium of exchange that does not have all the attributes of real currencies. Virtual currencies include cryptocurrencies, such as bitcoin and litecoin, which are not legal tender and are not issued or backed by any central bank or governmental authority. Virtual currencies have legitimate purposes and can be purchased, sold, and exchanged with other types of virtual currencies or real currencies like the U.S. dollar. This can happen through various mechanisms such as exchangers, administrators, or merchants that are willing to accept virtual currencies in lieu of real currency.

4.26.9.13.1
(11-12-2019)
Virtual Currency Terminology

- (1) Virtual Currency terms as defined in the FinCEN guidance are as follows:
- a. Real Currency - FinCEN's regulations define currency (also referred to as "real" currency) as "the coin and paper money" of the United States or of any other country that: is designated as legal tender and; circulates and; is customarily used and accepted as a medium of exchange in the country of issuance. (31 CFR 1010.100(m), *Currency*)
 - b. Virtual currency - A value that can be digitally traded and functions as a medium of exchange that operates like a currency in some environments but does not have all the attributes of real currency. Virtual currency does not have legal tender status in any jurisdiction. Virtual currency may be a unit of account and/or a store of value, but when tendered to a creditor as an offer of payment, the creditor is not obligated to accept it under the laws of any jurisdiction other than under the law of contract. Virtual currency fulfills the functions of currency only by agreement within the community of users of the virtual currency.
 - c. Convertible virtual currency (CVC) has an equivalent value in real currency or acts as a substitute for real currency. It can be exchanged back-and-forth for real currency. CVC may be referred to as open virtual currency. Bitcoin is an example of CVC. CVC may be backed by commodities, which will cause the value and the available amount of the virtual currency to fluctuate as the price of the commodity fluctuates. If CVC is backed by revenue changes in value, the value and amount of the virtual currency will change, based on the revenue generated by the business. CVC can also be backed by supply and demand, which will impact the value of outstanding currency and the availability of virtual currency.
 - d. Non-convertible virtual currency – A closed virtual currency intended to be specific to a virtual domain or world, such as a Massively Multiplayer Online Role-Playing Game (MMORPG) or a specific retailer. An MMORPG is an online game played cooperatively and/or competitively with thousands, even millions, or other players. Closed currencies cannot be exchanged for fiat/real currency.
 - e. Centralized virtual currency - Have a single administering authority or administrator that controls the system. An administrator issues the currency, establishes the rules for its use, maintains a central payment ledger, and has the authority to redeem the currency or withdraw it from circulation. Examples include Amazon coins and Ven.
 - f. Decentralized virtual currency – Is a distributed, open-source, math-based peer-to-peer virtual currencies that have no central administering authority, and no central monitoring or oversight. They are also known as cryptocurrencies. Examples of cryptocurrencies include Bitcoin, Litecoin, and Ethereum.

4.26.9.13.2
(11-12-2019)
Virtual Currency Defined

- (1) On March 18, 2013, the Financial Crimes Enforcement Network (FinCEN), which is a Treasury bureau that collects and analyzes financial transaction information to combat money laundering, terrorist financing, and other financial crimes, issued interpretive guidance to clarify the applicability of the existing Bank Secrecy Act (BSA) regulations to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies. The guidance defines virtual currency as "a medium of exchange that operates like a currency in some environments but does not have all the attributes of real currency. Virtual

currency does not have legal tender status in any jurisdiction". See <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>, for a copy of the FinCEN guidance.

- (2) Virtual currency is not "real" or fiat currency. Fiat currency is the name for what is traditionally recognized as currency. Fiat currency is the coin and paper money of a country and designated as its legal tender. It is the currency that circulates and is customarily accepted as a medium of exchange in the issuing country. Virtual currency is also different from fiat currency in that it does not exist in a physical form.
- (3) On May 9, 2019, FinCEN issued interpretive guidance to remind persons subject to BSA how FinCEN regulations relating to money services businesses (MSBs) apply to certain business models involving money transmission denominated in value that substitutes for currency, specifically, convertible virtual currency (CVC). See <https://www.fincen.gov/news/news-releases/new-fincen-guidance-affirms-its-longstanding-regulatory-framework-virtual> and <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincen-regulations-certain-business-models> for more information on guidance issued by FinCEN regarding virtual currency.
- (4) On May 9, FinCEN also issued an Advisory on Illicit Activity Involving Convertible Virtual Currency to assist financial institutions in identifying and reporting suspicious activity related to criminal exploitation of CVCs for money laundering, sanctions evasion, and other illicit financing purposes. The advisory highlights prominent typologies associated "red flags", and identifies information that would be most valuable to law enforcement if contained in suspicious activity reports. See FinCEN Advisory FIN-2019-A003, *Advisory on Illicit Activity Involving Convertible Virtual Currency*, <https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf>.

4.26.9.13.3 (11-12-2019) **Virtual Currency Participants**

- (1) FinCEN guidance refers to the participants in a generic virtual currency arrangement, using the terms "user", "administrator" and "exchanger".
- (2) User – A person who obtains virtual currency to purchase goods and services. Users can obtain virtual currency in several ways:
 - a. Purchase virtual currency from an exchanger or, for certain centralized virtual currencies, directly from the administrator, using real money,
 - b. Engage in specific activities that earn virtual currency payments (such as, respond to a promotion, complete an online survey, provide a real or virtual good or service), or
 - c. With some decentralized virtual currencies (such as, Bitcoin), self-generate units of the currency by "mining" them and receive them as gifts, rewards, or as part of a free initial distribution.

A user who obtains CVC and uses it to purchase real or virtual goods or services is not an MSB under FinCEN's regulations. Such activity, in and of itself, does not fit within the definition of "money transmission services" and therefore is not subject to FinCEN's registration, reporting, and recordkeeping regulations for MSBs.

- (3) Administrator – A person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency. An administrator establishes the rules for the virtual currency use and maintains the central payment ledger for the virtual currency. An administrator that accepts and transmits a CVC or buys or sells CVC for any reason is a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person.
- (4) Exchanger – A person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An exchanger may be sometimes referred to as a virtual currency exchange. Exchangers generally accept a wide range of payments, including cash, wires, credit cards, and other virtual currencies, and can be administrator-affiliated, non-affiliated, or a third-party provider. Exchangers can act as a bourse or as an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts.

4.26.9.13.4
(11-12-2019)
Law

- (1) An administrator or exchanger is a Money Service Business (MSB) under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person.
- (2) Refer to 31 CFR 1010.100(ff), *Money service business*, and IRM 4.26.5.3, *Entities Subject to BSA*, for the definition and categories of MSBs.
- (3) The FinCEN Final Rule published July 21, 2011 amended the definition of money transmitters. (31 CFR 1010.100(ff)(5)(i)(A), *In general*)
- (4) The definition of a money transmitter does not differentiate between real currencies and convertible virtual currencies. Accepting and transmitting anything of value, that substitutes for currency, makes a person a money transmitter under the regulations implementing the BSA requirements.
 - a. Acceptance of currency and transmission of currency do not have to occur in that order. A money transmitter that operates by giving credit to a transmittor is still a money transmitter.
 - b. Under FinCEN's regulations value that substitutes for currency includes CVC. The value accepted does not have to be the same as the value transmitted.
 - c. The term "location" is not defined in the FinCEN regulations, but a transaction constitutes transmission to another location when it is from the user's account at one location (such as, a user's real currency account at a bank) to the user's CVC account with the administrator or exchanger.
 - d. Transmission to another person occurs when an exchanger accepts currency, or its equivalent, from a user and credits the user with an appropriate portion of the exchanger's own CVC held with the administrator of the repository, then the exchanger transmits the internally credited value to third parties at the user's direction.
 - e. A transmittal of funds consists of a series of transactions beginning with the transmittor's transmittal order made for making payment to the recipient of the order including any transmittal orders issued by the transmittor's financial institution and any intermediary financial institution, intended to carry out the transmittor's transmittal order.

4.26.9.13.5
(11-12-2019)
**Regulatory
Requirements**

- (1) FinCEN has determined virtual currency administrators and exchangers are a Money Services Business (MSB) conducting money transmission services. Therefore, they are required to follow the regulatory requirements for money transmitters.
- (2) Money transmitters are subject to regulatory requirements applicable to all financial institutions such as an AML program, CTR and SAR filing, and requirements applicable to any person that is not a financial institution, such as CMIR and FBAR filing, as well as specific regulatory requirements applicable to those financial institutions that are money service businesses, such as registration with FinCEN and maintaining an MSB agent list.
- (3) The regulations covering money transmitters of virtual currency are found in 31 CFR Part 1010, *General provisions*, and 31 CFR 31 CFR Part 1022, *Rules for Money Services Businesses*.

4.26.9.13.5.1
(11-12-2019)
**Registration
Requirements**

- (1) 31 CFR 1022.380(a)(1), *In general*, states a money transmitter will register as an MSB, and as part of its registration and registration renewals, it must maintain a list of its agents.
- (2) Other MSB registration requirements for money transmitters are:
 - a. Maintain a list of its agents.
 - b. Retain a copy of the registration form.
 - c. Renew the registration each two calendar-year period following the initial registration period.
 - d. Re-register if the money transmitter experiences a change in ownership or control that requires the business to be re-registered under State law; if there is a transfer of more than 10 percent of the voting power or equity interests (other than a money services business that must report such transfer to the Securities and Exchange Commission); or experiences a more than 50 percent increase in the number of its agents during any registration period.

4.26.9.13.5.2
(11-12-2019)
**Anti-Money Laundering
Program Requirements**

- (1) 31 CFR 1022.210, *Anti-money laundering programs for money services businesses*, of the regulations requires a money service business to develop, implement and maintain an effective AML program that is reasonably designed to prevent the money service business from being used to facilitate money laundering, terrorist financing, or other financial crimes. The AML program must be in writing and should clearly set forth the details of the program, including the responsibilities of the individuals and/or departments involved. To ensure the program is suitable for the business, it must be commensurate with the risks posed by the business location, size, nature and volume of financial services provided.
- (2) An AML program must be made available to the Department of Treasury or its designee upon request.
- (3) At a minimum, MSBs must establish an AML program that includes the following four elements:
 - a. Policies, procedures, and internal controls based on the MSB's assessment of the money laundering and terrorist financing risk associated with its lines of business.

- b. Designation of a compliance officer who is responsible for ensuring that the program is implemented effectively and is updated, as necessary, to reflect changes in the risk assessment, requirements of the BSA and guidance issued by the Department of Treasury; and ensuring appropriate individuals are trained on the BSA.
- c. Ongoing training of appropriate persons concerning their responsibilities under the program.
- d. Independent testing to monitor and maintain an adequate program.

4.26.9.13.5.2.1
(11-12-2019)

**AML Policies and
Procedures**

- (1) An MSB's AML program must incorporate policies, procedures, and internal controls based upon the MSB's assessment of the money laundering and terrorist financing risks associated with its line(s) of business. It must also address its filing and reporting requirements. Much of its risk will depend on its products, customers, business operations and geographic locations for receiving and transmitting funds. (31 CFR 1022.210(d)(1))
- (2) Virtual currency businesses should assess the potential vulnerability to money laundering and terrorist financing by incorporating policies, procedures, and internal controls to address:
 - a. Anonymity funding – Virtual currency systems can be traded via the Internet, which are non-face-to-face customer relationships and may permit anonymous funding.
 - b. Cash funding or third-party funding – Ensure the funding source is properly identified.
 - c. Anonymous transfers – Ensure the MSB incorporates reasonable Know Your Customer (KYC) policies and procedures to identify the sender and recipient when required by the regulations.
 - d. Segmentation of services responsibility – Ensure the responsibility for AML compliance and supervision/enforcement is clear.
 - e. Geographic reach – Customer and transactions records may be held by different entities, often in different jurisdictions.
 - f. Business operations and processes – Ensure the types/roles of participants providing services in virtual currency payments systems and platforms are clear.
- (3) The program must include policies, procedures, and internal controls to assist the MSB in monitoring and identifying transactions that may involve use of the MSB to facilitate money laundering or terrorist financing, including provisions for making reasonable inquiries to determine whether a transaction involves money laundering or terrorist financing, and for refusing to consummate, withdrawing from, or terminating such transactions.
- (4) MSBs are required to file currency transaction reports (CTRs) and suspicious activity reports (SARs).
- (5) If MSBs become subject to additional requirements, they must update their AML compliance programs to include appropriate policies, procedures, training, and testing functions relating to the additional BSA requirements.

4.26.9.13.5.2.2
(11-12-2019)

Compliance Officer

- (1) The MSB must designate a compliance officer responsible for administering the AML program. The person should be competent and knowledgeable regarding BSA requirements, money laundering issues and risks, and the MSB/money transmitters/virtual currency industry. (31 CFR 1022.210(d)(2))

- (2) The compliance officer must ensure that:
 - a. The program is properly implemented.
 - b. The program is updated, as necessary, to reflect changes in the risk assessment, current requirements, and further guidance issued by the Department of the Treasury.
 - c. The appropriate personnel are trained as necessary.

4.26.9.13.5.2.3
(11-12-2019)

Education and Training

- (1) The MSB must ensure that employees are trained concerning their responsibilities under the AML program. Employees should be trained in AML issues and be able to recognize possible signs of money laundering and terrorist financing. Training should be ongoing and should be based on the employee's responsibilities, any revisions to the law, and the activities of the MSB. (31 CFR 1022.210(d)(3))
- (2) Training can be conducted by internal or external parties and can include videos, computer-based training, booklets, and other similar items. The level, frequency, and focus of the training should be determined by the responsibilities of the employees and to the extent their functions bring them in contact with the BSA requirements, or possible money laundering activities.
- (3) The success of an MSB's AML program depends on its application throughout all the MSB's BSA business activities, including appropriate education and training of employees. An MSB should inform all employees that it has an AML program designed and intended to detect and deter money laundering and terrorist financing, and that their awareness and participation are important. MSBs should encourage and train their employees to contact management (or delegate) regarding suspicious activity that they observe or of which they become aware.

4.26.9.13.5.2.4
(11-12-2019)

Independent Testing

- (1) Independent testing is required to be conducted to ensure the AML program is adequate. It must be conducted periodically, based on the risks of the MSB's operations and should be conducted by personnel who are knowledgeable regarding BSA requirements. The testing does not need to be performed by an external party. It may be conducted by an employee, but it must be objective. Independent testing cannot be conducted by the MSB's compliance officer, anyone who reports to the compliance officer, or by a person involved in the operations of the AML program. (31 CFR 1022.210(d)(4))
- (2) There are no specific guidelines for independent testing; however, the scope of the independent testing should be adequate to test the adequacy and effectiveness of the MSB's AML program, including enough transactional testing. This may include but is not limited to:
 - a. Verifying that management has adopted and approved an AML program, conducted employee training, and appointed a compliance officer.
 - b. Ensuring that the AML program includes the appropriate elements, such as internal controls, to ensure ongoing compliance, risk assessment guidance, designation of a compliance officer, employee training, and independent testing.
 - c. Interviewing management to determine their commitment to and understanding of the program.

- d. Interviewing the compliance officer to assess his or her understanding of the law, the regulations, and the management of the business' AML program.

4.26.9.13.6
(11-12-2019)
Recordkeeping and Retention

- (1) On January 3, 1995, FinCEN issued a rule that requires banks and nonbank financial institutions to collect and retain information on certain funds transfers and transmittals of funds. ("Recordkeeping rule"— 31 CFR 1010.410(e), *Nonbank financial institutions*)
- (2) At the same time, FinCEN issued the "travel rule" (CFR 1010.410(f)), which requires banks and nonbank financial institutions to include certain information on funds transfers and transmittals of funds sent to other banks or nonbank financial institutions.
- (3) The recordkeeping rule requires financial institutions to retain information on transmittals of funds of \$3,000 or more and requires banks to retain information on funds transfers of \$3,000 or more.
- (4) Under the recordkeeping rule, if acting as a transmitter's financial institution, the financial institution must retain either the original, microfilmed, copied, or electronic record for transmittals of funds of \$3,000 or more:
 - a. The name and address of the transmitter,
 - b. The amount of the transmittal order,
 - c. The execution date of the transmittal order,
 - d. Any payment instructions received from the transmitter with the transmittal order,
 - e. The identity of the recipient's financial institution,
 - f. As many of the following items as are received with the transmittal order: the name and address of the recipient, the account number of the recipient, and any other specific identifier of the recipient, and
 - g. If the transmitter's financial institution is a nonbank financial institution, any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order. (31 CFR 1010.410(e)(1)(ii))
- (5) If acting as an intermediary financial institution, or a recipient financial institution, either the original, microfilmed, copied, or electronic record of the received transmittal order. (31 CFR 1010.410(e)(1)(ii) and 31 CFR 1010.410(e)(1)(iii))
- (6) The recordkeeping rule requires that the data be retrievable. (CFR 1010.410(e)(4)). Records required to be retained by the recordkeeping rule must be made available to Treasury upon request.
- (7) Unless there is an exemption to the definition of transmittal of funds or to the Funds Transfer Rule, for transactions \$3,000 or more the financial institutions involved in the transmission chain must do the following:
 - a. The transmitter's financial institution must obtain, verify if applicable, evaluate, and store key information from the transmitter, about the transmitter itself, and about the recipient, and the underlying transaction.
 - b. Any intermediary financial institution must receive, evaluate, and store information from the transmitter's financial institution.
 - c. The recipient's financial institution must obtain, verify if applicable, evaluate, and store key information from the recipient, about the recipient itself.

- (8) The U.S. Treasury issued a Final Rule that requires all financial institutions to include certain information in transmittal orders for funds transfers of \$3,000 or more. (31 CFR 1010.410, *Records to be made and retained by financial institutions*) The rule applies to both banks and nonbanks. (31 CFR 1010.410(f)) Because it is broader in scope, the Travel Rule uses more expansive terms, such as “transmittal order” instead of “payment order” and “transmittor’s financial institution” instead of “originating bank”. The broader terms include the bank-specific terms. This requirement is commonly referred to as the “Travel Rule”.
- (9) Under the travel rule, a financial institution, acting as the transmittor’s financial institution, must obtain and include in the transmittal order the following information on transmittals of funds of \$3,000 or more:
 - a. name and, if the payment is ordered from an account, the account number of the transmittor,
 - b. the address of the transmittor,
 - c. the amount of the transmittal order,
 - d. the execution date of the transmittal order,
 - e. the identity of the recipient’s financial institution,
 - f. as many of the following items as are received with the transmittal order: the name and address of the recipient, the account number of the recipient, and any other specific identifier of the recipient, and
 - g. either the name and address or the numerical identifier of the transmittor’s financial institution.
- (10) A financial institution acting as an intermediary financial institution must include in its respective transmittal order the same data points listed above, if received from the sender. (31 CFR 1010.410(f)(1)-(2))
- (11) Unless there is an exemption to the definition of transmittal of funds, or to the Funds Travel Rule, for transactions \$3,000 or more the financial institutions involved in the transmission chain must do the following:
 - a. The transmittor’s financial institution must pass on to the intermediary financial institution most of the information received from the transmittor.
 - b. Any intermediary financial institution must pass on to the financial institution that follows in the transmittal chain the information received from the transmittor’s financial institution.
 - c. The recipient’s financial institution must receive, evaluate, and store the information received from either the transmittor’s financial institution or an intermediary financial institution.
- (12) Funds transfers or the transmittal of funds governed by section 903(7) of the *Electronic Fund Transfer Act of 1978* (Title XX, Pub. L. 95-630, 92 Stat. 3728, 15 USC 1693, et seq.), as well as any other funds transfers that are made through an automated clearinghouse, an automated teller machine, or a point-of-sale system, are excluded from the definition of “funds transfer” and the definition of “transmittal of funds”. In other words, the funds transfer rule (recordkeeping) and funds travel rule do not apply. See the definitions in 31 CFR 1010.100, *General Definitions*.

Note: An owner-operator of a CVC kiosk (commonly called “CVC automated teller machines (ATMs) or CVC vending machines”) who uses an electronic terminal to accept currency from a customer and transmit the equivalent

value in CVC (or vice versa) qualifies as a money transmitter. See FinCEN guidance, FIN-2019-G001, issued May 9, 2019, page 17 at <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincen-regulations-certain-business-models>.

4.26.9.13.7
(11-12-2019)
Reporting Requirements

- (1) BSA-related reporting requirements for MSBs are administered by the US Department of Treasury's Financial Crimes Enforcement Network (FinCEN). Financial institutions must file reports electronically through the BSA E-Filing System. Required reports include the following:
 - a. Currency Transaction Report (CTR) – 31 CFR 1022.310, *Reports of transactions in currency*
 - b. Report of International Transportation of Currency or Monetary Instruments (CMIR) – 31 CFR 1010.340, *Reports of transportation of currency or monetary instruments*
 - c. Report of Foreign Bank and Financial Accounts (FBAR) – 31 CFR 1010.350, *Reports of foreign financial accounts*
 - d. Suspicious Activity Report (SAR) – 31 CFR 1022.320, *Reports by money services businesses of suspicious transactions*

4.26.9.13.7.1
(11-12-2019)
Currency Transaction Reports

- (1) Administrators and exchangers of virtual currency have the same requirements as other MSBs to file Currency Transaction Reports (CTRs) – 31 CFR 1010.311, *Filing obligations for reports of transactions in currency*.
- (2) A CTR is filed for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through or to a virtual currency administrator or exchanger which involves a transaction in currency of more than \$10,000.
- (3) Multiple currency transactions are treated as a single transaction if the financial institution has knowledge that they are by or on behalf of any person and result in either cash in or cash out totaling more than \$10,000 during any one business day. (31 CFR 1010.313(b), *Multiple transactions*)
- (4) A CTR is filed within 15 days following the date the reportable transaction occurred – 31 CFR 1010.306(a)(1). The CTR must be filed electronically.

4.26.9.13.7.2
(11-12-2019)
Suspicious Activity Reports

- (1) Administrators and exchangers of virtual currency have the same requirements as other MSBs to file Suspicious Activity Reports (SARs) for transactions of \$2,000 or more.
- (2) Administrators and exchangers must ensure that procedures are in place to monitor transactions for suspicious activity.
- (3) The SAR must be filed electronically.
- (4) Administrators and exchangers of virtual currency are MSBs and therefore, must file suspicious activity reports. 31 CFR 1022.320(a)(1) requires a transaction to be reported if it is conducted or attempted by, at, or through an MSB and involves funds, including aggregated funds, or other assets of at least \$2,000, and the MSB knows, suspects, or has reason to suspect that the transaction, or pattern of transactions:

- a. Involve funds derived from illegal activity or is intended to or conducted to hide or disguise funds or assets (such as, ownership, source, location) derived from illegal activity as part of a plan to violate or evade any Federal law or regulation.
 - b. Is designed to evade any requirements or regulations under the BSA.
 - c. Serves no business or apparent lawful purpose, and the MSB knows of no reasonable explanation for the transaction after examining the available facts, or
 - d. Involves use of the MSB to facilitate criminal activity.
- (5) An MSB may also file a suspicious activity report on transactions it believes are relevant to the possible violation of any law or regulation but whose reporting is not required by 31 CFR 1022.320(a)(1).

4.26.9.13.7.3
(11-12-2019)
**Other Required BSA
Reports if Warranted**

- (1) Administrators and exchangers must also file:
- a. *Report of Foreign Bank and Financial Accounts (FBAR)*, FinCEN Form 114, and
 - b. *Report of International Transportation of Currency and Monetary Instruments (CMIR)*, FinCEN Form 105.
- (2) All FinCEN Forms 105 must be filed with the customs officer in charge at any port of entry or departure.
- (3) If a virtual currency administrator or exchanger failed to file FinCEN 105 or meet the CMIR requirements, make a referral to Customs through the BSA Policy Office. See IRM 4.26.6.8, *Technical Assistance*.

4.26.9.13.8
(11-12-2019)
**Other BSA
Requirements**

- (1) Administrators and exchangers must have procedures in place for:
- a. Suspicious activity monitoring
 - b. Customer, employee and agent due diligence
 - c. OFAC screening
- (2) In accordance with the Funds Transfer and Funds Travel rules, virtual currency MSBs may be required to collect certain identifying information. In the virtual currency world, anonymity is easily obtained with the use of avatars and public spaces. Additionally, the speed at which funds can be transferred across boundaries makes it difficult to identify the origin of the funds. Due to the online nature of the business, verification of the customer's identity presents a challenge. Collecting customer information will not only address some money laundering concerns, but also will provide companies with better data with which to perform risk assessments, and to obtain a more accurate picture of their customer base and footprint, which could lead to improved business ideas and additional products to fit certain demographics, enhancing monitoring activities and other benefits to additional analytics.
- (3) The virtual currency businesses can assess customer due diligence by:
- a. Collecting and validating customer information commensurate with the risks identified in their risk assessment.
 - b. Screening new customers to ensure compliance with sanctions.
 - c. Implementing controls sufficient to protect sensitive customer information.

