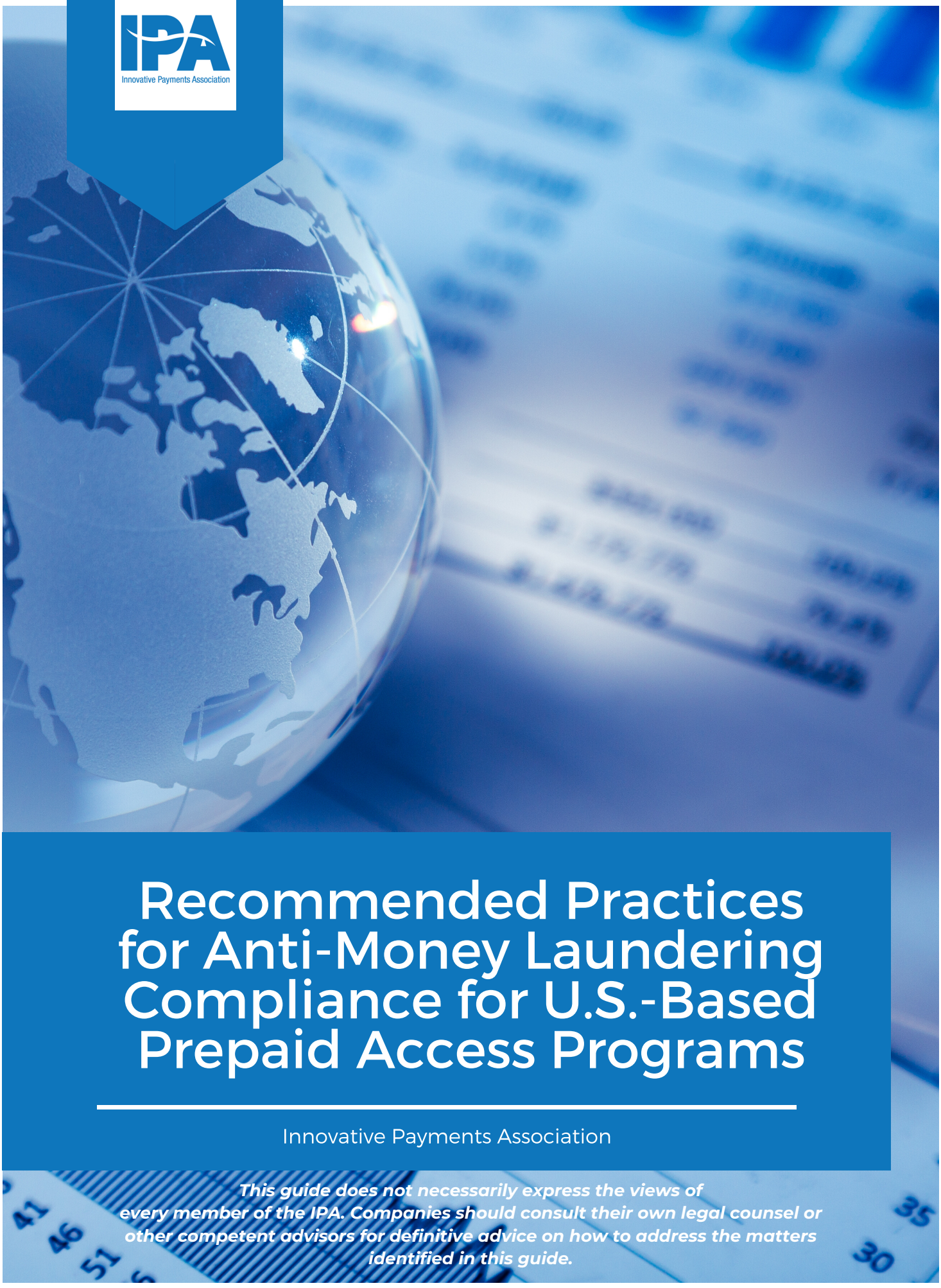


Recommended Practices for Anti-Money Laundering Compliance for U.S.-Based Prepaid Access Programs

Innovative Payments Association

This guide does not necessarily express the views of every member of the IPA. Companies should consult their own legal counsel or other competent advisors for definitive advice on how to address the matters identified in this guide.

Our Disclaimer

The information contained in these Recommended Practices is for general guidance on matters of interest only. The application and impact of authoritative guidance and laws will vary depending on the facts involved. Given the changing nature of laws, rules, and regulations, there may be omissions or errors in the information contained in these Recommended Practices.

These Recommended Practices are not intended to represent compliance with any Payment Network rules and policies for prepaid access products. Each Issuer of prepaid access must comply with the rules and policies of the applicable Payment Network(s).

Accordingly, the information in these Recommended Practices is provided with the understanding that the licensors, authors, and publishers are not engaged in rendering legal, accounting, tax, or other professional advice or services. The Recommended Practices should not be used as a substitute for consultation with professional accounting, tax, legal, or other competent advisors. Before making any decision or taking any action, you should consult a professional advisor. While we have made reasonable attempts to ensure that the information contained in these Recommended Practices is from reliable sources, the Innovative Payments Association (IPA) is not responsible for the information, any errors or omissions, or for the results obtained from using this information.

All information in these Recommended Practices is provided "AS IS," without warranty of any kind including, but not limited to, completeness, accuracy, timeliness, or of the results obtained from use of this information. There are no warranties of any kind, express or implied, including, but not limited to warranties of performance, merchantability, or fitness for a particular purpose. In no event will the IPA, its affiliates, or the members, agents, or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information contained in these Recommended Practices or for any consequential, special, or similar damages, even if advised of the possibility of such damages. This disclaimer is subject to applicable law and may not apply, or may apply only to a limited extent, in certain jurisdictions.

About the IPA

The Innovative Payments Association (IPA) is a nonprofit, inter-industry trade association that supports the growth and success of innovative payments access products and represents the common interests of the many participants in this new and rapidly growing payments category. The IPA's working groups drive issues management and education objectives for the Association's more than 60 members.

For additional information, visit www.IPA.org.

Table of Contents

GLOSSARY OF ACRONYMS

The following acronyms are used in these Recommended Practices:

AML *Anti-Money Laundering*

ATM *Automated Teller Machine*

B-TO-B *Business to Business*

BSA *Bank Secrecy Act*

CDD *Customer Due Diligence*

C.F.R. *Code of Federal Regulations*

CIP *Customer Identification Program*

CIIC *Customer Identification Information Collection*

CTF *Counter-Terrorist Financing*

CTR *Currency Transaction Report*

FATF *Financial Action Task Force*

FDIC *Federal Deposit Insurance Corporation*

Financial institution *Banks or MSBs*

FinCEN *Financial Crimes Enforcement Network*

FSA *Flexible Spending Account*

HIDTA *High Intensity Drug Trafficking Area*

HIFCA *High Intensity Money Laundering Related Financial Crimes Area*

HAS *Health Savings Account*

INCSR *International Narcotics Control Strategy Report*

MSB *Money Services Business*

NSL *National Security Letter*

OCC *Office of the Comptroller of the Currency*

OFAC *Office of Foreign Assets Control*

PCI DSS *Payment Card Industry Data Security Standard*

RFPA *Right to Financial Privacy Act*

SAR *Suspicious Activity Report*

SDN *Specially Designated National*

TIN *Taxpayer Identification Number*

INTRODUCTION

As the trade association representing members of the network branded prepaid access[1] industry, the Innovative Payments association (IPA) encourages practices that reduce opportunities for prepaid access to be used in illicit activities and to support national (and international) efforts combating money laundering, terrorist financing and financial crime. Such practices include effectively managed Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance programs.

To make ***all*** prepaid industry participants aware of their BSA/AML compliance responsibilities for prepaid access and to encourage all to implement appropriate practices, the IPA initially developed this document in 2008. Given changes in the regulatory regime, it was time to update the document. This document represents a compilation of the principles and practices of a cross-section of IPA members that have committed significant resources to applying BSA/AML requirements to prepaid access issued in the United States.

Foundation of these Recommended Practices

This document is based on the following statement of the basic requirements for a financial institution's BSA/AML compliance program:

Financial institutions, including banks and certain Money Services Businesses (MSBs), are required to have in place programs to ensure the institution's compliance with BSA/AML requirements[2]. When a financial institution contracts with a third-party agent to market, distribute, or support aspects of a prepaid access program, the financial institution should ensure that the third-party agent implements adequate BSA/AML compliance programs.

The compliance programs must be in writing and approved by the financial institution's board[3], with such approval to be noted in the board meeting minutes. The four pillars of an effective compliance program include:

1. A system of internal controls to ensure ongoing compliance including written policies and procedures;
2. Independent testing of compliance;

[1] Network branded prepaid cards carry the logo of a payment network such as American Express, Discover, Mastercard, or Visa, as well as one or more PIN debit networks. From a transaction authorization/processing perspective, they "ride the rails" of the existing credit card or ATM/debit card payment systems and, at a minimum, enable Cardholders to pay for purchases at a variety of merchants that accept the card brand. Depending on the type of prepaid card and the purpose for which it has been issued, there may be some restrictions on card use. For example, some cards are limited for use in the United States and others are limited to eligible purchases (e.g., health care cards).

[2] All businesses are also required to implement programs to ensure compliance with the sanctions programs administered by OFAC. This document does not address OFAC compliance programs.

[3] In this Guide, references to "Board" also means any similar governing body of a non-corporate entity.

3. On-going coordination and monitoring of compliance by a designated person; and

4. Training appropriate personnel.

Intent

These Recommended Practices are intended to be:

- **Flexible**. Industry participants in different areas of the prepaid value chain may apply these Recommended Practices differently depending on a variety of factors such as their role in the value chain, the products they offer, the funding source(s) of those products, their geographic location, and their charter.

- **Dynamic**. These Recommended Practices apply to the current environment. The prepaid access industry is complex, and its products and functionality are still emerging. These Recommended Practices are subject to change as situations warrant.

- **A baseline**. In certain situations, and for certain industry participants, it may be appropriate to view these Recommended Practices as a baseline for their BSA/AML compliance efforts.

How to Use these Recommended Practices

The IPA encourages every member of the network branded prepaid access industry—not only IPA members—to emulate the leading organizations that have contributed to this document and incorporate these practices into their own customized compliance programs and practices. We recommend that organizations required to have and maintain an effective BSA/AML compliance program use these Recommended Practices as either (a) a starting point to develop their programs or (b) a point of comparison to ensure the completeness of their programs.

To be clear, each organization that is obligated to have and maintain a BSA/AML compliance program must work with its legal counsel, compliance officers, line officers, and others to create a custom program and practices that address the unique risks associated with its specific role in the prepaid access value chain and the products and product features it offers. These Recommended Practices should be considered one of a number of resources an organization draws on to develop its BSA/AML compliance program and establish/update appropriate practices.

The IPA recognizes that all methods of payment and funds exchange are vulnerable to misuse. We believe, however, that well-run prepaid access programs are less vulnerable than other media of exchange such as cash

and checks.[4] We also believe that the convenience of prepaid access is and will continue to displace cash transactions by giving those without access to traditional banking relationships an opportunity to participate in mainstream financial activity that leaves an electronic footprint of every transaction.

Key Participants in the Prepaid Access Value Chain

In order to properly evaluate AML risks and implement proper internal controls, it is important to have a basic understanding of certain participants in the prepaid access value chain and their respective roles:

"Cardholder" - The owner/user of the prepaid access. This may be the prepaid access purchaser (e.g., general purpose spending card) or card recipient (e.g., gift card, payroll card, or disaster relief card).

"Distributor" - An organization that markets and distributes prepaid access. The distributor typically has a contract with an Issuer or a Program Manager. Examples include a shopping center or retailer selling gift cards or general-purpose prepaid cards, an employer offering payroll cards to employees, or an employee benefits company offering Health Savings Account (HSA) or Flexible Spending Accounts (FSA) cards to plan beneficiaries. Under the FinCEN Prepaid Access Rule, discussed below, a distributor may also be considered a "Seller" of prepaid access.

"Issuer" - An entity, which is typically a bank, credit union, or MSB, that issues a prepaid access to a cardholder and may serve as the holder of funds that have been prepaid and are awaiting disbursement. Also called the issuing bank. The Issuer must be licensed by the payment network to participate in their prepaid access programs. For prepaid access bearing the brand of American Express, the prepaid access is issued directly by American Express to the cardholder. For prepaid access bearing the brand of Discover, the prepaid access may be issued directly by Discover, or by a bank or MSB which is a licensee of Discover, to the cardholder.

"Payment Network" - Payment networks such as American Express, Discover, Mastercard, and Visa (and others) that act as gateways between acquirers and Issuers for authorizing and funding transactions made using prepaid access bearing their brand. The payment networks issue rules and regulations applicable to Issuers and acquiring (merchant) banks that participate in their prepaid access programs.

"Processor" - A processor facilitates payment transactions for prepaid access. A processor may provide one or more of the following services related to a prepaid access program: (a) prepaid access account set up and prepaid access activation; (b) card plastics production; (c) cardholder agreement design and production; (d) mailing of prepaid access, cardholder agreements and privacy policies to Cardholders; (e) provision of authorizations for prepaid access transactions; (f) value load and reload processing; (g)

[4] An October 2007 article by an economic advisor and a senior payments consultant at the Federal Reserve Bank of Cleveland explores the decline in consumers' use of cash in 13 developed nations. Commenting on Norway's decline in cash use, the authors note, ".in 2000 over 60 percent of Norway's outstanding cash was associated with the underground economy—everything from tax evasion to drug trafficking...Norwegian payment data is more detailed than most other countries, so similar estimates are more difficult to obtain for other countries, but it is likely that cash plays a similarly outsized role in other countries' underground economies."

See page 8 of 13 at http://www.clevelandfed.org/Research/Commentary/2007/100107.cfm.

cardholder customer service (telephone and Web); (h) chargeback processing; (i) cardholder error and dispute resolution; (j) security/fraud control and reporting; (k) periodic cardholder statements; and (l) provision of settlement services with the payment networks. Some issuers and program managers also serve the role of a processor. For a particular prepaid access program, a processor may have a contract with an issuer, a program manager, or both. For purposes of these Recommended Practices, "Core Processing Services" mean the following services: (i) prepaid access account set up and card activation; (ii) provision of authorizations for prepaid access transactions; (iii) value load and reload processing; and (iv) security/fraud control and reporting.

"Program Manager" - A program manager is an entity that contracts with an Issuer to establish, market, and operate prepaid access programs. By way of example, a payroll processor may act as a program manager to offer employers prepaid access as one option for making payroll payments to employees. Typically, program managers are responsible for establishing relationships with processors and distributors. In some cases, an Issuer or its affiliate also may serve the role of a program manager. In a prepaid program which is not bank-centered, the program manager may be considered as a "provider of prepaid access" under the FinCEN Prepaid Access Rule (discussed further below).

"Third-party agent" - In these Recommended Practices, a third-party agent may be a program manager or distributor. Depending on the prepaid access type and program structure, other non-bank entities also may be third-party agents.

Document Overview

In addition to the Introduction and Conclusion, this document is organized into eight key sections, each of which addresses a specific aspect of BSA/AML compliance for prepaid access:

- **Section 1: Covered Entities.**

- **Section 2: Risk Assessment**. A multi-faceted risk assessment is the cornerstone of any organization's BSA/AML compliance program for prepaid access. This section discusses identifying the money laundering and terrorist financing risks associated with customers and transactions and implementing appropriate measures and controls to mitigate these risks. The risk assessment process enables the financial institution to better identify and mitigate any gaps in BSA/AML controls.

  This section highlights one of the most difficult aspects of dealing with money laundering and terrorist financing issues. The risk assessment process is complex and inherently subjective. The benefit of a subjective standard is that it provides organizations with the flexibility to adapt risk-based guiding principles to their specific situations. Subjective flexibility also encourages competition and product differentiation. The downside is that there are few hard and fast "rules" providing strict guidance, so there is little certainty in the decision-making process.

- **Section 3**: **Internal Controls**. Internal controls (policies, procedures, and processes) are a key tool to limit and control risks associated with prepaid access and comply with applicable BSA/AML laws and regulations.

  This section addresses internal controls that organizations should establish consistent with their role in the prepaid value chain.

- **Section 4: Federal Reporting Requirements**. Financial institutions subject to the BSA may be responsible for filing Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs) related to prepaid activity.

  This section provides information about the responsibilities of organizations to comply with federal law by filing SARs and CTRs.

- **Section 5: Customer Identification Program (CIP)/Customer Due Diligence (CDD**). As required by Section 326 of the USA PATRIOT Act, the Department of the Treasury adopted regulations that require Financial institutions to implement reasonable procedures to verify and maintain records relating to the identity of persons seeking to open an account and determining whether the persons are listed among known or suspected terrorists or terrorist organizations.

  This section addresses a variety of issues relating to requirements for establishing the identity of consumers and businesses buying prepaid access. It includes when CIP requirements apply and when they may not apply to prepaid access, how to mitigate risk related to “anonymous” prepaid access, risk-based CIP, and applying CIP to B-to-B prepaid access.

  This section also addresses general CDD obligations which may be imposed on a prepaid program; as well as details the introduction of the CDD Rule which became effective in May 2018. This rule amends The Bank Secrecy Act regulations, aims to improve financial transparency and prevent criminals and terrorists from misusing companies to disguise their illicit activities and launder their ill-gotten gains. The CDD Rule clarifies and strengthens customer due diligence requirements for U.S. banks and other financial entities.

- **Section 6: Third-party agents**. A financial institution that contracts with third-party agents accepts the risks related to the services provided by their agents. Prior to program launch, a financial institution should complete an appropriate due diligence review of the third-party agents engaged by the financial institution.

  This section details the requirements of risk-based due diligence evaluations that Issuers should conduct before engaging Third-party agents in their prepaid access programs.

- **Section 7: Independent Compliance Testing.** Independent, objective compliance testing is an essential step in evaluating whether appropriate internal controls are in place and being followed.

This section addresses the timing of independent testing and who may conduct independent testing as well as recommendations for the areas that should be checked as part of an independent review and, finally, how an independent review should be documented.

- **Section 8: Training Appropriate Personnel.** Financial institutions must ensure that appropriate personnel, including members of the financial institution's Board, are trained in all applicable aspects of BSA/AML requirements.

  This section provides a bullet-point list emphasizing the employees who should be included in a BSA/AML training program and topic areas that should be covered.

SECTION 1: COVERED ENTITIES

This section introduces the two primary categories of Financial institutions subject to BSA/AML compliance obligations: banks and MSBs. This section also sets forth relevant regulatory and statutory definitions, and it outlines the Prepaid Access Rule, which brought many prepaid firms within FinCEN's regulatory ambit. Finally, this section summarizes the BSA/AML requirements for banks and MSBs.

The BSA authorizes the Secretary of the Treasury to issue regulations requiring Financial institutions to keep records and file reports that "have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence matters, including analysis to protect against international terrorism." The Secretary delegated this authority to the Director of FinCEN by Treasury Order in 2002. FinCEN has since issued BSA-implementing regulations that appear at 31 C.F.R. Chapter X. With regard to the prepaid industry, these regulations essentially divide Financial institutions into two categories: banks (bank-centered programs) and MSBs (non-bank-centered programs). In addition, in June of 2013, FATF issued guidance on implementing a risk-based approach to anti-money laundering and countering the financing of terrorism for prepaid cards, mobile payments, and internet-based payment services ("FATF Guidance").[5]

Bank-Centered Programs

Banks and Their Agents

FinCEN defines Financial institutions to include banks, and FinCEN imposes certain reporting and record-keeping requirements upon banks. The regulations at 31 C.F.R. 1010.100(d) define a bank as "[e]ach agent, agency, branch or office within the United States of any person doing business in one or more of the capacities listed below:

1. A commercial bank or trust company organized under the laws of any State or of the United States;
2. A private bank;
3. A savings and loan association or a building and loan association organized under the laws of any State or of the United States;
4. An insured institution as defined in section 401 of the National Housing Act;
5. A savings bank, industrial bank or other thrift institution;
6. A credit union organized under the law of any State or of the United States;

[5] FATF, Guidance for a Risk Based Approach: Prepaid Cards, Mobile Payments, and Internet Based Payment Services, available at http://www.fatf- gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf (June 2013).

7. Any other organization (except an MSB) chartered under the banking laws of any state and subject to the supervision of the bank supervisory authorities of a State;

8. A bank organized under foreign law;

9. Any national banking association or corporation acting under the provisions of section 25(a) of the Act of December 23, 1913, as added by the Act of Dec. 24, 1919, ch.18, 41 Stat. 378, as amended (12 U.S.C. 611-32)."

General Requirements for Bank-Centered Programs

- **Maintain an AML Program**. The regulations generally require that banks maintain AML policies, procedures, and controls that are reasonably designed to detect and report any known or suspected money laundering or suspicious activity involving any account that is established, maintained, administered, or managed in the United States.

- **Currency Transaction Reporting**. The regulations require covered Financial institutions to report to FinCEN transactions in currency in amounts greater than $10,000.

- **Suspicious Activity Reporting**. Under the regulations, banks must report any transaction of $5,000 or more which it determines to be suspicious and the suspect is known. Banks must report any transaction of $25,000 or more which it determines to be suspicious when the suspect is unknown. Banks must report any transaction of any amount involving insider abuse.

- **Customer Identification Information Collection and Retention**. The regulations require a bank to implement a written CIP appropriate for its size and type of business. The CIP must include risk-based procedures for collecting customer information, verifying customer identities, collection beneficial owner information, record-keeping procedures for certain information, procedures for determining whether customers appear on any government list of known or suspected terrorists, and procedures for providing customers with adequate notice that the bank is requesting information to verify their identities.

- **Transaction Records**. With respect to certain funds transfers in the amount of $3,000 or more, a bank must maintain certain records for at least five years.

- **Information Sharing.** A federal, state, local, or foreign law enforcement agency investigating terrorist activity or money laundering may request that FinCEN solicit, on its behalf, certain information from a financial institution or a group of financial institutions (an "information request"). Upon receiving an information request (referred to as a "314(a) request"), a Financial institution must conduct a one-time search of its records to identify accounts or transactions of a named suspect. Unless otherwise instructed by an information request, Financial

Institutions must search their records for current accounts, accounts maintained during the preceding 12 months, and transactions conducted outside of an account by or on behalf of a named suspect during the preceding six months.

The Financial institution must search its records and report any positive matches to FinCEN within 14 days, unless otherwise specified in the information request.

Section 314(b) encourages Financial institutions located in the United States to share information in order to identify and report activities that may involve terrorist activity or money laundering. Section 314(b) also provides specific protection from civil liability. To avail itself of this statutory safe harbor from liability, a financial institution must notify FinCEN of its intent to engage in information sharing and that it has established and will maintain adequate procedures to protect the security and confidentiality of the information.

Non-Bank-Centered Programs

MSBs and the Prepaid Access Rule

Under a final rule issued by FinCEN in July 2011 (the "Prepaid Access Rule[6]"), certain entities that provide or sell "prepaid access" are considered to be MSBs and therefore financial institutions that fall within FinCEN's regulatory ambit for BSA regulatory purposes. Specifically, the Prepaid Access Rule creates new categories of MSBs to include "providers" and "sellers" of prepaid access. The Prepaid Access Rule generally applies to "prepaid access" provided under a "prepaid program," as those terms are defined in the rule. The rule also establishes exclusions from the definition of a prepaid program for certain types of arrangements that FinCEN believes present low or minimal risks.

The BSA regulations preclude a bank from being deemed any category of MSB. Accordingly, a bank cannot be a provider of prepaid access subject to the requirements of the Prepaid Access Rule, although banks remain subject to similar reporting and record-keeping requirements under the BSA. In Frequently Asked Questions ("FAQs") issued by FinCEN under the Prepaid Access Rule,[7] FinCEN has stated that "in situations in which a bank exercises 'principal oversight and control,' no participant is required to register as the provider of prepaid access. However, if a participant other than a bank chooses to register, that participant is the provider of prepaid access and has the responsibilities under the rule notwithstanding the bank's participation in the prepaid program. The [Prepaid Access] Rule does not relieve banks of their existing BSA obligations, including with respect to prepaid programs with which they are involved."

Definitions

The Prepaid Access Rule sets forth a chain of definitions that delineate whether a prepaid organization will be considered an MSB subject to FinCEN regulation.

[6] The Prepaid Access Rule is included as part of the FinCEN rules for Money Service Businesses at 31 C.F.R. Part 1022

[7] A copy of the FAQs may be found at: http://www.fincen.gov/news_room/nr/html/20111102.html

Prepaid Access

Because the term "stored value" has been perceived as an inaccurate term for the payment mechanisms it represented, the Prepaid Access Rule replaces the term "stored value" with "prepaid access." The Prepaid Access Rule defines "prepaid access" as

> *"Access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number, or personal identification number."*

The definition is extremely broad. In the FAQs, FinCEN noted that devices sold for future access to products or services (e.g., songs, iTunes, telephone minutes, megabytes, wireless top-up, games, software, etc.) are likely to be considered prepaid access.[8]

Closed-loop Prepaid Access

The definition of "closed-loop prepaid access" is important in the context of the Prepaid Access Rule's definitions of "prepaid program" and "sellers of prepaid access." For purposes of the Prepaid Access Rule, closed-loop prepaid access is defined as "Prepaid access to funds or the value of funds that can be used only for goods or services in transactions involving a defined merchant location (or set of locations), such as a specific retailer or retail chain, a college campus, or a subway system."

In the discussion contained in the Prepaid Access Rule, FinCEN noted that the definition "limits closed-loop prepaid access to use for goods and services, excluding transfers of value to third parties and cash withdrawals," other than de minimis redemptions of cash value required by law, such as state gift certificate laws which contain a cash-out requirement.

Prepaid Program

The Prepaid Access Rule generally applies to "prepaid programs." The definitions of "provider of prepaid access" and "seller of prepaid access" and many of the requirements of the Prepaid Access Rule are linked to the definition of "prepaid program." The Prepaid Access Rule defines the term prepaid program as "an arrangement under which one or more persons acting together provide(s) prepaid access."

The rule contains several exceptions to this definition, which are crucial to interpreting the specific requirements of the Prepaid Access Rule. Specifically, an arrangement is not considered a prepaid program if:

[8] FinCEN has determined, however, that a person's acceptance or transmission of convertible virtual currency is not subject to the Prepaid Access Rule because prepaid access is limited to real currencies. See Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies, FIN-2013-G001 (March 18, 2013).

1. It provides closed-loop prepaid access in amounts of $2,000 or less that can be associated with a prepaid access device or vehicle on any day;

2. It provides prepaid access solely to funds provided by a federal, state, local, territory and insular possession, or tribal government agency (e.g., for government payroll, tax refunds and government benefits such as unemployment, disability, social security and child support);

3. It provides prepaid access solely to funds from pre-tax flexible spending arrangements for health care and dependent care expenses (e.g., the type typically offered by employers to employees), or from Health Reimbursement Arrangements (as defined in 26 U.S.C. 105(b) and 125) for health care expenses[9]; or

4. It provides prepaid access solely to:
   - Employment benefits, incentives, wages or salaries; or
   - Funds not to exceed $1,000 maximum value and from which no more than $1,000 maximum value can be initially or subsequently loaded, used, or withdrawn on any day through a device or vehicle;

provided that such prepaid access does not permit:

- Funds or value to be transmitted internationally;
- Transfers between or among users of prepaid access within a prepaid program; or
- Loading additional funds or the value of funds from non-depository sources.

The FAQs issued by FinCEN provide several clarifications of these exceptions. As to the closed-loop prepaid access exception, the FAQs provide that the $2,000 threshold for closed-loop prepaid access is per device and it does not require aggregation of all purchases of separate closed-loop prepaid access devices bought by an individual in a single day. However, if the closed-loop prepaid access arrangement permits either individual reloads of more than $2,000 per device, or cumulative reloads per device that total more than $2,000 in one day, the arrangement no longer qualifies for the "closed-loop prepaid access" exception.

For reloadable temporary prepaid access devices, the FAQs provide that such arrangements are excluded from the definition of prepaid program regardless of whether the temporary device is reloadable or not, so long as the features of that device are limited as required to qualify for an exception. For example, if a device's maximum value, use, or withdrawal limit is less than $1,000 on any day, and it cannot be used internationally, reloaded at a non-depository source, or used to transfer value among the users, it is not subject to the rule.

As to the question of what "loading additional funds or the value of funds from non- depository sources" means, the FAQs clarify that the term means "providing funds or the value of funds intended for prepaid access by means of an entity that is not a depository institution, where that entity will then arrange for the funds to be available through the prepaid access. . . " Examples of reloads made through a depository institution include but

[9] Health Savings Accounts are not covered by this exemption because of the ability to mingle health and non-health related funds

are not limited to: ACH transfers from a bank account, cash or other deposit at a bank, or a check drawn on a bank and payable to the provider of prepaid access. By contrast, reloads that are not made through a depository institution include but are not limited to: reloads through retail store transactions (e.g., cash, check or credit card), wire transfers originating at money services businesses, or checks payable to a payee other than the provider of prepaid access.

Provider of Prepaid Access

Where the prepaid arrangement qualifies as a prepaid program, a program participant may be required to register with FinCEN as a "provider of prepaid access". In general, a "provider of prepaid access" is the single participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow program participants. The Prepaid Access Rule permits the participants of a prepaid program to designate who primarily controls and manages the program. However, if no provider is designated by agreement and registered as such with FinCEN, the de facto provider is the person with principal oversight and control over the prepaid program. Which person exercises "principal oversight and control" is a matter of facts and circumstances, but the activities that indicate the same include:

Organizing the prepaid program;

- Setting the terms and conditions of the prepaid program and determining that the terms have not been exceeded;
- Determining the other businesses that will participate in the prepaid program, which may include the issuing bank, the payment processor, or the distributor;
- Controlling or directing the appropriate party to initiate, freeze, or terminate prepaid access; and
- Engaging in activity that demonstrates oversight and control of the prepaid program.

As noted above, in situations in which a bank exercises "principal oversight and control," no participant would be required to register as a "provider of prepaid access".

The FAQs state "[t]he provider of prepaid access for a prepaid program is the participant in that prepaid program who registers with FinCEN as the provider of prepaid access for that program. Determination of which participant should register is a matter left to the participants. However, it is presumed that the participant registering as the provider of prepaid access has agreed to perform all of the duties required for providers of prepaid access under the [Prepaid Access Rule]."

Seller of Prepaid Access

The Prepaid Access Rule defines a "seller of prepaid access" as any person that receives funds or the value of funds in exchange for an initial loading of prepaid access if that person:

- Sells prepaid access offered under a prepaid program that can be used before the required verification of customer identification has occurred; or
- 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.

Unlike providers, sellers of prepaid access are not subject to a FinCEN registration requirement.

Under the FAQs, FinCEN states "[a] person that accepts payments for an initial or subsequent loading of prepaid access, including a general purpose retailer such as a pharmacy, convenience store, supermarket, or discount store, is not considered a "seller of prepaid access" if: (a) it does not sell prepaid access under a prepaid program that can be used before the user's identification needs to be verified; and (b) it has policies and procedures in place that are reasonably adapted to prevent the sale of more than $10,000 of any type of prepaid access to any one person on any one day.

Such a person is considered a "seller of prepaid access" if it either sells prepaid access described in item (a) above or doesn't have policies and procedures, and does engage in sales, described in item (b) above."

As to the latter question of when policies and procedures are considered to be "reasonably adapted" to prevent a sale of more than $10,000 to any person during any one day, the FAQs do not provide explicit guidance, but instead provide that "[t]here is no one set of policies and procedures that is 'reasonably adapted' to prevent sales of prepaid access that exceed $10,000 to any person during any one day. Such policies and procedures must be risk-based and appropriate to the particular retailer in question, taking into account facts such as its typical customers, its location(s), and the volume of its prepaid access sales. The fact that a retailer sells over $10,000 in prepaid access to one person in one day does not in and of itself mean that the retailer's policies and procedures are not 'reasonably adapted to prevent such a sale.'"

The FAQs clarified that the distribution of prepaid access products to other businesses for further distribution or sale to end users/consumers by those other businesses is not the type of activity intended to be covered by the Prepaid Access Rule, regardless of whether the activity exceeded $10,000 to one business (i.e., person) in one day. The FAQs provide that the definition of "seller" is intended to address sales to the end user/consumer of the prepaid access product, not to apply to businesses in the distribution channels that move the prepaid access products to the market.

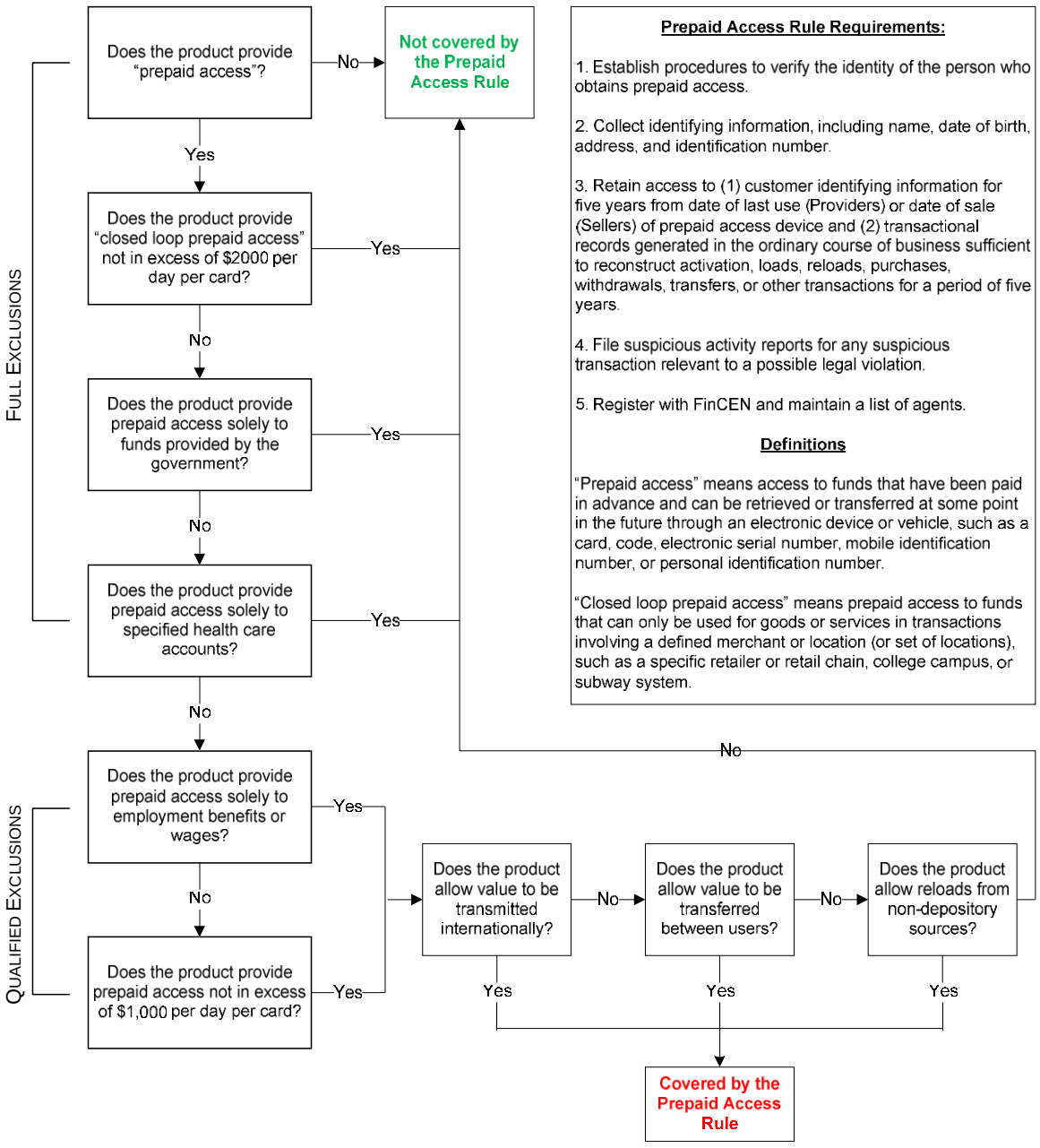
The FAQs also clarified the question of whether businesses are deemed "sellers" if they provide non-depository reloads to prepaid access. The FAQs state "[a]n entity reloading prepaid access from a non-depository source is a "seller," subject to the provisions of the Rule, if it (1) reloads funds onto prepaid access that is part of a prepaid program not subject to initial customer verification, or (2) both reloads in excess of $10,000 for any person on any given day, and does not have policies and procedures reasonably adapted to prevent such reloading for any person on any given day." The FAQ further provides that:

"Persons providing non-depository reloads of funds or the value of funds to prepaid access are not sellers if:

- They reload less than $10,000 of prepaid access that is not part of a prepaid access program covered under the [Prepaid Access Rule] for any person on any given day;
- They reload less than $10,000 of prepaid access that is part of a prepaid program covered under the [Prepaid Access Rule], but is subject to verification procedures after the initial sale of the prepaid access, for any person on any given day; and
- They have policies and procedures reasonably adapted to prevent the reloading of $10,000 for any person on any given day."

Finally, the FAQs provide "[a] person that qualifies as a 'seller of prepaid access' because of the person's reload business has the same obligations as any other 'seller of prepaid access,' including AML program, SAR filing, and recordkeeping requirements. However, such a seller does not have to obtain customer identification information under 31 C.F.R. 1022.210 from customers that have already provided customer identification information with respect to the prepaid access that they are reloading."

Prepaid Access Rule Coverage Flow Chart



General Requirements of the Prepaid Access Rule

Ultimately, if a prepaid program is not subject to one of the exemptions discussed above, the entity designated as the provider of prepaid access, as well as each seller of prepaid access, is considered an MSB and must comply with the requirements of the Prepaid Access Rule. The general requirements of the Prepaid Access Rule applicable to providers and/or sellers of prepaid access are as follows.

Requirements for Providers and Sellers of Prepaid Access

- **Maintain an AML Program.** Under the Prepaid Access Rule, all providers and sellers of prepaid access must develop, implement and maintain an AML program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. The AML program should include, among other items, requirements for verifying customer identification, filing reports, creating and retaining records and responding to law enforcement requests.

- **Currency Transaction Reporting**. The Prepaid Access Rule requires providers and sellers of prepaid access to report to FinCEN transactions in currency in amounts greater than $10,000.

- **Suspicious Activity Reporting.** The Prepaid Access Rule eliminates the previous exemption from suspicious activity reporting for stored value. Under the Prepaid Access Rule, any provider or seller of prepaid access must report any transaction of $2,000 or more which it determines to be suspicious.

- **Customer Identification Information Collection and Retention**. Under the Prepaid Access Rule, providers and sellers of prepaid access must implement procedures to verify the identity of any person who obtains prepaid access under a prepaid program and obtain identifying information concerning such a person, including name, date of birth, address, and identification number. Furthermore, sellers of prepaid access must also establish procedures to verify the identity of any person who obtains prepaid access to funds that exceed $10,000 during any one day and obtain the same identifying information concerning such person. Providers must retain access to this information for five years after the last use of the prepaid access device or vehicle, whereas sellers must retain such information for five years from the date of sale.

Additional Requirements for Providers of Prepaid Access

- **Comply with the Requirements Applicable to Sellers.** Providers must comply with all requirements applicable to sellers of prepaid access listed above, including the maintenance of an AML program, currency transaction and suspicious activity reporting, and customer identification information collection and retention.

- **Transaction Records Generated in the Ordinary Course of Business.** With respect to transactions relating to providers and sellers of prepaid access, the Prepaid Access Rule requires prepaid access providers (but not sellers) to retain transaction-specific records generated in the ordinary course of business for a period of five years. The types of records required to be maintained are those that would be needed to reconstruct prepaid access activation, loads, reloads, purchases, withdrawals, transfers or other prepaid-related transactions (e.g., information regarding the type of transaction, amount and location of transaction, date and time of transaction, and any other unique identifiers related to the transaction). These records need not be kept in any particular format, or by any particular participant in the prepaid program. The provider of prepaid access, however, bears the responsibility for complying with these recordkeeping requirements.

- **Registration with FinCEN.** The Prepaid Access Rule requires providers of prepaid access to register with FinCEN as an MSB using FinCEN Form 107 and comply with the associated agent list requirements. A provider must also identify each prepaid program for which it is the provider of prepaid access. Sellers of prepaid access are not required to register with FinCEN.

Financial Action Task Force Guidance

The Financial Action Task Force recognizes that the number and range of entities involved in providing prepaid access can make the identification of the entity ultimately responsible for the implementation of AML preventive measures difficult to determine. In light of this recognition, the FATF Guidance examines which entities involved in the provision of prepaid access fall within the definition of "Financial institution" and are thus covered by the FATF Recommendations.

FATF defines a "financial institution" broadly to include any natural or legal person conducting a business involved in one or more specific activities or operations on behalf of a customer. Those activities or operations include:

> Acceptance of deposits and other repayable funds from the public; lending; financial leasing; money or value transfer services; issuing and managing means of payment; financial guarantees and commitments; trading in money market instruments, foreign exchange, exchange/interest rate/index instruments, transferable securities, commodity futures trading; participation in securities issues and providing financial services related thereto; portfolio management; safekeeping/administration of cash or liquid securities; investing/managing funds or money on behalf of others; underwriting and placement of investment related insurance; and money/currency changing.

Any entity or individual conducting one or more of these operations is thus a "financial institution" for FATF purposes and subject to the AML preventative measures required by the FATF Recommendations (i.e., customer due diligence, record keeping, reporting of suspicious transactions). FATF recognizes, however, that there are difficulties in determining which entity remains responsible for such preventative measures on the national level.

SECTION 2: RISK ASSESSMENT

This section highlights one of the most difficult aspects of dealing with money laundering and terrorist financing issues, i.e., risk assessments that are complex and inherently subjective. The benefit of a subjective standard is that it provides organizations with the flexibility to adapt guiding principles to their specific situations, which also may encourage product differentiation. The downside is that there are few hard and fast "rules" providing strict guidance.

Both banks and MSBs are required to maintain an AML program that is reasonably designed to prevent the Financial institution from being used to facilitate money laundering and the financing of terrorist activities. A risk assessment is the cornerstone of a Financial institution's BSA/AML compliance program. Although attempts to launder money, finance terrorism, or conduct other illegal activities can stem from many different sources, certain products, services, customers, and geographic locations may be more vulnerable and have been historically abused by money launderers and criminals.

Financial institutions should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are appropriate to the risks identified. Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. A financial institution is expected to have a BSA/AML compliance program equal to its respective risk profile.

Each relationship that a U.S. bank has with another financial institution or third party as part of a prepaid access program should be governed by a contract or agreement outlining each party's responsibilities and should also consider each party's BSA/AML compliance requirements, due diligence procedures and any payment network obligations. It should be noted that the issuing bank maintains ultimate responsibility for BSA/AML compliance whether or not a contractual agreement exists.

The development of a BSA/AML risk assessment generally involves two steps: (1) identify the specific risk categories unique to the financial institution, and (2) conduct data analysis to quantify risk within each category.

Step One: Identify Specific Risk Categories

The first step of the risk assessment process is to identify the specific products, services, customers, entities, and geographic locations that may pose a risk to the financial institution.

Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. Although attempts to launder money, finance terrorism, or conduct other illegal activities through a financial institution can emanate from many different sources, certain products, services, customers, entities, and geographic locations may be more vulnerable or historically abused by money launderers and criminals.

Various factors, such as the number and volume of transactions, geographic locations, and nature of the customer relationships, should be considered when the Financial institution prepares its risk assessment. The differences in the way a Financial institution interacts with the customer (face-to-face contact versus electronic interaction) also should be considered. Because of these factors, risks will vary from one Financial institution to another.

Geographic Location Risk

- High-risk geographic locations may be either international or domestic. International high-risk geographic locations generally include:
- Countries subject to OFAC sanctions, including state sponsors of terrorism;
- Countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State;
- Jurisdictions determined to be "of primary money laundering concern" by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury, through FinCEN, pursuant to section 311 of the USA PATRIOT Act;
- Jurisdictions or countries monitored for deficiencies in their regimes to combat money laundering and terrorist financing by international entities such as the FATF;
- Major money laundering countries and jurisdictions identified in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR), in particular, countries which are identified as jurisdictions of primary concern;
- Offshore financial centers; and
- Other countries identified by the financial institution as high-risk because of its prior experiences or other factors (e.g., legal considerations or allegations of official corruption). Countries identified by credible sources as not having adequate AML or Counter-Terrorist Financing (CTF) systems or controls.

The extent to which a prepaid access can be used globally for making payments or transferring funds is an important factor to consider when determining the level of risk.

Domestic high-risk geographic areas may include banking offices doing business within, or having customers located within, locations designated as high-risk by the U.S. government, such as High Intensity Drug Trafficking Areas (HIDTAs) and High Intensity Money Laundering Financial Crimes Areas (HIFCAs).

Customer and Entity Risk

Each Financial institution must assess, based on its own criteria, whether a particular customer poses a higher risk of money laundering or terrorist financing. There is no universal consensus as to which customers pose a higher risk, but, as it relates to "typical" prepaid access customers, the following characteristics of customers have been associated with potentially higher risks:

- Foreign Financial institutions, including banks and foreign money services providers (e.g., casas de cambio, currency exchanges, and money transmitters);
- Nonbank Financial institutions (e.g., money services businesses; casinos and card clubs; brokers/dealers in securities; and dealers in precious metals, stones, or jewels);
- Senior foreign political figures and their immediate family members and close associates (collectively known as a "Politically Exposed Person" or PEP);
- Nonresident alien (NRA) and accounts of foreign individuals;
- Foreign corporations and domestic business entities, particularly offshore corporations (such as domestic shell companies, private investment companies, and international business corporations) located in high-risk geographic locations;
- Cash-intensive businesses (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs, vending machine operators, and parking garages);
- Non-governmental organizations and charities (foreign and domestic);
- Deposit brokers, particularly foreign deposit brokers;
- Professional service providers (e.g., attorneys, accountants, doctors, and real estate brokers);
- The cardholder is anonymous or unknown

Financial institutions should design and implement appropriate measures and controls to mitigate the potential money laundering risks of customers identified as higher risk as the result of their risk assessment processes. These measures and controls may include one or more of the following:

- Increased levels of CDD;
- Escalation for approval of the establishment of an account or relationship;
- Increased monitoring of transactions; and
- Increased levels of ongoing controls and reviews of relationships.

Product/Services Risk

Determining the potential money laundering and terrorist financing risks presented by products and services offered by a Financial institution also assists in overall risk assessment. Prepaid access programs are diverse and

range in product and services offered, and the customer base they serve. In evaluating the risk, financial institutions should take into account the program's specific features and functionalities, and consider the following issues and features in assessing the money laundering and terrorist financing risks related to its prepaid access products:

- How is the prepaid access distributed?
- Who is the customer (e.g., governmental agency, business, or consumer)?
- Is there an existing relationship with the customer?
- What are the sources of the funds?
- What are the methods of funding allowed? Anonymous funding methods (third party funding through cash reload networks or person-to-person) poses the highest potential risk. Allowing funding via another payment services that does not verify consumer identification can also create an anonymous funding mechanism.
- What is the expected level of prepaid activity? What is the type, velocity/frequency of funds that can be loaded and transacted?
- Is the prepaid access reloadable?
- Are value load sources restricted?
- Can the prepaid access be used to obtain cash (at ATMs, at point of sale, or through a cash advance transaction)? International cash access poses additional risk.
- Can funds be transferred from one prepaid access to another prepaid access or other financial account?
- Are bulk purchases of prepaid access permitted?
- Are multiple distribution channels allowed (i.e. Internet)?
- Can the prepaid access be used internationally?
- Is the amount of funds permitted on the prepaid access (at any one time and in the aggregate) limited?

FATF Guidance

The FATF Guidance identifies the following "unique" risks to prepaid access:

- **Non-face-to-face relationships and anonymity** - Non-face-to-face contact may indicate a higher risk, due to factors, such as impersonation fraud, of money laundering/terrorist financing. The FATF Guidance notes that the risk posed by anonymity may occur at purchase, registration, loading, reloading, or customer use. The FATF Guidance states the level of risk is relative to the functionality of the prepaid access.

- **Funding** - The FATF Guidance notes that funding of prepaid may occur in various ways with differing degrees of customer due diligence. The FATF Guidance is especially concerned with cash funding, which may be fully anonymous, and the ability to pass prepaid cards on to third parties. The FATF Guidance first notes that prepaid access reduces the incentives for providers to conduct comprehensive customer due diligence because credit risk is absent. A further risk associated with prepaid access funding includes reload ability with no limits.

- **Geographical Reach** - The FATF Guidance pays particular attention to open-loop prepaid access in examining this risk because those products often enable customers to make payments at both domestic and foreign points of sale. Additionally, the FATF Guidance notes that some prepaid access programs allow customers to make person-to-person transfers and that the compact physical size of the cards themselves increase their vulnerability because criminals may use them – in lieu of cash – to make cross-border transportations of value. The FATF Guidance highlights prepaid access ability to access funds internationally as being particularly vulnerable. Such vulnerability stems from the logistical benefits of transporting prepaid access with accounts loaded with high value not determinable from the prepaid access itself.

- **Access to Cash** - The FATF Guidance expresses concerns over the risk of access to cash through international automated teller machine ("ATM") networks. Such access increases the level of money laundering and terrorist financing risk and may be either direct, through prepaid access, or indirect, through mobile and internet payments interconnected with prepaid access.

- **Segmentation of Services** - A final risk identified by the FATF Guidance is the number of parties involved in providing prepaid access. Such risks include that the large number of parties increases the danger of losing customer or transaction information and that prepaid access providers will rely on agents and unaffiliated Third-party agents to establish customer relationships and reload funds. Further, the FATF Guidance notes that entities providing prepaid access may come from sectors unfamiliar with AML and CTF controls. Specific area of concern noted is segmented internet-based payment services as their cross-border nature means that providers may be located in jurisdictions with inadequate AMF/CTF regulation and supervision.

Step Two: Data Analysis

The second step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage in order to more accurately assess BSA/AML risk. This step involves evaluating data pertaining to the Financial institution's activities in relation to Customer Identification Program (CIP) and customer due diligence (CDD) information. The level and sophistication of analysis may vary by Financial institution. The detailed analysis is important because within any type of product or category of customer there will be accountholders that pose varying levels of risk. The following factors should be examined with particular scrutiny:

- Purpose of the account;
- Actual or anticipated activity in the account;
- Nature of the customer's business or occupation;
- Customer's location; and
- Types of products and services used by the customer.
- Source of the funds (from known and trusted source such as corporate or government loads, vs. loads by individuals)

A Financial institution's BSA/AML compliance program should adequately address its risk profile, as identified by the risk assessment. Management of the Financial institution should understand the institution's BSA/AML risk exposure and develop the appropriate policies, procedures, and processes to monitor and control BSA/AML risks. For example, the financial institution's monitoring systems to identify, research, and report suspicious activity should be risk-based, with particular emphasis on higher-risk products, services, customers, entities, and geographic locations as identified by the financial institution's BSA/AML risk assessment

Independent testing should review the risk assessment for reasonableness and applicability, and should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties It is recommended that independent testing of the risk assessment be conducted at least every 12 to 18 months, depending on the program's AML/BSA risk profile. Actual data should be used to support conclusions and evaluate the BSA/AML risks associated with the prepaid access program. Additionally, management should consider the staffing resources and the level of training necessary to promote adherence with these policies, procedures, and processes. Finally, an effective risk assessment should be an ongoing process—not a one-time exercise. A Financial institution should also update its risk assessment to identify changes in the risk profile as necessary, but not less than every twelve to eighteen months.

SECTION 3: INTERNAL CONTROLS

This section addresses internal controls that organizations should establish consistent with their role in the prepaid value chain.

Internal controls are the financial institution's policies, procedures, and processes established to limit and control risks and to achieve compliance with the BSA and applicable AML laws and regulations. The sophistication of internal controls should be commensurate with the size, structure, risks, and complexity of the financial institution. For a financial institution that uses third-party agents, such as program managers and processors, the financial institution must assure that the third-party agent's internal controls are adequate or impose controls when warranted.

Internal Controls—General

Any organization participating in the prepaid access value chain should maintain an overall environment that is conducive to managing risks and complying with BSA/AML requirements, as appropriate. These Recommended Practices assume that the organization has established an environment with internal controls of a general nature that:

- Identify operations (i.e., products, services, customers, entities, and geographic locations) more vulnerable to abuse by money launderers and criminals; provide for periodic updates to the financial institution's risk profile; and provide for a BSA/AML compliance program tailored to manage risks;
- Inform the board, or a committee thereof, and senior management, of compliance initiatives, identified compliance deficiencies, and corrective action taken, and notify directors and senior management of SARs filed;
- Identify a person or persons responsible for BSA/AML compliance;
- Provide for program continuity despite changes in management or employee composition or structure;
- Meet all regulatory recordkeeping and reporting requirements, meet recommendations for BSA/AML compliance, and provide for timely updates in response to changes in regulations;
- Implement risk-based CDD policies, procedures, and processes regarding cardholders, agents, vendors, sellers, and distributors;
- Ensure that all applications and systems maintaining cardholder data are compliant with PCI DSS;
- Identify reportable transactions and accurately file all required reports including SARs, CTRs, and CTR exemptions in a timely manner;[10]

[10] Reporting requirements under OFAC are not covered by this document.

- Provide for dual controls and the segregation of duties to the extent possible. For example, employees that complete the reporting forms (such as SARs, CTRs, and CTR exemptions) generally should not also be responsible for the decision to file the reports or grant the exemptions;

- Provide sufficient controls and systems for filing CTRs and CTR exemptions.

- Provide for sufficient controls and monitoring systems for timely detection and reporting of suspicious activity;

- Ensure that adequate controls are in place before new prepaid access products are offered.

- Provide for adequate supervision of employees who handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by the BSA and its implementing regulations; and

- Incorporate BSA/AML compliance into the job descriptions and performance evaluations of appropriate personnel; and

- Train employees to be aware of their responsibilities under the BSA regulations and internal policy guidelines.

Internal Controls—Prepaid Access[11]

In addition to the above, participants in the prepaid access value chain should establish controls specific to their prepaid access activities. Depending on the functions that an organization provides, specific prepaid-related internal controls may include systems to:

- Identify when a Cardholder has been issued an excessive number of prepaid access devices, based on program parameters;[12]

- For transaction aggregation and reporting, detect multiple prepaid access accounts in the same name or that use the same mailing address (postal, e-mail, or IP address), telephone number, Social Security number, and/or common funding source (same bank account, credit card, or debit card);

- Restrict value loads, card-to-card transfers and cash access based on amounts that are reasonable and appropriate for Cardholders and/or prepaid access product types, considering the purpose for which the prepaid access was issued. Issuers should consider establishing load limits for the number of loads allowed during a given time period and the maximum dollar amount allowed per load. In addition, Issuers should also consider establishing and monitoring daily/weekly cash access and purchase limits for Cardholders.

[11] Not all of the stated monitoring systems may be necessary or appropriate for all types of prepaid card products. Monitoring systems should be tailored to the particular card product and features offered.

[12] For anonymous card products sold in a retail environment, the appropriate control is a limit on the number of cards that can be purchased and the dollar value than may be loaded onto the cards at the point of sale.

- When loads are accomplished through credit or debit cards, use fraud monitoring tools—such as address verification services, card verification values, online verification systems (Visa Secure, Mastercard SecureCode), and fraud scoring systems—to detect potentially fraudulent transactions.

- Where card-to-card transfers can be made, monitoring and limits imposed on the possible transfers can be effective to mitigate risk. As a reminder, person-to-person loads followed by cash or transfers out may be indicative of a money mule.

- The FATF Guidance notes that limiting the functionality of prepaid access products to certain geographical areas makes them less attractive to money launderers or terrorist financiers. The FATF Guidance proposes that, given that risk corresponds to prepaid access functionality, Financial institutions should consider implementing individual tiers of services for customers. In this way, Financial institutions could apply differing restrictions for prepaid access to ensure they remain lower in risk and thus require simplified CDD measures.

- Limits or prohibitions on certain usage (e.g. merchant type) and on geographic usage, such as outside the United States or activity in the Middle East.

Additional Prepaid Monitoring

Monitoring is an essential activity to ensure that internal controls are achieving their goals and to provide early detection of suspicious situations. Depending on the functions that an organization provides, prepaid-related monitoring may include reviewing:

- Prepaid access activity to detect transactions of unusual size, volume, pattern, or type of activity—considering the purpose for which the prepaid access was issued. For example, cash value loads followed closely by cash withdrawals from ATMs (especially foreign ATMs) or excessive credits to the prepaid access should be detected and investigated. In addition, prepaid access activity should be monitored to detect suspicious volumes of transactions occurring through a single merchant or third-party Agent;

- Value loads made by or through third parties—such as retail load networks or employers—to assure that they are coming through expected load sources, in expected amounts and frequencies. Monitor for multiple unrelated funds transfers onto prepaid access product, such as tax refund fraud situations where multiple tax refunds are loaded onto one card;

- Reversals of funding transactions. Fraudulently used funding accounts should be added to a negative file and funding transactions should be evaluated against that file;

- International transactions;

- Return/refund transactions to confirm that the prepaid access was used to make corresponding purchases;

- Monitor purchases/loads of prepaid access for suspicious dollar amounts and/or patterns of multiple transactions for suspicious dollar amounts;[13]

- For consumer-funded prepaid access, monitor single-source funding to multiple prepaid access; and

- Sales agents for prepaid access sales/load transaction volumes that are suspicious (e.g., excessive based on expected transaction activity). Monitor sales of multiple small denomination prepaid access, and bulk purchases at the point of sale.

- The FATF Guidance suggests that prepaid access providers monitor activity for which there is no apparent legitimate or economic rationale. The FATF Guidance provides the example of a prepaid access user making frequent high-value transactions. According to the Guidance, such activity is uncharacteristic given that prepaid access "may not offer similar levels of protection . . . or benefits" as other products such as deposit insurance or the ability to accumulate interest.

- If ATM/PIN reloads are permitted or offered, as with all other cash loads, the loads should be monitored for possible structuring.

Prepaid Reporting

Periodic reports can assist organizations to identify potential prepaid-related issues and resolve them promptly. Depending on the functions that an organization provides, prepaid-related reporting may include:

- Load volumes (by cash, ACH, ATM, reload networks, credit/debit cards);

- ATM Activity reports (focus on foreign transactions);

- Funds transfer reports;

- New account activity reports;

- Reports to identify related or linked accounts (common addresses, phone numbers, e-mail addresses, and taxpayer identification numbers)

- Cash out transactions;

- Credits back to the prepaid access account;

- Multiple cash withdrawals per account;

- International transactions;

[13] For example, periodic cash load transactions in amounts just under reporting thresholds might indicate suspicious activity which should be investigated.

- Duplicate prepaid access sales;
- Excessive sales at retail; and
- Chargebacks and reversals of loads due to fraudulent or suspicious transactions.

SECTION 4: FEDERAL REPORTING REQUIREMENTS

This section provides information about the responsibilities of organizations to comply with federal law by filing SARs and CTRs.

Under the BSA and Prepaid Access Rule, financial institutions, including providers or sellers of prepaid access, are responsible for filing SARs and CTRs related to prepaid activity.[14] These organizations are urged to understand their prepaid- related SAR and CTR filing requirements and to take the necessary steps to ensure compliance. General information about SAR and CTR filing is provided in this Section.

Suspicious Activity Reports

SAR filing is the primary method by which financial institutions report suspected criminal activity. The SAR regulations mandate that a SAR must be filed for:

> Criminal violations involving insider abuse involving any amount;

> Criminal violations aggregating $5,000 or more when a suspect can be identified;

> Criminal violations aggregating $25,000 or more regardless of whether a potential suspect can be identified; and

> Transactions aggregating $5,000 or more ($2,000 or more for MSBs) that involve potential money laundering or violations of the BSA if the institution knows, suspects, or has reason to suspect that the transaction:

Potential Red Flags

- **A customer with an excessive number of cards (based on program parameters)**
- **A customer who is unwilling to provide required information to perform CIP**
- **A customer who presents unusual or suspicious identification documents that the financial institution cannot readily verify**
- **A customer who requests cards be shipped outside of the United States**
- **A customer uses different tax identification numbers with variations of his or her name**
- **A customer who is reluctant to provide the information needed for a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed**
- **A cardholder that coerces or attempts to coerce a bank employee to not file any required recordkeeping or reporting forms**
- **High dollar deposits followed by numerous small withdrawals**
- **A cardholder who makes multiple value loads on the same day at different load locations**
- **Large number of failed authorizations**
- **Transactions posted to the card account without corresponding authorizations**
- **Transactions occurring in more than one state or country on the same day**
- **Repetitive transactions occurring at the same time for the same amount each day or each week**
- **Transactions consistently occurring outside of the Cardholder's residential area**
- **Unexplainable transactions with no logical purpose**
- **Repeated transactions outside of the cardholder's normal activity**
- **Multiple transactions slightly below reportable thresholds**

[14] If an organization is uncertain about its filing responsibilities, it should check with qualified legal counsel.

- May involve potential money laundering or other illegal activity (e.g., terrorism financing);
- Is designed to evade the BSA or its implementing regulations; or
- Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the Financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Under the Prepaid Access Rule, providers and sellers of prepaid access are considered MSBs that are required to file SARs. Since most Issuers of network branded prepaid access are banks, MSBs and other third-party agents of an issuer should coordinate decisions to file SARs with the Issuer of the prepaid access. Among other considerations, the safe harbor for filing SARs (described further below) may not apply to the voluntary filing of a SAR by an entity that is neither a bank nor an MSB under the laws and regulations.[15]

Information on Filing Suspicious Activity Reports (SARs)

- **A Bank is required to file a SAR no later than 30 calendar days after the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect can be identified, the time period for filing a SAR is extended to no later than 60 calendar days from the date of detection of the incident.**
- **MSBs are required to file a SAR no later than 30 calendar days after the date of the initial detection, regardless of whether a suspect can be identified.**
- **Organizations may need to review transaction or account activity for a customer to determine whether to file a SAR. The need for a review of customer activity or transactions does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the organization, during its review or because of other factors, knows or has reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity.**
- **Financial institutions must keep a copy of any SAR filed and the original or business record equivalent of any supporting documentation for a period of 5 years from the date of filing. Supporting documentation must also be identified and maintained by the institution and is deemed to have been filed with the SAR.**
- **Financial institutions are required to notify the Board that SARs have been filed. Financial institutions may, but are not required to, provide actual copies of the SARs to the Board. Summaries, tables, and other forms of notification are acceptable.**
- **Federal law prohibits notifying anyone involved in the suspicious activity that a SAR is being filed or has been filed. This prohibition extends to disclosures that could indirectly result in notifying the subject of a SAR that a SAR has been filed, effectively precluding the disclosure of a SAR or even its existence to any persons other than appropriate law enforcement and supervisory agency or agencies.**
- **In most situations when federal law enforcement officials want to review a Financial institution's records pertaining to an individual, they must follow the RFPA, which requires the individual's permission, a search warrant, or other specified means. The RFPA, however, does not apply to financial records or information required to be reported in accordance with any federal statute or related rule. Because SARs are reported under federal law and regulation, the RFPA does not apply to information included in a SAR, nor does it apply to the information referenced in the SAR as supporting documentation.**
- **Federal law provides Financial institutions with broad liability protection when they provide customer information as part of a SAR filing (a "safe-harbor" protection). Specifically, Financial institutions that disclose any possible violation of law or regulation under the SAR rules or any other authority are not liable to any person for the disclosure itself or for any failure to notify the person involved in the transaction or any other person of the disclosure. This protection applies to any director, officer, employee, or agent of the Financial institution, as well as to the institution itself.**

[15] The safe harbor protection extends to "agents" of a Financial institution.

Financial institution policies, procedures, and processes should indicate the persons responsible for identifying, researching, and reporting suspicious activities. Appropriate policies, procedures, and processes should be in place to monitor and identify unusual activity. The process should ensure that all applicable information (e.g., criminal subpoenas, NSLs, and Section 314(a) requests, as applicable) is effectively evaluated. The level of monitoring should be dictated by the financial institution's assessment of risk, with particular emphasis on high-risk products, services, customers, and geographic locations. Monitoring systems typically include employee identification or referrals, manual systems, automated systems, or any combination. The financial institution should ensure adequate staff is assigned to identifying, researching, and reporting suspicious activities, taking into account the financial institution's overall risk profile and the volume of transactions.

Upon identifying unusual activity, additional research is typically conducted. The decision to file a SAR is a subjective judgment, within the guidelines mandated. CDD information may assist financial institutions evaluate if the unusual activity is considered suspicious. Thorough documentation provides a record of the SAR decision-making process including final decisions not to file a SAR.

Financial institutions are required to file complete and accurate reports that include all relevant information available, including cyber-related information. If a financial institution knows, suspects, or has reason to suspect that a cyber-event was intended, in whole, or in part, to conduct or facilitate a transaction or series of transactions, it should be considered part of an attempt to conduct suspicious activity, and included in the SAR. While suspicious transactions may not always involve a cyber-event, relevant cyber information should be included in SARs when available.[16]

Financial institutions should also note that filing a SAR does not relieve financial institutions from any other applicable requirements to timely notify the appropriate Payment Network and regulatory agencies of events concerning the critical systems and information or of disruptions in their ability to operate.16 If an organization is unsure about its cyber-related reporting SAR requirements, it should check with qualified legal counsel.

Suspicious activity reports are confidential, and the Bank Secrecy Act and federal regulations specifically prohibit the unauthorized disclosure of the SAR, or any information that may reveal the existence of a SAR. Both civil and criminal penalties may be imposed for SAR disclosure violations.

Under 31 U.S.C. 5318(g)(3), federal law protects Financial institutions from civil liability for all reports of suspicious transactions made to appropriate authorities, regardless of whether such reports are filed pursuant to SAR regulations. Therefore, the safe harbor protects SARs filed above the required reporting threshold, as well as to SARs filed voluntarily on any activity below the threshold. The safe harbor applies to reports made by the Financial institution itself, and it extends directors, officers, employees, and agents of the financial institution.

Currency Transaction Reports (CTRs)

[16] FinCEN Advisory FIN-2016-A005 "Advisory to Financial institutions on Cyber-Events and Cyber-Enabled Crime" (October 2016) and FinCEN FAQ on Cyber-Event October 25, 2016:https://www.fincen.gov/frequently-asked-questions-faqs-regarding-reporting-cyber-events-cyber-enabled-crime-and-cyber

Under 31 C.F.R. 1010.330, unless an exemption applies,[17] Financial institutions must file a CTR for transactions in currency by any one person that amount to more than $10,000 in one day.

Multiple currency transactions that occur in one day are treated as a single transaction if the Financial institution has knowledge that they are by or on behalf of the same person and result in either cash in or cash out totaling more than $10,000 during any one business day. Financial institutions must design appropriate systems to identify and aggregate cash transactions.

All CTRs must be filed electronically within 15 days following the date of the transaction. The Financial institution must retain a copy of each report filed for 5 years from the date of the report.

A CTR should not be filed for suspicious transactions involving $10,000 or less in currency OR to indicate that a transaction of more than $10,000 is suspicious; appropriate SAR filing procedures should be followed in these situations. However, if a transaction is suspicious AND in excess of $10,000 in currency, then both a CTR and the appropriate Suspicious Activity Report form must be filed.

[17] The exemptions to filing CTRs are beyond the scope of this document.

SECTION 5: CUSTOMER IDENTIFICATION PROGRAM (CIP) AND CUSTOMER DUE DILIGENCE (CDD)

This section addresses a variety of issues relating to requirements for establishing the identity of consumers and businesses buying prepaid cards. It includes when CIP requirements apply and when they may not apply to prepaid cards, how to mitigate risk related to "anonymous" prepaid cards, risk-based CIP, and applying CIP to B-to-B prepaid cards.

As required by Section 326 of the USA PATRIOT Act, the Department of the Treasury, through FinCEN, has adopted regulations that require Financial institutions to implement reasonable procedures for:

> Verifying the identity of any person seeking to open an account, to the extent reasonable and practicable;

> Maintaining records of the information used to verify the person's identity including name, address, and other identifying information; and

> Determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the Financial institution by any government agency.

Recommendations for Anonymous Prepaid Cards

For prepaid cards where the consumer provides the funds to load the card and where Cardholder name and Cardholder data are not collected and verified ("anonymous cards"), risk mitigation steps may include:

- **Limiting the amount of the initial value load - These Recommended Practices support requiring compliance with the CIP rule requirements for consumer-funded prepaid card where the value load is $1,000 or more. Payment Network rules vary on this requirement and, in many cases, set a lower limit**
- **Prohibiting reloads**
- **Prohibiting cash access**
- **Prohibiting cross border access for anonymous prepaid cards**
- **Requiring a purchaser of an unusually large number of cards to provide CIP information as well as the rationale for the bulk purchase.**

USA PATRIOT Act Section 311 – Special Measures

Section 311 of the USA PATRIOT Act amended the BSA by adding 31 USC 5318A, which authorizes the Secretary of Treasury to require domestic financial institutions and agencies to take certain special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts of primary money laundering concern.

Specific special measures may be imposed by an order without prior public notice and comment, but such orders must be of limited duration and must be issued together with a Notice of Proposed Rulemaking.

Types of Special Measures

There are five (5) types of special measures that can be imposed, either individually, jointly or in any combination, and they are as follows:

i. **Recordkeeping and Reporting of Certain Financial Transactions**
ii. **Information Relating to Beneficial Ownership**
iii. **Information Relating to Certain Payable Through Accounts**
iv. **Information Relating to Certain Correspondent Accounts**
v. **Prohibitions or Conditions on Opening or Maintaining Certain Correspondent or Payable through Accounts**

CIP Requirements for Banks

The CIP rules applicable to banks, savings associations, and credit unions are set forth at 31 C.F.R. 1020.220. The regulations require a bank to include risk-based procedures for verifying the identity of each customer, enabling the bank to form a reasonable belief that it knows the true identify of each customer. At a minimum, the bank must obtain the following information from a customer prior to opening an account:

i. Name;

ii. Date of birth, for an individual;

iii. Address, which shall be:

   a. for an individual—a residential or business street address;

   b. for an individual who does not have a residential or business street address—an Army Post Office or Fleet Post Office box number, or the residential or business street address of next of kin or another contact individual (a Post Office box number is NOT sufficient); or

c. for a person other than an individual (e.g., a corporation, partnership, or trust)—a principal place of business, local office, or other physical location; and

iv. Identification number, which shall be:

a. for a U.S. person—a taxpayer identification number; or

b. for a non-U.S. person—one or more of the following: taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of any other government-issued document evidencing nationality and residence and bearing a photograph or similar safeguard.

The CIP must contain risk-based procedures for verifying the identity of the customer within a reasonable period of time after an account is opened. It is not necessary to establish the accuracy of every element of identifying information obtained, but enough information must be verified to form a reasonable belief that the financial institution knows the true identity of the customer. The financial institution's procedures must describe when it will use documentary, nondocumentary methods, or a combination.

A financial institution using documentary methods to verify a customer's identity must have procedures that establish minimum acceptable documentation. The rule reflects the federal banking agencies' expectations that financial institutions will review an unexpired government-issued form of identification from most customers. This identification must provide evidence of a customer's nationality or residence and bear a photograph or similar safeguard. Examples of acceptable identification include a driver's license or passport. Other forms of identification may be used if they enable the financial institution to form a reasonable belief that it knows the true identity of the customer. Given the availability of counterfeit and fraudulently obtained documents, a financial institution is encouraged to review more than a single document to ensure that it has a reasonable belief that it knows the customer's true identity.

For a "person" other than an individual (such as a corporation, partnership, or trust), the financial institution should obtain documents showing the legal existence of the entity such as certified articles of incorporation, an unexpired government-issued business license, a partnership agreement, or a trust instrument.

A financial institution using nondocumentary methods to verify a customer's identity must have procedures that set forth the methods the financial institution will use.

Nondocumentary methods may include contacting a customer; independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement. For prepaid access products, typical nondocumentary methods include verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source.

The financial institution's CIP procedures must also address the following situations: An individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard; the financial institution is not familiar with the documents presented; the account is opened without obtaining documents (e.g., the financial institution obtains the required information from the customer with the intent to verify it); the customer opens the account without appearing in person; or the Financial institution is otherwise

presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents.

The CIP must address situations where, based on its risk assessment of a new account opened by a customer that is not an individual, the Financial institution will obtain information about individuals with authority or control over such accounts, including signatories, in order to verify the customer's identity. This verification method applies only when the Financial institution cannot verify the customer's true identity using documentary or nondocumentary methods. For example, a Financial institution may need to obtain information about and verify the identity of a sole proprietor or the principals in a partnership when the financial institution cannot otherwise satisfactorily identify the sole proprietorship or the partnership.

The CIP must include procedures for determining whether the customer appears on any federal government list of known or suspected terrorists or terrorist organizations.

Financial institutions will be contacted by the U.S. Treasury in consultation with their federal banking agency when a list is issued.

The CIP must include procedures for when the bank cannot form a reasonable belief that it knows the true identify of a customer. These procedures should describe:

1. When the bank should not open an account;

2. The terms under which a customer may use an account while the bank attempts to verify a customer's identity;

3. When the bank should close an account after attempts to verify a customer's identity have failed; and

4. When the bank should file a SAR in accordance with applicable law and regulation.

Finally, the CIP must include procedures for providing customers with adequate notice that the bank is requesting information to verify their identities. Notice is considered adequate if the bank generally describes the identification requirements and provides the notice in a manner reasonably designed to ensure that a customer is able to view the notice—or is otherwise given notice—before opening an account. Sample language is provided below:

> ***IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT*** *— To help the government fight the funding of terrorism and money laundering activities, federal law requires all Financial institutions to obtain, verify, and record information that identifies each person who opens an account. What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.*

A Financial institution's CIP must include recordkeeping procedures. At a minimum, the Financial institution must retain the identifying information (name, address, date of birth for an individual, TIN, and any other information required by the CIP) obtained at account opening for a period of five years after the account is closed or becomes dormant. The bank must also keep a description of the following for five years after the record was made:

- Any document that was relied on to verify identity, noting the type of document, the identification number, the place of issuance, and, if any, the date of issuance and expiration date.[18]
- The method and the results of any measures undertaken to verify identity.
- The results of any substantive discrepancy discovered when verifying identity.

The federal banking agencies and FinCEN issued guidance in March 2016 to clarify CIP requirements for banks that issue prepaid cards.[19]

Topic covered included:

- The applicable CIP requirements are derived by, first, determining whether an Account (as defined) is created and, second, identifying the Customer (as defined).
- An Account is created when a Customer exercises the ability to reload funds onto the prepaid card, or accesses the prepaid card's credit or overdraft features.
- Depending on the nature of the prepaid card program, the Customer could be either the cardholder or the third-party card provider.
- A bank's CIP requirements should be applied to the Customer.
- The guidance also reiterates a bank's responsibility of entering into well-constructed, enforceable contracts with third-party program managers.

Later, on May 11, 2016, the Financial Crimes Enforcement Network (FinCEN) issued the Customer Due Diligence Requirements for financial institutions (CDD Rule) as a final rule with mandatory compliance on May 11, 2018. The CDD Rule, which amends Bank Secrecy Act regulations, aims to improve financial transparency and prevent criminals and terrorists from misusing companies to disguise their illicit activities and launder their ill-gotten gains. The CDD Rule clarifies and strengthens customer due diligence requirements for U.S. banks, mutual funds, brokers or dealers in securities, futures commission merchants, and introducing brokers in commodities. The CDD Rule requires these covered financial institutions to identify and verify the identity of the natural persons (known as beneficial owners) of legal entity customers who own, control, and profit from companies when those companies open accounts.

[18] A Financial institution may keep photocopies of identifying documents that it uses to verify a customer's identity; however, the CIP regulation does not require it. A Financial institution's verification procedures should be risk-based and, in certain situations, keeping copies of identifying documents may be warranted. In addition, a Financial institution may have procedures to keep copies of the documents for other purposes, for example, to facilitate investigating potential fraud. However, if a Financial institution does choose to retain photocopies of identifying documents, it should ensure that these photocopies are physically and electronically secured to adequately protect against possible identity theft.

[19] https://www.fdic.gov/news/news/financial/2016/fil16021a.pdf

The CDD Rule has four core requirements. It requires covered financial institutions to establish and maintain written policies and procedures that are reasonably designed to:

1. Identify and verify the identity of customers;
2. Identify and verify the identity of the beneficial owners of companies opening accounts;
3. Understand the nature and purpose of customer relationships to develop customer risk profiles;
4. Conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information;
5. With respect to the requirement to obtain beneficial ownership information, financial institutions will have to identify and verify the identity of any individual who owns 25 percent or more of a legal entity, and an individual who controls the legal entity.

While items 1, 3 and 4 were already mandated by various regulations, the CDD introduces additional requirements for financial institutions to identify customers who are business entities. See Appendix 2 for a listing of business entities by category and the impact of the rule.

CIP Requirements for Banks - Entities

When a customer has been identified as a business entity, the identification and verification of the beneficial owners of the customer is required. The identification and verification of the beneficial owners of the customer is detailed in the section below.

Beneficial Ownership Identification and Verification

Information for beneficial owners must be both current AND certified by a natural person, to the best of his or her knowledge, who is authorized by the customer to open/manage the account. Note – previously collected alternate sources of beneficial ownership information, such as the W-8BEN, are not permitted.

If information exists that is contrary to the beneficial owner information presented at the time of account opening, then BSA/AML team is notified and confirm the legitimacy of the information from acceptable documentary sources before the business customer.

The percentage equity interest of each beneficial owner has in the legal entity customer and the controlling individual's title (e.g., a Chief Executive Officer, Chief Financial Officers, Managing Member, General Partner, President, etc.) must be collected/documented. Verification of beneficial owners require the review of one unexpired government issued photo ID; a secondary document is not required.

Beneficial Owner Collection of Additional Ownership or Equity Interests

In addition to the natural persons identified as beneficial owners, PPMS requires that the collection of the name, address, identification number and percentage ownership for any other entities that may have 25% or more ownership interest in the Customer but are not a natural person.

Certification

The CDD Final Rule requires that the person opening the Account on behalf of a Business/Legal Entity Customer must certify to the best of his or her knowledge that the Beneficial Ownership information provided is accurate.

Triggering Events

In addition to the beneficial owner information required when a Business Customer opens a new account; the CDD Rules has defined instances triggering when beneficial owner information must be obtained or updated for a Customer previously not required to provide beneficial owner information or where beneficial owner should be revisited (hereinafter called "Triggering Event").

The following is a list of Triggering Events:

- When the Legal Entity which is a Customer that enters into a new agreement or amends a current agreement with an existing third party (this includes contract slated for auto-renewals).
- Beneficial owner re-certification is required when any of the following occurs:
  - Change in beneficial ownership.
  - Change in the third party's name or tax identification number.
  - Negative news regarding the Customer or a current beneficial owner.
  - Equity interests are structured to avoid reporting threshold.
  - When a beneficial owner or customer is identified as an OFAC match.
  - When a beneficial owner is identified as a PEP.
  - Any confirmed suspicious activity on customer or a current beneficial owner.

Documenting Excluded Entities

The Final Rule exempts or excludes some customers from having to provide all, or a portion of, the Beneficial Ownership information. Certain Legal Entity Customers are excluded from the requirement to identify BOs and two categories (charities and non-profits) partially excluded.

The categories of entirely excluded customers include:

- Financial institutions regulated by a federal functional regulator or bank regulated by a state regulator.
- Certain US and non-US government entities.

- Domestic Public companies[20].
- Investment companies, advisors and other registered with Securities and Exchange Commission (SEC).
- Certain entities registered with the Commodity Futures Trading Commission (CFTC).
- Certain foreign financial institutions.
- Insurance companies subject to state regulations.

Charities and non-profit organizations do not need to provide the ownership information. However, the PPMS requires the collection and verification of the control prong as per the Regulations.

A full list of exclusions as defined by the Final Rule can be found at Appendix 3. Periodic reviews are required to ensure that the excluded customer can legally continue to be excluded (that is, their status has not changed).

Collection and Verification Exceptions

Collection Exception

A collection exception is a case where the bank's electronic data records show information obtained from the source of record regarding a prospective Customer or Beneficial Owner's identifying information collected may not be complete or is erroneous.

Where the bank records indicate that the information on any accounts may be missing, invalid or otherwise inaccurate data; the information must be updated forthwith, and the bank may choose to close, suspend or block the business account. In the event a business entity account has been closed, suspended or blocked, the cards funded by the business entity are allowed to spend down the current balance on the cards. However, the cards will not be allowed to be reloaded until such time the exception has been cleared.

Verification Exception

If a customer or beneficial owner cannot be verified at account opening, then the options are as follows:

- If the accountholder is an individual, allow them to have a card with limited functionality
- Deny Account opening and reject any loads or security deposit.
- Open the account, but the account cannot be used until the accountholder or beneficial owner is verified.

Generally, verification of a Customer or beneficial owner's identity must take place within a reasonable timeframe, which is usually deemed to be fourteen (14) calendar days and thirty (30) calendar day for General Business Use Prepaid Products. If, despite attempts to verify prospective Customer's identity, and this cannot be done (a reasonable belief that you the true identity of the Customer) then the following should occur:

- Allow the accountholder to spend down the funds on the card.

[20] This is for entities publicly traded on domestic exchanges that are regulated by the SEC such as the NYSE or NASDAQ. This does not included entities publicly traded on foreign exchanges.

- If a beneficial owner, the customer to which the beneficial owner is tied will have their account closed, suspended or blocked. (Individual cards previously loaded by the customer will not be closed but will not be able to receive further reloads).
- Return any funds loaded to card/account in accordance with internal procedures.

Record Retention

The following information for beneficial owners and beneficial owners process is retained:

- Identifying information obtained from the customer or beneficial owner:
- Name, address, date of birth and identification number will be retained for **5 years after the date the account is closed.**
- A description of any non-documentary methods of verification used and the results of such methods to verify the prospective customer's or BO's identity will be retained **for 5 years after the record is created.**
- A description of each of the document(s) relied on for verification. This will be **retained for 5 years after the record is created.**

The CIP rule does not alter a bank's authority to use a Third-party agent, such as an agent or service provider, to perform CIP services on its behalf. Therefore, a bank Issuer is permitted to arrange for a Third-party agent (e.g., a Program Manager), acting as its agent, to verify the identity of its customer. The bank may also arrange for a Third-party agent to maintain its records. However, as with any other responsibility performed by a Third-party agent, the bank is ultimately responsible for that Third-party agent's compliance with the bank's CIP. As a result, banks should establish adequate controls and review procedures for such relationships.

A description of the resolution of any substantive discrepancy discovered when verifying the identifying information obtained from a prospective customer ***will be retained for 5 years after the record is created****.*

Customer Identification Information Collection (CIIC) Requirements for MSBs.

The CIIC requirements for MSBs are designed to mirror the CIP requirements of other Financial institutions and draw on the explanations and interpretations issued with respect to those requirements. Under 31 C.F.R. 1022.210(d)(1)(iv), an MSB that is a provider or seller of prepaid access must establish procedures to verify the identity of a person who obtains prepaid access under a prepaid program. The MSB must collect identifying information, including, at a minimum: name, date of birth, address, and identification number. Sellers of prepaid access must also establish procedures to verify the identity of a person who obtains prepaid access to funds that exceed $10,000 during any one day and obtain identifying information concerning such a person, including name, date of birth, address, and identification number. Providers of prepaid access must retain access to such identifying information for five years after the last use of the prepaid access device or vehicle. Sellers of prepaid access must retain such information for five years from the date of the sale of the prepaid access device or vehicle.

It is important to remember that the applicability of the CIIC requirement depends on the definitions set out in Section 1. For example, open-loop prepaid access to funds less than $1,000 through a device or vehicle that does not allow international use, transfers between prepaid access products within one prepaid program, or loads from non- depository sources does not require a provider to collect customer identification because such a program does not qualify as a "prepaid program" under the Prepaid Access Rule.

With respect to sellers of prepaid access, there are only two situations under which an entity would become a "seller of prepaid access" subject to customer identification/collection requirements. The first situation arises where the customer can access funds under a prepaid access program prior to the completion of customer identification procedures. In this situation, which links to the definition of "prepaid program," both the provider and seller are responsible for the collection of customer information. By agreement they may allocate this responsibility among themselves.

The second situation arises where there are sales of any type of prepaid access to funds that exceed $10,000 to any person during any one day. Since this definition is linked to the sale of more than $10,000 of any type of prepaid access, whether covered under a prepaid program or not (e.g., closed-loop access), there may be situations under which an entity may be a seller, but not a provider, and therefore nevertheless obligated to collect customer identification.

B-to-B Uses

When a business entity seeks to purchase prepaid access for distribution to customers and employees, and the business entity provides funding for the prepaid access, the Financial institution should follow its CIP and collect and verify relevant information regarding the business entity.[21]

Customer Due Diligence

The cornerstone of a strong BSA/AML compliance program is the adoption and implementation of comprehensive CDD policies, procedures, and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing. The objective of CDD should be to enable the Financial institution to predict with relative certainty the types of transactions in which a customer is likely to engage. These processes assist the Financial institution in determining when transactions are potentially suspicious. The concept of CDD begins with verifying the customer's identity and assessing the risks associated with that customer. Processes should also include enhanced CDD for higher-risk customers and ongoing due diligence of the customer base.

Effective CDD policies, procedures, and processes provide the critical framework that enables the Financial institution to comply with regulatory requirements and to report suspicious activity. CDD policies, procedures, and processes are critical to the Financial institution because they can aid in:

- Detecting and reporting unusual or suspicious transactions that potentially expose the Financial institution to financial loss, increased expenses, or reputational risk.

[21] If anonymous cards are sold in a B-to-B relationship, the Issuer should consider implementing the controls set forth in Section 2.

- Avoiding criminal exposure from persons who use or attempt to use the Financial institution's products and services for illicit purposes.
- Adhering to safe and sound banking practices.

BSA/AML policies, procedures, and processes should include CDD guidelines that:

- Are commensurate with the financial institution's BSA/AML risk profile, paying particular attention to higher-risk customers.
- Contain a clear statement of management's overall expectations and establish specific staff responsibilities, including who is responsible for reviewing or approving changes to a customer's risk rating or profile, as applicable.
- Ensure that the financial institution possesses sufficient customer information to implement an effective suspicious activity monitoring system.
- Provide guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.
- Ensure the financial institution maintains current customer information.

Management should have a thorough understanding of the money laundering or terrorist financing risks of the financial institution's customer base. Under this approach, the financial institution should obtain information at account opening, or within a reasonable time from account opening, sufficient to develop an understanding of normal and expected activity for the customer's occupation or business operations. This understanding may be based on account type or customer classification.

This information should allow the financial institution to differentiate between lower-risk customers and higher-risk customers at account opening. financial institutions should monitor their lower-risk customers through regular suspicious activity monitoring and customer due diligence processes. If there is indication of a potential change in the customer's risk profile (e.g., expected account activity, change in employment or business operations), management should reassess the customer risk rating and follow established financial institution policies and procedures for maintaining or changing customer risk ratings.

Much of the CDD information may be confirmed through an information-reporting agency, banking references (for larger accounts), correspondence and telephone conversations with the customer, and visits to the customer's place of business. Additional steps may include obtaining third-party references or researching public information (e.g., on the Internet or commercial databases).

CDD processes should include periodic risk-based monitoring of the customer relationship to determine whether there are substantive changes to the original CDD information (e.g., change in employment or business operations).

Customers that pose higher money laundering or terrorist financing risks present increased exposure to financial institutions; due diligence policies, procedures, and processes should be enhanced as a result. Enhanced due diligence (EDD) for higher- risk customers is especially critical in understanding their anticipated transactions and implementing a suspicious activity monitoring system that reduces the financial institution's reputation, compliance, and transaction risks. Higher-risk customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the financial institution.

The financial institution may determine that a customer poses a higher risk because of the customer's business activity, ownership structure, anticipated or actual volume and types of transactions, including those transactions involving higher-risk jurisdictions. If so, the financial institution should consider obtaining, both at account opening and throughout the relationship, the following information on the customer:

- Purpose of the account
- Source of funds and wealth
- Individuals with ownership or control over the account, such as beneficial owners, signatories, or guarantors
- Occupation or type of business (of customer or other individuals with ownership or control over the account)
- Financial statements
- Banking references
- Domicile (where the business is organized)
- Proximity of the customer's residence, place of employment, or place of business to the financial institution
- Description of the customer's primary trade area and whether international transactions are expected to be routine
- Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers
- Explanations for changes in account activity

As due diligence is an ongoing process, a financial institution should take measures to ensure account profiles are current and monitoring should be risk-based. financial institutions should consider whether risk profiles should be adjusted, or suspicious activity reported when the activity is inconsistent with the profile.

SECTION 6: THIRD-PARTY AGENTS

This section details the requirements of risk-based due diligence evaluations Issuers should conduct before engaging Third-party agents in their prepaid card programs.

Like many debit and credit card programs, prepaid access programs often use Third-party agents to perform specialized services that supplement the Issuer's core competencies or that take advantage of the Third-party agent's scale advantage. There are many benefits to these arrangements, including cost efficiencies and the advantages of doing business with organizations with specific expertise in processing, distributing, selling, or storing prepaid access products.[22]

Third-party Agent relationships are common to both bank-centered and non-bank- centered programs and require robust compliance management systems. Guidance issued by the federal banking agencies confirms that use of a Third-Party Agent increases the need for compliance oversight from start to finish.[23] The Financial institution's board of directors (or a board committee) and senior management are responsible for overseeing the financial institution's overall risk management processes. The board, senior management, and employees within the lines of businesses who manage the Third-Party Agent relationships have distinct but interrelated responsibilities to ensure that the relationships and activities are managed effectively and commensurate with their level of risk and complexity, particularly for relationships that involve critical activities. The five main elements of an effective Third-party agent risk compliance management process include:

i. **Risk assessment**—the process of assessing risks and options for controlling Third Party Agent arrangements;
ii. **Due diligence in selecting a Third-party agent**—the process of selecting a qualified entity to implement the activity or program;
iii. **Contract structuring and review**—the process of ensuring that the specific expectations and obligations of both the institution and the Third-party agent are outlined in a written contract prior to entering into the arrangement; the contract should map the relationship and define its structure;
iv. **Oversight**—the process of reviewing the operational and financial performance of Third-party agent activities to ensure that the Third-Party Agent meets and can continue to meet the terms of the contractual arrangement; and
v. **Termination** - Developing a contingency plan to ensure that the financial institution can transition the activities to another third party, bring the activities in- house, or discontinue the activities when a

[22] Examples of such programs include agent bank programs, employer-payroll card programs, merchant gift card programs, insurance company claims card programs, rebate company promotional card programs, and other programs involving third-party Processors, co-branding partners, activation and load service providers, and reload networks

[23] OCC Bulletin 2013-29, Third-Party Relationships, October 30, 2013, http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html; FDIC FIL-43-2013, FDIC Supervisory Approach to Payment Processing, September 27, 2013, http://www.fdic.gov/news/news/financial /2013/fil13043.html; FDIC FIL-44-2008, Guidance for Managing Third-Party Risk, June 6, 2008, http://www.fdic.gov/news/news/financial /2008/fil08044a.html; CFPB Bulletin 2012-03, April 13. 2012,Service Providers; Federal Reserve Board, Guidance on Managing Outsourcing Risk, SR 13-19 CA 13-21, December 5, 2013, http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service- providers.pdf

contract expires, the terms of the contract have been satisfied, in response to contract default, or in response to changes to the financial institution's or third party's business strategy.

1. Risk Assessment

The FDIC and the OCC have identified numerous categories of risk to which a financial institution may be exposed by virtue of a third-party agent relationship. The institution's board or senior management should understand the nature of these risks in the context of current or planned use of third parties and in establishing risk oversight and control systems. Categories of third-party agent risk include:

- **Compliance risk** is the risk arising from violations of laws, rules, regulations, or from noncompliance with the institution's internal policies, procedures, or business standards. For example, compliance risk is implicated where a third-party agent engages in deceptive practices, does not comply with notice and disclosure regulations, or does not adequately protect customer information from data breaches.

- **Reputation risk** is the risk arising from negative public opinion. Reputation risk stems from dissatisfied customers, unexpected customer financial loss, interactions not consistent with institutional policies, inappropriate recommendations, security breaches, and violations of law. Any negative publicity involving the third-party agent—whether or not the publicity is related to the institution—could result in reputation risk.

- **Strategic risk** is the risk arising from adverse business decisions or the failure to effectively implement business decisions. The use of a third-party agent to offer products or services that do not help the institution achieve an adequate return on investment exposes the institution to strategic risk.

- **Operational risk** is the risk of loss resulting from inadequate or failed internal processes, people, systems or external events. Third-party relationships often integrate the internal processes of the third-party agent with the institution's processes and can increase operational complexity and risk.

- **Transaction risk** is the risk arising from problems with service or product delivery. A third-party agent's failure to meet customer expectations due to inadequate capacity, technological failure, human error, or fraud exposes the institution to transaction risk. The lack of an effective business resumption plan and appropriate contingency plans increase transaction risk. Weak control over third-party technology may result in threats to security and the integrity of systems and resources. These issues could result in unauthorized transactions or the inability to conduct business as expected.

- **Credit risk** is the risk that a Third-party agent is unable to meet the contractual terms of the relationship or to otherwise financially perform as expected. The basic form of credit risk involves the financial condition of the Third-party agent itself.

- **Country risk** is the exposure to the economic, social, and political conditions and events in a foreign country that may adversely affect the ability of a foreign based Third-party agent to meet the level of service

required by the arrangement. In extreme cases, this exposure could result in the loss of data, R&D efforts, or other assets.

2. Due Diligence in Selecting a Third-Party Agent

A financial institution that contracts with a third-party agent accepts the risks related to the services provided by its agents. Therefore, prior to program launch, a financial institution should complete a thorough due diligence review of the third parties with which it plans to partner. Recommended practices include:

- Where an Issuer contracts with a third-party agent Distributor or Program Manager to market, distribute or support aspects of a prepaid access program, the Issuer must ensure, through contract requirements and initial and on-going due diligence procedures, that the Distributor/Program Manager implements adequate BSA/AML compliance programs.

- Where an Issuer or Program Manager contracts with a Processor to provide Core Processing Services for its prepaid access programs, the Issuer or Program Manager must ensure that the Processor implements adequate BSA/AML compliance programs and internal controls.

- Where a Program Manager contracts with a third-party agent Distributor to market, distribute, or support aspects of a prepaid access program, the Program Manager must ensure, through contract requirements and initial and on-going due diligence procedures, that the Distributor implements adequate BSA/AML compliance programs.

Special Considerations for Third-Party Reload Arrangements

If the financial institution is selling or reloading prepaid cards through retail store establishments, it should ensure compliance with any applicable federal or state:

- **Laws regulating and/or licensing non-bank providers of money services businesses**
- **Banking or branching laws regulating activities of the Issuer and/or its agents and other Third Party Agent**

A review of the third parties should be conducted based on the financial institution's risk assessment of the third-party agent and the details of the prepaid program. Particular attention should be given to ensuring that any issues or concerns identified as part of the initial due diligence have been addressed appropriately. When determining the extent of review that may be required, the financial institution should consider the functions being performed by the third-party agent; the level of review may be tiered accordingly. Reviews should be risk-based and, as appropriate, may consist of elements including, but not limited to, financial assessment and background and reference checks.

The due diligence review may include one or more of the following:

- A financial review of the third-party agent utilizing one or more of the following:
  - Credit reports;

- Personal and business financial statements; and/or
- Income tax returns.

- A background review of the third-party agent including:
  - Background and reference checks;
  - Identification of prior agent relationships; and
  - Identification of prior business bankruptcy filings.
- A compliance review of all relevant BSA/AML requirements:
  - CIP practices as required by the USA PATRIOT Act;
  - Implementation and maintenance of an effective BSA/AML program;
  - Written documentation of BSA/AML program; and
  - Independent review reports of compliance.
- Physical inspection of the business premises of the agent, whenever feasible;
- A review to ensure that all third parties have appropriate risk controls in place prior to program launch (as well as ongoing reviews to ensure continued compliance) based on the risk profiles of the product and third-party agent;
- A review of current registrations or licenses required for the third-party agent to conduct business with respect to prepaid access products;
- Checks on all parties against the Specially Designated National (SDN) list published by OFAC and for other prohibited transactions or persons designated under OFAC regulations; and
- Finally, financial institutions should ensure that agent/client/employer training is included in overall training plans and that there is an ongoing training and communication strategy for all third-party agent programs.

3. Contract Structuring and Review

Once the third-party agent is selected, the arrangement with the third-party agent should be governed by a well-constructed, enforceable service contract that clearly defines expectations, duties, rights, and obligations of each party. A binding contract or agreement should include, at a minimum:

- the scope of the relationship and explicit details about all services to be performed by the service provider, including training of employees and customer service;

- a complete description of the costs and fees for services, the parties responsible for payment, and any conditions under which the cost structure may be changed, or the relationship may be terminated without penalties;

- responsibilities for providing and receiving information, including the frequency and types of reports, consumer complaints, materiality thresholds, and procedures in the event of service disruption or security breaches that pose a material risk to the financial institution;

- plans for business resumptions, continuity, and contingencies in the event of problems affecting the Third-Party Agent's operations—these plans should outline each party's responsibilities, provide for testing of plans and the frequency of testing, and state the Financial institution's right to obtain the results of such tests;

- a clause that outlines the BSA/AML and OFAC obligations of the parties, including monitoring and reporting suspicious activity;

- a clause that provides for the institution's right to audit the third-party agent to monitor its performance—generally, institutions need to ensure that periodic independent internal and/or external audits are conducted to ensure prudent operations and compliance with applicable laws and regulations;

- a clause outlining agency authority to examine the third-party agent under federal law, and assess the provider's ability to perform under its contractual obligations;

- a clause that defines (1) how the parties will share information about fraud losses and suspicious activity and (2) the process for sharing and/or indemnifying losses; and

- a clause outlining the authority of the institution to terminate the relationship.

Any material or significant contract with a third-party agent should prohibit assignment, transfer, or subcontracting by the third-party agent of its obligations unless the institution consents to the assignment after performing adequate due diligence.

4. Oversight

Finally, the institution should engage in an ongoing, proactive compliance review of all third-party agent relationships. The oversight component of a compliance management system should include:

- Board approval and annual review of all significant third-party agent arrangements and review of material changes when they occur;

- periodic management review of third-party agent operations for consistency with contractual terms, internal risk management policies and procedures, and laws and regulations;

- appointment of an individual or committee to coordinate oversight activities, such as monitoring of the Third-party agent's quality of service, risk management, financial condition, and applicable controls and reports;

- documentation and reporting of identified weaknesses to the Board;

- maintenance of records for all aspects of the Third-party agent relationship, including valid contracts, business plans, risk analyses, due diligence, oversight activities, and dispute resolution documents, and for what period of time; and

- procedures for terminating or probating Third Party Agent relationships based on findings from audits and performance monitoring.

5. Termination.

A financial institution may terminate third-party relationships for various reasons, including expiration or satisfaction of the contract, desire to seek an alternate third party, desire to bring the activity in-house or discontinue the activity, or breach of contract. Management should ensure that relationships terminate in an efficient manner, whether the activities are transitioned to another third party, brought in-house, or discontinued. In the event of contract default or termination, the Financial institution should have a plan to bring the service in-house if there are no alternate third parties. This plan should cover (1) capabilities, resources, and the time frame required to transition the activity while still managing legal, regulatory, customer, and other impacts that might arise, (2) risks associated with data retention and destruction, information system connections and access control issues, or other control concerns that require additional risk management and monitoring during and after the end of the third-party relationship, (3) handling of joint intellectual property developed during the course of the arrangement, and (4) reputation risks to the financial institution if the termination happens as a result of the third party's inability to meet expectations. The extent and flexibility of termination rights may vary with the type of activity.

SECTION 7: INDEPENDENT COMPLIANCE TESTING

This section addresses the timing of independent testing and who may conduct independent testing. This section also provides recommendations for the areas that should be checked as part of an independent review and, finally, how an independent review should be documented.

Independent, objective compliance testing is an essential step in evaluating whether appropriate internal controls are in place and being followed. Testing can point out areas that need improvement or have been overlooked, as well as confirming that proper policies, procedures, and processes are being carried out.

Qualifications of Independent Testers

Each Issuer, Program Manager and any Processor performing Core Processing Services should arrange for independent testing of their BSA/AML compliance program. It is recommended that such independent testing occur at least every 12 to 18 months, depending on their BSA/AML risk profile. The independent testing may be performed by the internal audit department, outside auditors, consultants, or other qualified independent parties. Financial institutions that do not employ outside auditors/consultants or have internal audit departments may comply with this requirement by using qualified persons who are not involved in or reporting through persons responsible for the day-to-day compliance functions being tested.

As for Issuers, persons conducting the testing should report to the board or to a designated board committee comprised primarily or completely of outside directors.

Those persons responsible for conducting an objective independent evaluation of the written BSA/AML compliance program should perform testing for specific compliance with the BSA and evaluate pertinent management information systems (MIS). Testing should be risk based and evaluate the quality of risk management for all banking operations, departments, and subsidiaries. Risk-based testing programs will vary depending on the financial institution's size, complexity, scope of activities, risk profile, quality of control functions, geographic diversity, and use of technology. An effective risk-based testing program will cover all of the financial institution's activities. The frequency and depth of each activity's audit will vary according to the activity's risk assessment. Risk-based testing enables the board and auditors to use the financial institution's risk assessment to focus the audit scope on the areas of greatest concern. The testing should assist the board and management in identifying areas of weakness or areas where there is a need for enhancements or stronger controls.

Independent Testing Recommendations

Independent testing should, at a minimum, include:

- An evaluation of the overall integrity and effectiveness of the compliance program including policies, procedures, and processes;

- A review of the financial institution's risk assessment for reasonableness given the financial institution's risk profile (products, services, customers, entities, and geographic locations);

- Appropriate risk-based transaction testing to verify the financial institution's adherence to BSA recordkeeping and reporting requirements (e.g., CIP, SARs, CTRs, CTR exemptions, OFAC matches, and information sharing requests);

- An evaluation of management's efforts to resolve violations and deficiencies noted in previous reviews and regulatory examinations including progress in addressing outstanding supervisory actions, if applicable;

- A review of staff training for adequacy, accuracy, and completeness;

- A review of the effectiveness of the suspicious activity monitoring systems (manual, automated, or a combination) used for BSA/AML compliance;
    - Related reports may include, but are not limited to:
        - Suspicious activity monitoring reports
        - Large currency aggregation reports
        - Monetary instrument records
        - Funds transfer records
        - Nonsufficient funds (NSF) reports
        - Large balance fluctuation reports
        - Account relationship reports

- An assessment of the overall process for identifying and reporting suspicious activity including a review of filed or prepared SARs to determine their accuracy, timeliness, completeness, and effectiveness of the financial institution's policy. The assessment should also review situations where suspected suspicious activity was detected but, following an analysis of the facts, a decision was made to not file a SAR, and the documentation supporting such decision.

- An assessment of the integrity and accuracy of MIS used in the BSA/AML compliance program. MIS includes reports used to identify large currency transactions, aggregate daily currency transactions, funds transfer transactions, monetary instrument sales transactions, and analytical and trend reports.

Documenting Independent Testing

Auditors are encouraged to use a sampling methodology in their independent testing, which includes determining appropriate sample size. Sampling allows the auditor to observe a random subset to learn about the multitude of items from which they are drawn. There are a number of Sampling Methodologies. In determining the Sampling Methodology to use, the quantity, quality and nature of the population to be reviewed and the overall risk should be considered. The Sampling Method recommended or required by the appropriate regulatory body or governing entity of the financial institution, should also be taken into consideration.

Non-Statistical Sampling – Judgmental sampling allows the auditor to review an identified percentage of a specific population and helps identify specific exceptions. Statistical Sampling includes Numerical Sampling and Proportional Sampling. In Numerical Sampling, each item in a population is equally likely to be selected in the

sample and this methodology can be helpful when the frequency of errors, exceptions or other features of interest is of primary concern. In Proportional Sampling, the likelihood of an item being selected is proportionate to the item's size or value, and this methodology can be helpful when the objective of the sample is to review items for a specific characteristic, such as the dollar amount of the transaction. In that scenario, large dollar amounts have a greater chance of being selected than smaller ones; all items greater than a certain amount and a representative number of smaller items are generally selected.[24]

Auditors should document the review scope, procedures performed, transaction testing completed, and findings of the review. Any violations, policy or procedures exceptions, or other deficiencies noted during the review should be included in a review report and reported to the board or a designated committee in a timely manner.

Periodic external independent audits should be considered, which serve to validate the internal audit reviews and/or identify gaps or concerns not previously recognized.

The board or designated committee and the review staff should track review deficiencies and document corrective actions.

[24] Comptroller's Handbook: Sampling Methodologies - https://occ.treas.gov/publications/publications-by-type/comptrollers-handbook/sampling-methodologies/index-ch-sampling-methodologies.html

SECTION 8: TRAINING APPROPRIATE PERSONNEL

This section provides a bullet-point list emphasizing the board members and employees who should be included in a BSA/AML training program and topic areas that should be covered.

Financial institutions must ensure that appropriate personnel, including members of the financial institution's board, are trained in all applicable aspects of BSA/AML requirements.

The training should be tailored to the person's specific responsibilities. In addition, an overview of the BSA/AML requirements typically should be given to new staff during employee orientation.

The board and senior management should be informed of changes and new developments in the BSA, its implementing regulations and directives, and the federal banking agencies' regulations. While the Board may not require the same degree of training as banking operations personnel, they need to understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance, and the risks posed to the financial institution. Without a general understanding of the BSA, the board cannot adequately provide BSA/AML oversight; approve BSA/AML policies, procedures, and processes; or provide sufficient BSA/AML resources.

Training and training programs should:

- Include regulatory requirements and the Financial institution's internal BSA/AML policies, procedures, and processes;
- Be tailored to an individual's specific responsibilities within the company;
- Be provided to new staff as appropriate;
- Encompass information related to applicable operational lines;
- Be ongoing and incorporate current developments and changes to the BSA or any related regulations;
- Ensure that new product and service development incorporates a BSA review step;
- Include changes to internal policies, procedures, processes, and monitoring systems;
- Reinforce the importance that the board and senior management place on the financial institution's compliance with the BSA and ensure that all employees understand their roles in maintaining an effective BSA/AML compliance program; and;
- Be documented.

APPENDIX

Appendix 1 – Statutes

12 U.S.C. 1829b, 12 U.S.C. 1951–1959, and 31 U.S.C. 5311, et seq.

"The Bank Secrecy Act"

12 U.S.C. 1818(s)

"Compliance with Monetary Recordkeeping and Report Requirements"

Requires that the appropriate federal banking agencies shall prescribe regulations requiring insured depository institutions to establish and maintain procedures reasonably designed to assure and monitor the compliance of such depository institutions with the requirements of the BSA. In addition, this section requires that each examination of an insured depository institution by the appropriate federal banking agency shall include a review of the procedures, and that the report of examination shall describe any problem with the procedures maintained by the insured depository institution. Finally, if the appropriate federal banking agency determines that an insured depository institution has either 1) failed to establish and maintain procedures that are reasonably designed to assure and monitor the institution's compliance with the BSA; or 2) failed to correct any problem with the procedures that a report of examination or other written supervisory communication identifies as requiring communication to the institution's Board of Directors or senior management as a matter that must be corrected, the agency shall issue an order requiring such depository institution to cease and desist from the violation of the statute and the regulations prescribed thereunder. Sections 1818(b)(3) and (b)(4) of Title 12 of the U.S.C. extend section 1818(s) beyond insured depository institutions.

Regulations

U.S. Treasury/FinCEN

31 C.F.R. Chapter X

Sets forth FinCEN regulations that promulgate the BSA. Relevant subsections are described below.

PART 1010—GENERAL PROVISIONS

Subpart A—General Definitions

1010.100 General definitions.

Subpart B—Programs

Subpart C—Reports Required To Be Made

Subpart D—Records Required To Be Maintained

Subpart E—Special Information Sharing Procedures To Deter Money Laundering and Terrorist Activity

1020.500 General.

1020.520 Special information sharing procedures to deter money laundering and terrorist activity for banks.

1020.540 Voluntary information sharing among financial institutions.

Subpart F—Special Standards of Diligence; Prohibitions; and Special Measures

1020.600 General.

1020.610 Due diligence programs for correspondent accounts for foreign financial institutions.

1020.620 Due diligence programs for private banking accounts.

1020.630 Prohibition on correspondent accounts for foreign shell banks; records concerning owners of foreign banks and agents for service of legal process.

1020.670 Summons or subpoena of foreign bank records; termination of correspondent relationship.

PART 1022—RULES FOR MONEY SERVICES BUSINESSES

Subpart A—Definitions

1022.100 Definitions.

Subpart B—Programs

1022.200 General.

1022.210 Anti-money laundering programs for money services businesses.

Subpart C—Reports Required To Be Made By Money Services Businesses

1022.300 General.

1022.310 Reports of transactions in currency.

1022.311 Filing obligations.

1022.312 Identification required.

1022.313 Aggregation.

1022.314 Structured transactions.

1022.315 Exemptions.

1022.320 Reports by money services businesses of suspicious transactions.

1022.380 Registration of money services businesses.

Subpart D—Records Required To Be Maintained By Money Services Businesses

1022.400 General.

1022.410 Additional records to be made and retained by dealers in foreign exchange.

1022.420 Additional records to be maintained by providers and sellers of prepaid access.

Subpart E—Special Information Sharing Procedures To Deter Money Laundering and Terrorist Activity

1022.500 General.

1022.520 Special information sharing procedures to deter money laundering and terrorist activity for money services businesses.

1022.540 Voluntary information sharing among financial institutions.

Subpart F—Special Standards of Diligence; Prohibitions; and Special Measures for Money Services Businesses

1022.600 General.

Board of Governors of the Federal Reserve System

Regulation H — 12 C.F.R. 208.62

"Suspicious Activity Reports"

Sets forth the requirements for state member banks for filing a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.

Regulation H — 12 C.F.R. 208.63

"Procedures for Monitoring Bank Secrecy Act Compliance"

Sets forth the requirements for state member banks to establish and maintain procedures to ensure and monitor their compliance with the BSA.

Federal Deposit Insurance Corporation

12 C.F.R. 326 Subpart B

"Procedures for Monitoring Bank Secrecy Act Compliance"

Sets forth requirements for state nonmember banks to establish and maintain procedures to ensure and monitor their compliance with the BSA.

12 C.F.R. 353

"Suspicious Activity Reports"

Establishes requirements for state nonmember banks to file a SAR when they detect a known or suspected violation of federal law, a suspicious transaction relating to a money laundering activity, or a violation of the BSA.

National Credit Union Administration

12 C.F.R. 748

"Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance"

Requires federally insured credit unions to maintain security programs and comply with the BSA.

12 C.F.R. 748.1

"Filing of Reports"

Requires federally insured credit unions to file compliance and Suspicious Activity Reports.

12 C.F.R. 748.2

"Procedures for Monitoring Bank Secrecy Act (BSA) Compliance"

Ensures that all federally insured credit unions establish and maintain procedures reasonably designed to assure and monitor compliance with the recordkeeping and reporting requirements in the BSA.

Office of the Comptroller of the Currency

12 C.F.R. 21.11

"Suspicious Activity Report"

Ensures that national banks file a Suspicious Activity Report when they detect a known or suspected violation of federal law or a suspicious transaction relating to a money laundering activity or a violation of the BSA. This section applies to all national banks as well as any federal branches and agencies of foreign financial institutions licensed or chartered by the OCC.

12 C.F.R. 21.21

"Procedures for Monitoring Bank Secrecy Act (BSA) Compliance"

Requires all national banks to establish and maintain procedures to ensure and monitor their compliance with the BSA.

Other Materials

Federal Financial institutions Examination Council (FFIEC)

The FFIEC's web site (www.ffiec.gov) includes the following information:

- BSA/AML Examination Manual InfoBase.

- Information Technology Handbooks.

U.S. Government

Interagency U.S. Money Laundering Threat Assessment (MLTA) (December 2005) - The MLTA is a government-wide analysis of money laundering in the United States. The MLTA offers a detailed analysis of money laundering methods, ranging from well- established techniques for integrating dirty money into the financial system to modern innovations that exploit global payment networks as well as the Internet. (www.treas.gov/press/releases/reports/js3077_01112005_MLTA.pdf)

Financial Crimes Enforcement Network (FinCEN)

FinCEN's web site (www.fincen.gov) includes the following information:

- BSA Forms — Links to BSA reporting forms, and instructions for magnetic and electronic filing.
- SAR Activity Reviews – Trends, Tips & Issues and By the Numbers — Meaningful information about the preparation, use, and value of Suspicious Activity Reports (SARs) filed by financial institutions.
- BSA Guidance — Frequently Asked Questions, FinCEN rulings, guidance on preparing a complete and accurate SAR narrative, and country advisories.
- Reports — Links to FinCEN Reports to Congress, the U.S. Treasury's National Money Laundering Strategy, and the U.S. State Department's International Narcotics Control Strategy Report.
- Federal Register notices.
- Enforcement actions.

Financial Action Task Force on Money Laundering (FATF)

FATF's web site (www.fatf- gafi.org) includes a number of useful reports and recommendations

Guidance for a Risk Based Approach: Prepaid Cards, Mobile Payments, and Internet Based Payment Services, available at http://www.fatf- gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf (June 2013).

Appendix 2 - Listing of Business Entities by Category and the Impact of the Rule

Business Category	Description	Subject to Beneficial Ownership Requirements
Sole Proprietorship-no EIN	*A sole proprietor is someone who owns an unincorporated business. Income from the business is reported with the owners TIN.*	**NO** - The business is not a separate entity from the owner/ individual
Sole Proprietorship-with EIN	*A sole proprietor is someone who owns an unincorporated business*	**NO** - Income from the business is reported with the business EIN
General Partnership	*Assumes that profits, liability and management duties are divided equally among partners. For unequal distribution, the percentages assigned to each partner is required to be documented in the partnership agreement.*	**YES**
Limited Liability Partnership (LLP)	*LLPs partners have limited liability as well as limited input in management decisions. These limits depend on the extent of each partner's investment percentage.*	**YES**
Corporation (for-profit). Includes "S" or "C" corporation.	*A corporation is a legal entity.*	**YES**
Limited Liability Corporation	*A business structure allowed by state statute.*	**YES**
Nonprofit corporation	*This is exempt from the federal corporate income tax under Section 501 (c) (3) of the Internal Revenue Code*	**YES** – only the control prong should be documented
Non-chartered organization	*A group of persons who create an informal entity. The entity may not have articles or other documents to establish its formation. An EIN is required. Examples include: Clubs, civic organizations, etc.*	**YES** – only the control prong should be documented
Cooperative	*A cooperative is a business / organization owned by and operated*	**YES**

	for the benefit of those using its services. Profits and earnings generated by the cooperative are distributed among the members.	

Appendix 3 - CDD Final Rule Excluded Entities

The Final Rule does allow for some Customers to be excluded from having to provide all, or a portion of, the Beneficial Ownership information. Exclusions include:

1. Accounts opened by sole proprietorships or unincorporated associations.
2. Accounts opened under ERISA (e.g. FSA/HRA).
3. A financial institution regulated by a Federal functional regulator or a bank regulated by a State bank regulator.
4. A person described in § 1020.315(b)(2) through (5) of this chapter—§ 1010.230(e)(2)(ii):

    A. *A department or agency of the United States, of any State, or of any political subdivision of a State.*
    B. *Any entity established under the laws of the United States, of any State, or of any political subdivision of any State, or under an interstate compact between two or more States, that exercises governmental authority on behalf of the United States or of any such State or political subdivision.*
    C. *Any entity (other than a bank) whose common stock or analogous equity interests are listed on the New York, American (NYSE MKT), or NASDAQ stock exchange.*
    D. *Any entity organized under the laws of the United States or of any State at least 51 percent of whose common stock or analogous equity interests are held by a listed entity.*
    E. *An issuer of a class of securities registered under section 12 of the Securities Exchange Act of 1934 or that is required to file reports under section 15(d) of that Act.*
    F. *An investment company, as defined in Section 3 of the Investment Company Act of 1940, that is registered with the SEC under that Act.*
    G. *An investment adviser, as defined in section 202(a)(11) of the Investment Advisers Act of 1940, that is registered with the SEC under that Act.*
    H. *An exchange or clearing agency, as defined in section 3 of the Securities Exchange Act of 1934, that is registered under section 6 or 17A of that Act.*
    I. *Any other entity registered with the SEC under the Securities and Exchange Act of 1934.*
    J. *A registered entity, commodity pool operator, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant, each as defined in section 1a of the Commodity Exchange Act, that is registered with the CFTC.*

K. *A public accounting firm registered under section 102 of the Sarbanes-Oxley Act.*

L. *A bank holding company, as defined in section 2 of the Bank Holding Company Act of 1956 (12 U.S.C. 1841), or savings and loan holding company, as defined in section 10(n) of the Home Owners' Loan Act.*

M. *A pooled investment vehicle that is operated or advised by a financial institution excluded under this paragraph.*

N. *An insurance company that is regulated by a State.*

O. *A financial market utility designated by the Financial Stability Oversight Council under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.*

P. *A foreign financial institution established in a jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution.*

Q. *A non-U.S. governmental department, agency or political subdivision that engages only in governmental rather than commercial activities.*

R. *Any Legal Entity only to the extent that it opens a private banking Account subject to 31 CFR 1010.620.*

S. *Non-excluded Pooled Investment Vehicles.*

T. *Intermediated Account Relationships:*
   i. *Investment Accounts excluded.*
   ii. *Attorney client and escrow Accounts (IOLTA).*

U. *Charities and NPO:*
   i. *Excluded from ownership, still need control.*
   ii. *Defined as any Legal Entity that is established as a nonprofit corporation or similar entity and has filed its organizational documents with the appropriate state authority as necessary.*
   iii. *Includes community organizations.*

V. *Private label retail credit Accounts established at the point-of-sale.*

W. *Accounts established for the purchase and financing of postage where payments are remitted directly by the FI to the provider of postage products.*

X. *Commercial Accounts to Finance Insurance Premiums.*

Y. *Accounts to finance the purchase or lease of equipment.*

Note – the preceding three exclusions do not apply when:

I. *The Legal Entity Customer can make payments to, or receive payments from, third parties.*

II. *A cash refund is available. In this instance the requirements must be met at the time of initial remittance or at the time such refund occurs.*