DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

SMALL BUSINESS/SELF-EMPLOYED DIVISION

April 27, 2017

Control: SBSE-04-0417-0010
Expires: 04/16/2018
Impacted IRM: 4.26.9

MEMORANDUM FOR DIRECTOR, SPECIALTY EXAMINATION; CHIEF, BSA EXAMINATION; TERRITORY/GROUP MANAGERS, BSA EXAMINATION; AND BSA EXAMINERS

FROM: Alfredo Valdespino */s/ Alfredo Valdespino*
Director, Examination-Specialty Policy

SUBJECT: Addressing Prepaid Access Issues in Bank Secrecy Act Examination Cases

This interim guidance conveys new IRM 4.26.9.12 subsection, *Prepaid Access*, which contains an overview of and procedures for addressing prepaid access issues encountered in Bank Secrecy Act (BSA) examination cases.

This attached guidance is effective immediately. It will be incorporated into IRM 4.26.9, *Examination Techniques for Bank Secrecy Act Industries,* within one year from the date of this memorandum.

Contact BSA Policy Analysts Geraldine Everson or Feli Buggs, for questions regarding this memorandum.

Distribution:
www.IRS.gov

4.26.9.12 (MM-DD-YYYY) Prepaid Access Defined

(1) Prepaid access is access to funds or the value of funds paid in advance and retrievable or transferrable 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 Code of Federal Regulations (CFR), Chapter X, § 1010.100(ww).

(2) The above definition is intentionally non-technology specific to cover future advances in technology.

4.26.9.12.1 (MM-DD-YYYY) 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 Bank Secrecy Act (BSA) regulations (31 CFR Parts 1010 and 1022) applicable to money services businesses (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(b) Superseded the terms, "issuer" and "redeemer" of stored value with "providers" and "Sellers" of prepaid access.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, e.g., 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.

4.26.9.12.2 (MM-DD-YYYY) 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) 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.

(c) 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 similar to paper check settlement. Some prepaid cards (i.e., payroll cards and government-funded prepaid cards) are loaded via ACH transactions.

(d) 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.

(e) 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.

(f) 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.

(g) J-Hook - Looped end hook used by retailers in stores to display merchandise including prepaid cards.

(h) 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.
- 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).

- Loads and reloads from non-depository sources include, but are not limited to, retail store transactions (e.g., by cash, check, or credit card), wire transfers originating at an MSB, or checks payable to a party other than the prepaid access Provider.

(i) Load Fee - A fee charged when a prepaid card is loaded or reloaded with money.
(j) 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.
(k) 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.
(l) Network Branded Prepaid Card - A prepaid card displaying the logo of a card brand (e.g., 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.
(m) Network Branded Prepaid Card Association (NBPCA) - A nonprofit trade association. See www.nbpca.org.
(n) 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).
(o) Provider – The prepaid program participant that agrees to serve as the principal conduit for access to information. See IRM 4.26.9.12.4, *Prepaid Access Provider.*
(p) Reissue - The creation and issuance of a new prepaid card with the same card number and expiration date as the previous card.
(p) Remittance Card - A prepaid card that facilitates transfers of funds by consumers, usually to friends/family in their home countries.
(q) 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 4.26.9.12.5.1.1, *Who Is Not Required to Register.*
(r) 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.
(s) Value Chain - The entities that play a role in making prepaid products available might include the issuer/issuing bank, program manager, processor, and distributor.

(3) 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 (MM-DD-YYYY) 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).

(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 postings are available at https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-regarding-prepaid-access and https://www.fincen.gov/resources/statutes-regulations/guidance/final-rule-definitions-and-other-regulations-relating, respectively.

4.26.9.12.3.1 (MM-DD-YYYY) 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).
  (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. See IRM 4.26.9.12.3.2.3, *Employment-Related Limited Exclusions*
  (c) 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.
  (d) Allows loading of additional funds from non-depository sources.

4.26.9.12.3.2 (MM-DD-YYYY) 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 (MM-DD-YYYY) 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).
      - 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 (MM-DD-YYYY) 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 (MM-DD-YYYY) 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 (MM-DD-YYYY) 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 (MM-DD-YYYY) 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, etc.

(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 4.26.9.12.6.7, *Red Flags,* for more details.

(6) An entity reloading prepaid access from a non-depository source is considered to be a "Seller," subject to the regulations, if it:

(a) Both 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.

- The phrase "can be used before verification of customer ID" refers only to use of features of a prepaid access product that qualify as a prepaid program under the regulations.

Example 1 - 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. ***Note:*** The above 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 2 - 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.

- 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.

4.26.9.12.5 (MM-DD-YYYY) 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 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.

4.26.9.12.5.1 (MM-DD-YYYY) 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. 31CFR § 1022.380(d)(1).
   (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).
   (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) The Provider only is required to register. 31 CFR § 1022.380.

4.26.9.12.5.1.1 (MM-DD-YYYY) 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)). A Seller of prepaid access, as defined in 31 CFR § 1010.100(ff)(7), 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 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) The 31 CFR § 1010.100(ff)(8)(i) 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.

4.26.9.12.5.2 (MM-DD-YYYY) 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.

4.26.9.12.5.3 (MM-DD-YYYY) 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

4.26.9.12.3.1 (MM-DD-YYYY) 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). 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 (e.g., location, size, customer, prepaid product features, volume of the particular 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); and
(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 31CFR § 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.

4.26.9.12.3.2 (MM-DD-YYYY) Customer Identification Requirements

(1) The 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 (e.g., convenience stores, 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.

4.26.9.12.3.3 (MM-DD-YYYY) Suspicious Activity Reports

(1) The 31 CFR § 1022.210(d)(1)(iv) requires Sellers of prepaid access 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.

(a) A CTR is filed for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, though, 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). See IRM 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). The CTR must be filed electronically with FinCEN.

(2) 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:

(i) Involve funds derived from illegal activity or is intended to or conducted to hide or disguise funds or assets (e.g. ownership, source, location) derived from illegal activity as part of a plan to violate or evade any Federal law or regulation;

(ii) Is designed to evade any requirements or regulations under the BSA,

(iii) Serves no business or apparent lawful purpose and the MSB knows of no reasonable explanation for the transaction after examining the available facts, or

(iv) Involves use of the MSB to facilitate criminal activity.

(3) A Provider or Seller may also file a SAR on transactions it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by 31 CFR § 1022.320(a)(1).

4.26.9.12.3.4 (MM-DD-YYYY) Recordkeeping Requirements

(1) Section 1022.420 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 the prepaid access last use.
   (c) Sellers must retain customer identification information for five year from the date the prepaid access was sold.

4.26.9.12.3.4.1 (MM-DD-YYYY) 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)

4.26.9.12.3.4 (MM-DD-YYYY) 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.

4.26.9.12.4 (MM-DD-YYYY) 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) Many prepaid card programs have features that mitigate the BSA/AML inherent risk in prepaid access relationships and transactions. The assessment of a prepaid access program's potential money laundering risks should consider the program's features, including limitations on the source and amount of funds placed on the cards, how the cards are used, and the number of cards one person can own.

(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

4.26.9.12.4.1 (MM-DD-YYYY) 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 (e.g., 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.

4.26.9.12.4.2 (MM-DD-YYYY) 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 particular 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.

4.26.9.12.4.3 (MM-DD-YYYY) 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 (e.g., 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.

4.26.9.12.4.4 (MM-DD-YYYY) Card Expiration

(1) Prepaid programs offering cards with a predetermined and limited lifespan (e.g., 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.

4.26.9.12.4.5 (MM-DD-YYYY) 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 a large number of 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, e.g., the ability to limit the use of the card to particular jurisdictions.

4.26.9.12.4.6 (MM-DD-YYYY) 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 (e.g., 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 finds data is required in addition to cardholder ID verification, enhanced due diligence on cardholders, enhanced transaction monitoring, and caps on ATM withdrawals.

4.26.9.12.4.7 (MM-DD-YYYY) 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) The means by which 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, e.g., 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 4.26.9.12.5, *Risk Mitigation*, below.
   (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.

4.26.9.12.4.8 (MM-DD-YYYY) 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 risk when value transfers between unrelated cardholders, or involve value transfers with other prepaid access programs are allowed.
(3) Card programs decrease risk when no value can be loaded from another card and value transfers between unrelated cardholders are not allowed.

4.26.9.12.4.9 (MM-DD-YYYY) 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 a given 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.

4.26.9.12.4.10 (MM-DD-YYYY) 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 (e.g., 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 timeframe (velocity or speed of fund use).

4.26.9.12.4.11 (MM-DD-YYYY) Intended Scope of Card Use

(1) Prepaid access programs can be designed to limit use to a specific merchant or shopping establishment (e.g., 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 (e.g., 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 decreases 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 (e.g., card use restricted to targeted merchant types),
(c) Transaction/velocity limits on card use.

4.26.9.12.4.12 (MM-DD-YYYY) 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 (i.e. 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) If not sold face-to-face:
   - Collection and verification of cardholder information.
   - Monitored transactions are monitored.
   - Limits on loads/spending and ATM transactions
   - Short prepaid card expiration dates

4.26.9.12.5 (MM-DD-YYYY) 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 regularly 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, etc.)
    (i) Location-level monitoring of retail partner card sale and load activity, for example, peer groups of retail partners by geographic area (e.g. city, ZIP Code, etc.)

4.26.9.12.6 (MM-DD-YYYY) 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.
(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.

4.26.9.12.6.1 (MM-DD-YYYY) Pre-Plan

(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 4.26.6.4.8.3 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 4.26.6.4.8.4 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.

4.26.9.12.6.2 (MM-DD-YYYY) Initial Contact

(1) ALL initial taxpayer contacts must be made by mail to combat phone scams, phishing, and identity theft.

(2) Examiners will use the Initial Contact Letter 4313 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 IRS.gov should not be included when sending copies of letters and the information document requests with Letter 937*, Transmittal Letter for Power of Attorney*, to representatives and appointees.

(5) This guidance is consistent with the Form 2848 instructions, and Form 8821.

4.26.9.12.6.3 (MM-DD-YYYY) 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.

4.26.9.12.6.4 (MM-DD-YYYY) 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 interviewees 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.

4.26.9.12.6.5 (MM-DD-YYYY) Assessing Risk
[Reserved]

4.26.9.12.6.6 (MM-DD-YYYY) 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.

4.26.9.12.6.6.1 (MM-DD-YYYY) 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) The 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.

4.26.9.12.6.6.2 (MM-DD-YYYY) 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, etc.
(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

(5) 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.

4.26.9.12.6.6.3 (MM-DD-YYYY) 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.

4.26.9.12.6.6.3.1 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 4.26.6.4.1.3, *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 explanations as to why each violation occurred.
(5) IRM 4.26.9, *Examination Techniques for Bank Secrecy Act Industries*, for in-depth BSA examination techniques; and IRM 4.26.13, *Structuring*, if structured transactions are detected.

4.26.9.12.6.6.3.2 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,
        - Have the report filed, or
        - 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 a number of occasions (i.e., 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 (i.e., 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 of time.

(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.

4.26.9.12.7 (MM-DD-YYYY) 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.

4.26.9.12.7.1 (MM-DD-YYYY) 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 accountholder.
   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 the majority 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, e.g., providing a Texas phone number but a Michigan address.
i) Tax refunds deposited to accounts with recently added secondary cardholders.
j) Multiple prepaid cards mailed to the same physical location or general geographic vicinity (e.g., same street address but different apartment numbers).
k) Unrelated accounts linked by suspicious and unusual email formats (e.g., abcdefg@hotmail.com; bcdefgh@hotmail.com, etc.) 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.

4.26.9.12.7.2 (MM-DD-YYYY) 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 also IRM 4.26.9.12.4.1 (MM-DD-YYYY) Knowledge about Customers.

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.

4.26.9.12.8 (MM-DD-YYYY) Verifying Seller Monitoring
[Reserved]

4.26.9.12.9 (MM-DD-YYYY) Examining Recordkeeping Compliance
[Reserved]

4.26.9.12.10 (MM-DD-YYYY) Finalizing the Exam
[Reserved]

4.26.9.12.11 (MM-DD-YYYY) Closing a Case
(1) Complete the work paper 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*, and 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 IRM 4.26.6, *Bank Secrecy Act Examiner Responsibilities.*