



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

***This guide does not necessarily express the views of every member of the NBPCA. 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 Card Brand rules and policies for prepaid card products. Each Issuer of a prepaid card must comply with the rules and policies of the applicable Card Brand(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 Network Branded Prepaid Card Association (NBPCA) 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 NBPCA, 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 NBPCA...

The Network Branded Prepaid Card Association (NBPCA) is a nonprofit, inter-industry trade association that supports the growth and success of network branded prepaid cards and represents the common interests of the many participants in this new and rapidly growing payments category. The NBPCA's working groups drive issues management and education objectives for the Association's more than 35 members. For additional information, visit [www.NBPCA.com](http://www.NBPCA.com).

## TABLE OF CONTENTS

<b>Glossary of Acronyms</b>	4
<b>Introduction</b>	5
■ Entities Covered by BSA/AML Requirements	5
■ Key Participants In the Prepaid Card Value Chain	6
■ Foundation of these Recommended Practices	8
■ Intent	8
■ How to Use these Recommended Practices	9
■ Document Overview	9
<b>Section 1: Risk Assessment</b>	12
■ Geographic Location Risk	12
■ Customer Risk	13
■ Product/Services Risk	14
<b>Section 2: Internal Controls</b>	16
■ Internal Controls—General	16
■ Internal Controls—Prepaid Cards	17
■ Prepaid Monitoring	18
■ Prepaid Reporting	19
<b>Section 3: Federal Reporting Requirements</b>	20
■ Suspicious Activity Reports	20
■ Currency Transaction Reports	22
<b>Section 4: Know Your Customer</b>	23
■ Determining When CIP Applies	23
■ Risk-Based CIP	24
■ B2B Uses	24
<b>Section 5: Third-Party Agents</b>	25
■ Due Diligence Review	26
<b>Section 6: Independent Compliance Testing</b>	28
■ Qualifications of Independent Testers	28
■ Independent Testing Recommendations	28
■ Documenting Independent Testing	29
<b>Section 7: Training Appropriate Personnel</b>	30
<b>Appendix</b>	31

## GLOSSARY OF ACRONYMS

The following acronyms are used in these Recommended Practices:

<b>AML</b>	Anti-Money Laundering
<b>ATM</b>	Automated Teller Machine
<b>B2B</b>	Business to Business
<b>BSA</b>	Bank Secrecy Act
<b>CDD</b>	Customer Due Diligence
<b>C.F.R.</b>	Code of Federal Regulations
<b>CIP</b>	Customer Identification Program
<b>CTF</b>	Counter-Terrorist Financing
<b>CTR</b>	Currency Transaction Report
<b>FATF</b>	Financial Action Task Force
<b>FDIC</b>	Federal Deposit Insurance Corporation
<b>FinCEN</b>	Financial Crimes Enforcement Network
<b>FSA</b>	Flexible Spending Account
<b>HIDTA</b>	High Intensity Drug Trafficking Area
<b>HIFCA</b>	High Risk Money Laundering Related Financial Crimes Area
<b>HSA</b>	Health Savings Account
<b>INCSR</b>	International Narcotics Control Strategy Report
<b>MSB</b>	Money Services Business
<b>NSL</b>	National Security Letter
<b>OCC</b>	Office of the Comptroller of the Currency
<b>OFAC</b>	Office of Foreign Assets Control
<b>OTS</b>	Office of Thrift Supervision
<b>PCI DSS</b>	Payment Card Industry Data Security Standard
<b>RFPA</b>	Right to Financial Privacy Act
<b>SAR</b>	Suspicious Activity Report
<b>SDN</b>	Specially Designated National

## INTRODUCTION

As the trade association representing members of the network branded prepaid card<sup>1</sup> industry, the NBPCA encourages practices that reduce opportunities for prepaid cards 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 BSA/AML compliance programs.

To make **all** prepaid industry participants aware of their BSA/AML compliance responsibilities for prepaid cards and to encourage **all** to implement appropriate practices, the NBPCA developed this document outlining “Recommended Practices for Anti-Money Laundering Compliance for U.S.-Based Prepaid Card Programs.” This document represents a compilation of the principles and practices of a cross-section of NBPCA members that have committed significant resources to applying BSA/AML requirements to prepaid cards issued in the United States.

### Entities Covered by BSA/AML Requirements

The BSA gives the Secretary of the Treasury broad discretion to define the entities subject to the BSA along with report and record-keeping requirements. FinCEN, a bureau within Treasury, administers and issues regulations pursuant to the BSA. These regulations appear at 31 C.F.R. 103 - Financial Recordkeeping and Reporting of Currency and Foreign Transactions.

#### ■ Banks and Their Agents

The regulations, at 31 C.F.R. 103.11(c), 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;

---

<sup>1</sup> Network branded prepaid cards carry the logo of a major network such as American Express, Discover, MasterCard, or Visa. 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 to use in the United States and others are limited to eligible purchases (i.e., health care cards).

For the purposes of this document, the word “prepaid” refers to network branded (open-loop) prepaid - unless otherwise specified.

- (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;
- (7) Any other organization (except a 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)."

#### ■ MSBs

Certain MSBs are defined as financial institutions for BSA regulatory purposes and fall within FinCEN's regulatory ambit. MSBs under 31 C.F.R. 103.11(uu) include: (a) an issuer of stored value, other than a person who does not issue such stored value in a total amount greater than \$1,000 in currency or monetary or other instruments for any person on any day in one or more transactions; (b) a seller or redeemer of stored value, other than a person who does not sell such stored value in an amount greater than \$1,000 in currency or monetary or other instruments to, or redeem such instruments for an amount greater than \$1,000 from, any person on any day in one or more transactions; and (c) a money transmitter.

Under current regulations, MSB issuers, sellers and redeemers of stored value are exempt from the FinCEN registration requirements and SAR filing requirements but must otherwise comply with all other BSA/AML requirements.

#### **Key Participants in the Prepaid Card 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 card value chain and their respective roles:

“Card Brand” - 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 cards bearing their brand. The Card Brands issue rules and regulations applicable to Issuers and acquiring (merchant) banks that participate in their card programs.

“Cardholder” - The owner/user of the prepaid card. This may be the card 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 cards. 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 HSA or FSA cards to plan beneficiaries.

“Issuer” - An entity, which is typically a bank, that issues a prepaid card to a Cardholder. Also called the issuing bank. The Issuer must be licensed by the Card Brand to participate in their card programs. For prepaid cards bearing the brands of American Express or Discover, the Issuer may be a financial institution which has an issuer agreement with American Express or Discover or the card may be issued directly by American Express or Discover to the Cardholder.

“Processor” - A Processor facilitates payment transactions for prepaid cards. A Processor may provide one or more of the following services related to a prepaid card program: (a) card account set up and card activation; (b) card plastics production; (c) Cardholder agreement design and production; (d) mailing of cards, Cardholder agreements and privacy policies to Cardholders; (e) provision of authorizations for card transactions; (f) value load and reload processing; (g) 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 Card Brands. Some Issuers and Program Managers also serve the role of a Processor. For a particular card 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) card account set up and card activation; (ii) provision of authorizations for card transactions; (iii) value load and reload processing; and (iv) security/fraud control and reporting.

“Program Manager” - A Program Manager is a non-bank entity that contracts with an Issuer to establish, market, and operate prepaid card programs. By way of example, a payroll processor may act as a Program Manager to offer employers prepaid payroll cards 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.

“Third-Party Agent” - In these Recommended Practices, a third-party agent may be a Program Manager or Distributor. Depending on the card type and program structure, other non-bank entities also may be third-party agents.

## 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:

Certain enumerated financial institutions, including banks and certain MSBs, are required to have in place programs to ensure the institution's compliance with BSA and AML requirements.<sup>2</sup> When a financial institution contracts with a third party to market, distribute, or support aspects of a prepaid card 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 of Directors<sup>3</sup>, with such approval to be noted in the board meeting minutes. The compliance programs must include:

- A system of internal controls to ensure ongoing compliance including written policies and procedures;
- Independent testing of compliance;
- On-going coordination and monitoring of compliance by a designated person; and
- 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 card 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.

---

<sup>2</sup> All businesses are also required to implement programs to ensure compliance with the sanctions programs administered by the Office of Foreign Asset Control (OFAC). This document does not address OFAC compliance programs.

<sup>3</sup> In this Guide, references to "Board of Directors" or "Directors" also means any similar governing body of a non-corporate entity.

## How to Use these Recommended Practices

The NBPCA encourages every member of the network branded prepaid card industry—not only NBPCA 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 card 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 NBPCA recognizes that all methods of payment and funds exchange are vulnerable to misuse. We believe, however, that well run prepaid card programs are less vulnerable than other media of exchange such as cash and checks.<sup>4</sup> We also believe that the convenience of prepaid cards 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.

## Document Overview

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

- **Section 1: Risk Assessment.** A multi-faceted risk assessment is the cornerstone of any organization's BSA/AML compliance program for prepaid cards. This section discusses identifying the money laundering and terrorist financing risks associated

---

<sup>4</sup> 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>.

with customers and transactions and implementing appropriate measures and controls to mitigate these risks.

This section highlights one of the most difficult aspects of dealing with money laundering and terrorist financing issues, i.e., 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 2: Internal Controls.** Internal controls (policies, procedures, and processes) are a key tool to limit and control risks associated with prepaid cards 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 3: Federal Reporting Requirements.** Financial Institutions subject to the BSA may be responsible for filing SARs and 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 4: Know Your Customer.** 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 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 B2B prepaid cards.

- **Section 5: 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 cards programs.

- **Section 6: 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 if an external party cannot be used 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 7: Training Appropriate Personnel.** Financial institutions must ensure that appropriate personnel, including members of the financial institution's Board of Directors, 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: RISK ASSESSMENT

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 emanate 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. Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same.

*This section highlights one of the most difficult aspects of dealing with money laundering and terrorist financing issues, i.e., risk assessment 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, so there is little certainty in the decision-making process.*

Identifying the money laundering and terrorist financing risks of products, customers and/or transactions enables financial institutions to determine and implement proportionate measures and controls to mitigate these risks. Risks for some customers may become evident only once the customer has commenced using the prepaid card (or, for merchants, selling)—making transaction monitoring a fundamental component of a risk-based approach. Money laundering risks may be measured using various criteria. The most commonly used risk criteria are geographic location risk, customer risk, product risk and services risk.

### Geographic Location Risk

High-risk geographic locations may be either international or domestic.

International high-risk geographic locations generally include:

- Foreign jurisdictions that are designated as a "primary money laundering concern" in accordance with Section 311 of the USA PATRIOT Act;
- 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;
- Countries identified by the FATF as non-cooperative in the fight against money laundering or identified as "Jurisdictions of Primary Concern" in the INCSR, issued annually by the U.S. State Department; 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).

Domestic high-risk geographic areas include HIDTAs and HIFCAs.

### **Customer Risk**

Each financial institution must assess, based on its own criteria, whether a particular customer poses a higher risk of money laundering. There is no universal consensus as to which customers pose a higher risk, but, as it relates to “typical” prepaid card customers, the following characteristics of customers have been identified with potentially higher money laundering risks:

- Customers or third-party agents located in HIDTAs<sup>5</sup> or HIFCAs<sup>6</sup>;
- Foreign financial institutions including banks and foreign money service providers;
- Non-bank financial institutions (e.g., MSBs; 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 politically exposed persons or PEPs);
- Nonresident alien 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);
- Professional service providers (e.g., attorneys, accountants, doctors, and real estate brokers);
- The use or involvement of intermediaries within the relationship (however, the involvement of an intermediary that is subjected to adequate BSA/AML regulation and is supervised for compliance with such regulation or otherwise employs adequate BSA/AML procedures generally poses reduced money laundering risks); and
- Customers who have counter-parties or beneficiaries located in high risk geographic regions.

---

<sup>5</sup> The current listing of these areas can be found at [www.whitehousedrugpolicy.gov/hidta/index.html](http://www.whitehousedrugpolicy.gov/hidta/index.html).

<sup>6</sup> The current listing of these areas can be found at [www.irs.gov/compliance/enforcement/article/0,,id=107510,00.html](http://www.irs.gov/compliance/enforcement/article/0,,id=107510,00.html).

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 risks presented by products and services offered by a financial institution also assists in overall risk assessment. A financial institution should consider the following issues and features in assessing the money laundering risks related to its prepaid card products:

- How are prepaid cards distributed?
- Who is the customer (e.g., governmental agency, business, or consumer; is there an existing relationship with the customer) for the cards?
- How are the cards funded?
- What is the expected level of prepaid activity?
- Are the prepaid cards reloadable?
- Are value load sources restricted?
- Can the prepaid cards be used to obtain cash (at ATMs, at point of sale, or through a cash advance transaction)?
- Can funds be transferred from one prepaid card to another prepaid card or other financial account?
- Are bulk purchases of Cards permitted?
- Are multiple distribution channels allowed (i.e., Internet)?
- Can the card be used internationally?

- Is the amount of funds permitted on the prepaid card (at any one time and in the aggregate) limited?

## SECTION 2: INTERNAL CONTROLS

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.

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

### Internal Controls—General

Any organization participating in the prepaid card 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 (products, services, customers, and geographic locations) vulnerable to abuse by money launderers and criminals, provide for periodic updates to the financial institution's risk profile (recommended that a new risk review be undertaken at least every 12 to 18 months), and provide for a BSA/AML compliance program tailored to manage the identified risks;
- Keep the financial institution's Board of Directors and senior management informed of compliance initiatives, identified compliance issues and deficiencies, corrective actions taken, and 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 and CTRs;<sup>7</sup>
- Provide for dual controls and segregation of duties (employees who complete the reporting forms (e.g., SARs, CTRs, and CTR exemptions) also should not be responsible for filing the reports or granting the exemptions);
- Provide for sufficient controls and monitoring systems for timely detection and reporting of suspicious activity;
- Establish policies and procedures for implementing risk mitigating actions;
- 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 compliance into the job descriptions and performance evaluations of appropriate personnel.

### **Internal Controls—Prepaid Cards<sup>8</sup>**

In addition to the above, participants in the prepaid card value chain should establish controls specific to their prepaid card 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 cards, based on program parameters;<sup>9</sup>
- For transaction aggregation and reporting, detect multiple card 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 and cash access based on amounts that are reasonable and appropriate for Cardholders and/or card product types, considering the purpose for which the cards were issued. Issuers should establish 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 establish and monitor daily/weekly cash access and purchase limits for Cardholders.

---

<sup>7</sup> Reporting requirements under OFAC are not covered by this document.

<sup>8</sup> 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.

<sup>9</sup> 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.

- Monitor purchases/loads of cards for suspicious dollar amounts and/or patterns of multiple transactions for suspicious dollar amounts;<sup>10</sup>
- For consumer-funded cards, monitor single-source funding to multiple prepaid cards; and
- When loads are accomplished through credit or debit cards, use fraud monitoring tools—such as address verification services, card verification values, online verification systems (Verified by Visa, MasterCard SecureCode), and fraud scoring systems—to detect potentially fraudulent transactions.

## **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:

- Card activity to detect transactions of unusual size, volume, pattern, or type of activity—considering the purpose for which the cards were issued. For example, cash value loads followed closely by cash withdraws from ATMs (especially foreign ATMs) or excessive credits to the card should be detected and investigated. In addition, card activity should be monitored to detect suspicious volumes of transactions occurring through a single merchant or third party;
- 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;
- Reversals of funding transaction reversals to detect potential fraud. 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 card was used to make corresponding purchases;
- Sales agents for card sales/load transaction volumes that are suspicious (e.g., excessive based on expected transaction activity). Monitor sales of multiple small denomination cards, and bulk purchases at the point of sale.

---

<sup>10</sup> For example, periodic cash load transactions in amounts just under reporting thresholds might indicate suspicious activity which should be investigated.

## **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, credit/debit cards);
- Cash out transactions;
- Credits back to the prepaid card account;
- Multiple withdrawals per account;
- International transactions;
- Duplicate card sales; and
- Chargebacks and reversals of loads due to fraudulent transactions.

## SECTION 3: FEDERAL REPORTING REQUIREMENTS

Organizations subject to the BSA may be responsible for filing SARs and CTRs related to prepaid activity.<sup>11</sup> 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 below including a recommendation about MSBs and SAR filings.

### 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:

- Insider abuse involving any amount;
- Violations of federal law aggregating \$5,000 or more when a suspect can be identified;
- Violations of federal law aggregating \$25,000 or more regardless of a potential suspect; 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:

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

#### Potential Red Flags

- A customer with an excessive number of cards (based on program parameters)
- A customer who is unwilling to provide information required by the CIP
- A customer who presents unusual or suspicious identification documents that the financial institution cannot readily verify
- A customer who requests a shipment of cards 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

<sup>11</sup> If an organization is uncertain about its filing responsibilities, it should check with qualified legal counsel.

- Involves funds from illegal activities or is intended or conducted to hide or disguise illicit funds or assets as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under federal law;
- Is designed to evade any of the BSA regulations; or
- Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the institution knows of no reasonable explanation for the transaction after examining the available facts including the background and possible purpose of the transaction.

Under FinCEN regulations, MSBs involved in the issuance, sale, or redemption of stored value products are not currently required to file SARs. Since most Issuers of network branded prepaid cards are banks, MSBs and other third-party agents of an Issuer should coordinate decisions to file SARs with the Issuer of the prepaid card. 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

#### Information on Filing SARs

- A financial institution is required to file a SAR within 30 calendar days after the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect was identified on the date of detection of the incident requiring the filing, the financial institution can delay filing a SAR for an additional 30 calendar days to identify a suspect. However, that is the maximum length of time the financial institution may delay the reporting. In no case may reporting be delayed more than 60 calendar days after the date of initial detection of a reportable transaction. If no suspect can be identified by the end of the 60 days, a SAR must be filed without the identity information.
- The 30-day (or 60-day) period does not begin until an appropriate review is conducted and a determination is made that the transaction under review is “suspicious” within the meaning of the SAR regulations.
- 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 five years from the date of the filing of the SAR. Supporting documentation must also be identified and maintained by the institution and is deemed to have been filed with the SAR.
- 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.

bank nor an MSB under the laws and regulations.<sup>12</sup>

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 an inherently subjective judgment. 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.

### **Currency Transaction Reports**

Under 31 C.F.R. 103.22(b)(1), unless an exemption applies,<sup>13</sup> 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 within 15 days following the date of the transaction (25 days if the financial institution files electronically). The financial institution must retain a copy of each report filed for five years from the date of the report.

---

<sup>12</sup> The safe harbor protection extends to "agents" of a financial institution.

<sup>13</sup> The exemptions to filing CTRs are beyond the scope of this document.

## SECTION 4: KNOW YOUR CUSTOMER

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.

*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 B2B prepaid cards.*

### 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 recommend requiring compliance with the CIP rule requirements for consumer-funded prepaid card where the value load is \$1,000 or more - Card Brand rules vary on this requirement and, in many cases, set a lower limit
- Prohibiting reloads
- Prohibiting cash access
- Requiring a purchaser of an unusually large number of cards to provide CIP information as well as the rationale for the bulk purchase.

### Determining When CIP Applies

The CIP rules applicable to banks, savings associations, and credit unions are set forth at 31 C.F.R. 103.121.<sup>14</sup> In the CIP rules, the definition of "account" does not expressly address prepaid cards. The OTS, in its gift card guidance, concludes that gift cards are typically not subject to CIP requirements. OTS advises, however, that Issuers of open system reloadable prepaid cards should develop systems to apply CIP to those types of gift card products. These Recommended Practices take the position that non-reloadable prepaid cards (such as, but not limited to, gift, rewards, and rebate) do not create an account relationship between the financial institution and the Cardholder, so CIP requirements do not apply to Cardholders. However, in B2B transactions, discussed below, the business entity acquiring and funding non-reloadable prepaid cards for distributions to employees or customers should be subject to CIP requirements.

Notwithstanding the above, CIP should be considered based on an assessment of the risks presented by a prepaid card such as the amount of value involved, functionality, potential Cardholders, and card usage.

<sup>14</sup> The know your customer program requirements applicable to MSBs are set forth in 31 C.F.R. 103.125.

## **Risk-Based CIP**

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 documents, 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.

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. For prepaid card 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 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.

## **B2B Uses**

When a business entity seeks to purchase cards for distribution to customers and employees, and the business entity provides funding for the cards, the financial institution should follow its CIP and collect and verify relevant information regarding the business entity.<sup>15</sup>

---

<sup>15</sup> If anonymous cards are sold in a B2B relationship, the Issuer should consider implementing the controls set forth on page 24.

## SECTION 5: THIRD-PARTY AGENTS

Like many debit and credit card programs, prepaid card 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's scale advantage. There are many benefits to these arrangements including cost efficiencies and the advantages of doing business with organizations with specific expertise such as processing, distributing, selling, or storing prepaid card products.<sup>16</sup>

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

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 Distributor or Program Manager to market, distribute or support aspects of a prepaid card 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 contracts with a Processor to provide Core Processing Services for its card programs, the Issuer must ensure that the Processor implements adequate BSA/AML compliance programs and internal controls.
- Where a Program Manager contracts with a third-party Distributor to market, distribute, or support aspects of a prepaid card 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.
- Where a Program Manager contracts with a Processor to provide any Core Processing Services, the Program Manager must ensure, through contract requirements and initial and on-going due diligence procedures, that the Processor implements adequate BSA/AML compliance programs.

A review of the third parties should be conducted based on the financial institution's risk assessment of the third party 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; the level of review may be tiered accordingly. Reviews

---

<sup>16</sup> Examples of such programs include agent bank programs, employer-payroll card programs, merchant gift card programs, insurance company claims card programs, rebate company rebate card programs, and other programs involving third-party Processors, co-branding partners, activation and load service providers, and reload networks.

should be risk-based and, as appropriate, may consist of elements including, but not limited to, financial assessment and background and reference checks.

### **Due Diligence Review**

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

- A financial review of the third party 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 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 to conduct business with respect to prepaid card products;

#### **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 service providers

- Checks on all parties against the 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 programs.

## SECTION 6: INDEPENDENT COMPLIANCE TESTING

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.

*This section addresses the timing of independent testing and who may conduct independent testing if an external party cannot be used 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.*

### 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. 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 of Directors or to a designated board committee comprised primarily or completely of outside Directors.

### 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, and geographic locations);
- Appropriate 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;
- 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.

### **Documenting Independent Testing**

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 an review report and reported to the Board of Directors or a designated committee in a timely manner.

The Board of Directors or designated committee and the review staff should track review deficiencies and document corrective actions.

## SECTION 7: TRAINING APPROPRIATE PERSONNEL

Financial institutions must ensure that appropriate personnel, including members of the financial institution's Board of Directors, 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.*

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 of Directors 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

### **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. 103 — “Financial Recordkeeping and Reporting of Currency and Foreign Transactions” - Sets forth FinCEN regulations that promulgate the BSA. Relevant subsections are described below.

31 C.F.R. 103.11 — “Meaning of Terms” - Sets forth the definitions used throughout 31 C.F.R. Part 103.

31 C.F.R. 103.18 — “Reports by Banks of Suspicious Transactions” - Sets forth the requirements for banks to report suspicious transactions of \$5,000 or more.

31 C.F.R. 103.20 — “Reports by Money Services Businesses of Suspicious Transactions” - Sets forth the requirements for MSBs to report suspicious transactions of \$2,000 or more..

31 C.F.R. 103.22 — “Reports of Transactions in Currency” - Sets forth the requirements for financial institutions to report currency transactions in excess of \$10,000. Includes 31 C.F.R. 103.22(d) — “Transactions of Exempt Persons,” which sets forth the

requirements for financial institutions to exempt transactions of certain persons from currency transaction reporting requirements.

31 C.F.R. 103.23 — “Reports of Transportation of Currency or Monetary Instruments” - Sets forth the requirements for filing a Currency or Monetary Instruments Report.

31 C.F.R. 103.27 — “Filing of Reports” - Filing and recordkeeping requirements for Currency Transaction Reports (CTRs), Report of International Transportation of Currency or Monetary Instruments (CMIR), and Report of Foreign Bank and Financial Accounts (FBAR).

31 C.F.R. 103.28 — “Identification Required” - Sets forth the requirement that financial institutions verify the identity of persons conducting currency transactions in excess of \$10,000.

31 C.F.R. 103.29 — “Purchases of Bank Checks and Drafts, Cashier’s Checks, Money Orders, and Traveler’s Checks” - Sets forth the requirements that financial institutions maintain records relating to purchases of monetary instruments with currency in amounts between \$3,000 and \$10,000.

31 C.F.R. 103.33 — “Records to Be Made and Retained by Financial Institutions” - Sets forth recordkeeping and retrieval requirements for financial institutions, including funds transfer recordkeeping and transmittal requirements.

31 C.F.R. 103.34 — “Additional Records to Be Made and Retained by Banks” - Sets forth additional recordkeeping requirements for banks.

31 C.F.R. 103.38 — “Nature of Records and Retention Period” - Sets forth acceptable forms of records required to be kept and establishes a five-year record-retention requirement.

31 C.F.R. 103.41 — “Registration of Money Services Businesses” - Requirements for money services businesses to register with the U.S. Treasury/FinCEN.

31 C.F.R. 103.57 — “Civil Penalty” - Sets forth potential civil penalties for willful or negligent violations of 31 C.F.R. Part 103.

31 C.F.R. 103.59 — “Criminal Penalty” - Sets forth potential criminal penalties for willful violations of 31 C.F.R. Part 103.

31 C.F.R. 103.63 — “Structured Transactions” - Prohibits the structuring of transactions to avoid the currency reporting requirement.

31 C.F.R. 103.100 — “Information Sharing Between Federal Law Enforcement Agencies and Financial Institutions” - Establishes procedures and information sharing

between federal law enforcement and financial institutions to deter money laundering and terrorist activity.

31 C.F.R. 103.110 — “Voluntary Information Sharing Among Financial Institutions” – Establishes procedures for voluntary information sharing among financial institutions to deter money laundering and terrorist activity.

31 C.F.R. 103.120 — “Anti-Money Laundering Program Requirements for Financial Institutions Regulated by a Federal Functional Regulator or a Self-Regulatory Organization, and Casinos” - Establishes, in part, the standard that a financial institution regulated only by a federal functional regulator satisfies statutory requirements to establish an AML program if the financial institution complies with the regulations of its federal functional regulator governing such programs.

31 C.F.R. 103.121 — “Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks” - Sets forth the requirement for banks, savings associations, credit unions, and certain non-federally regulated banks to implement a written Customer Identification Program.

31 C.F.R. 103.125 — “Anti-Money Laundering Programs for Money Services Businesses”.

*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.

### *Office of Thrift Supervision*

12 C.F.R. 563.177 — “Procedures for Monitoring Bank Secrecy Act (BSA) Compliance” - Requires savings associations to implement a program to comply with the recordkeeping and reporting requirements in the BSA.

12 C.F.R. 563.180 — “Suspicious Activity Reports and Other Reports and Statements” - Sets forth the rules for savings associations or service corporations for filing a SAR with the appropriate federal law enforcement agencies and the U.S. Treasury.

### **Other Materials**

#### *Federal Financial Institutions Examination Council (FFIEC)*

The FFIEC’s web site ([www.ffiec.gov](http://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](http://www.treas.gov/press/releases/reports/js3077_01112005_MLTA.pdf))

*Financial Crimes Enforcement Network (FinCEN)*

FinCEN's web site ([www.fincen.gov](http://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](http://www.fatf-gafi.org)) includes the following publications:

- Forty Recommendations to Combat Money Laundering and Terrorism
- Special Recommendations Against Terrorist Financing
- Interpretive Notes to FATF Recommendations
- Non-Cooperative Countries or Territories
- Typologies on Money Laundering Risk • Trade Based Money Laundering
- New Payment Methods