

Prepaid Access - Overview

Objective. *Assess the adequacy of the bank’s systems to manage the risks associated with prepaid access products, and management’s ability to implement effective monitoring and reporting systems.*

Prepaid access is defined 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.²¹⁸

Banks often rely on multiple third parties to accomplish the design, implementation, and maintenance of their prepaid access programs. These third parties may include program managers, distributors, marketers, merchants, and processors. Some banks that offer prepaid access products do so as the issuing bank. In addition to issuing prepaid access, banks may participate in other aspects of a prepaid program such as marketing and distributing products issued by another financial institution. FinCEN regulations define certain non-bank providers and sellers of prepaid access as money services businesses (MSBs).

Prepaid access can be issued in an electronic or physical form and linked to funds held in a pooled account. Consumers use both electronic and physical prepaid products to access funds held by banks in pooled accounts that are linked to subaccounts.

The growth of prepaid access as a financial tool continues to flourish. While prepaid cards are the most well-known and popular products used by consumers at this time, prepaid access products are continuing to evolve. This section is intended to address prepaid card relationships as well as other types of prepaid access. Guidance on risk factors and risk mitigation for prepaid cards is based on current practice and is not intended to exclude other types of prepaid access.

Prepaid Cards

Prepaid access can cover a variety of products, functionalities, and technologies. Physical access, issued in the form of prepaid cards, is currently the most popular form and is widely used for payments by governments, businesses and consumers. Most payment networks require that their branded prepaid cards be issued by a bank that is a member of that payment network. Prepaid cards operate within either an “open” or “closed” loop system. Open loop prepaid cards can be used for purchases at any merchant that accepts cards issued for use on the payment network associated with the card and to access cash at any automated teller machine (ATM) that connects to the affiliated ATM network. Examples of open loop prepaid cards include payroll cards, general purpose reloadable (GPR) cards, and certain gift cards. Some prepaid cards may be reloaded, allowing the cardholder or other person (such as an employer) to add value. Closed loop prepaid cards generally can only be used to buy goods or services from the merchant issuing the card or a select group of merchants or service providers that participate in a specific network. Examples of closed loop prepaid cards include merchant-specific retail gift cards, mall cards, and mass transit system cards.

²¹⁸ 31 CFR 1010.100(ww).

Closed loop prepaid cards generally do not allow for cash access, although they can often be resold through third-party Web sites in exchange for other closed loop cards or payment via check, ACH or other method.

Prepaid cards are highly flexible and can be customized to meet the needs of the specific program. Some prepaid card programs are designed for specific limited-use purposes, such as flexible spending account (FSA) or health savings account (HSA) cards that can be used to purchase specific health-related services. Some prepaid card programs are used by state and federal government agencies to disburse government benefits (e.g., disability, unemployment, etc.) or provide income tax refunds, or by employers to deliver wage and salary payments.

Like debit cards, prepaid cards provide a compact and transportable way to maintain and access funds. Consumers use prepaid cards in a variety of ways, such as purchasing products, making transfers to other cardholders within the prepaid program, and paying bills. They also offer individuals an alternative to cash and money orders. As an alternate method of cross-border funds transmittal, a small number of prepaid card programs may issue multiple cards per account, so that persons in another country or jurisdiction can access the funds loaded by the original cardholder via ATM withdrawals of cash or merchant purchases. For such programs, risk-based customer due diligence should be conducted on the original cardholder and transactions should be subjected to risk-based monitoring.

Prepaid Access Participants

Prepaid access programs often rely on multiple third parties to accomplish the design, implementation, and maintenance of their programs. Within a prepaid access program, these parties are known by the following terms:

- **Program Manager.** Runs the program's day-to-day operations. This entity may or may not also be the entity that creates the program and designs the features and characteristics of the prepaid product. May be a provider of prepaid access (Money Services Business (MSB)) under FinCEN's rule.²¹⁹
- **Network.** Any of the payment networks that clear, settle, and process transactions.
- **Distributor.** An organization that markets and distributes prepaid products.
- **Provider of Prepaid Access.** A participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow program participants. The provider must register with FinCEN as an MSB and identify each prepaid program for which it is the provider of prepaid access. As an MSB, providers of prepaid access are subject to certain BSA/AML responsibilities. A bank that serves as a provider of prepaid access has no requirement to register with FinCEN.
- **Payment Processor.** The entity that tracks and manages transactions and may be responsible for account set-up and activation; adding value to products; and fraud control and reporting.

²¹⁹ 31 CFR 1010.100(ff)(4)(i)

- **Issuing Bank.** A bank that offers network branded prepaid products to consumers and may serve as the holder of funds that have been prepaid and are awaiting instructions to be disbursed.
- **Seller or Retailer.** A convenience store, drugstore, supermarket, or location where a consumer can buy a prepaid product.

Contractual Agreements

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 an agreement or a contract describing each party's responsibilities and other relationship details, such as the products and services provided. The agreement or contract should also consider each party's BSA/AML and OFAC compliance requirements, customer base, due diligence procedures, and any payment network obligations. The issuing bank maintains ultimate responsibility for BSA/AML compliance whether or not a contractual agreement has been established.

Risk Factors

As with other payment instruments, money laundering, terrorist financing, and other criminal activity may occur through prepaid access and prepaid card programs if effective controls are not in place. For example, law enforcement investigations have found that some prepaid holders have used false identification and funded their initial loads with stolen credit cards, or have purchased multiple prepaid cards under aliases. In the placement phase of money laundering, because many domestic and offshore banks offer prepaid access products or services with currency access through ATMs internationally, criminals may load cash from illicit sources onto prepaid access products and send them to accomplices inside or outside the United States. Generally, domestically issued prepaid cards can only be loaded in the United States. Investigations have disclosed that both open and closed loop prepaid cards have been used in conjunction with, or as a replacement to, bulk cash smuggling. Although prepaid access is increasingly regulated and is issued by highly regulated banks, some third parties involved in marketing or distributing prepaid access programs may or may not be subject to regulatory requirements, oversight, and supervision. In addition, these requirements may vary by party.

Prepaid access programs are extremely diverse in the range of products and services offered and the customer bases they serve. In evaluating the risk profile of a prepaid access program, banks should consider the program's specific features and functionalities. Higher potential money laundering risk associated with prepaid access would result if the holder is anonymous, or if the holder or purchaser provides fictitious holder/purchaser information. Higher risk is also associated with cash access (especially internationally), and the volume and velocity of funds that can be loaded or transacted. Other risk factors include type and frequency of loads and transactions, geographic location where the transaction activity occurs, the relationships between the bank and parties associated with the program, value limits, distribution channels, and the nature of funding sources. Transactions using prepaid access may pose the following unique risks to the bank:

- Funds may be transferred to or from an unknown third party.

- Verification of cardholder identity may be done entirely remotely, relying on third-party program managers, processors or distributors.
- As with other modes of electronic payments (e.g., ACH, wire transfer, credit and debit cards), holders may be able to use prepaid access products internationally, thus avoiding border restrictions and reporting requirements applicable to cash and monetary instruments.
- Transactions may be credited or debited to the user's payment product immediately, although there may be a lag in delivery of funds to the issuing bank, creating a load timing risk for the bank (also referred to as a "funds in flight" risk).
- Specific holder activity may be difficult to determine by reviewing activity through a pooled account.
- Data in underlying pooled accounts may be held or managed by third parties, separate from the issuing bank.
- Marketing of payment products, customer service, and onboarding of new customers (both consumer and business customers) may be handled primarily by third parties separate from the issuing bank.
- The customer may perceive the transactions as less transparent.
- Source of payroll funding may come through an intermediary bank and may not be transparent.

Risk Mitigation

Banks that offer prepaid access or otherwise participate in prepaid access programs should have policies, procedures, and processes sufficient to manage the related BSA/AML risks as required under the BSA and implementing regulations, as well as under payment network rules. Guidance provided by the Network Branded Prepaid Card Association is an additional resource for banks that provide prepaid card services.²²⁰

BSA/AML risk mitigation is an important factor for prepaid access programs, involving several key components:

- Conducting appropriate due diligence on any third-party service provider.
- Conducting a risk assessment of the prepaid access product itself including product features and how it is distributed and loaded.
- Monitoring transactions conducted or attempted by, at or through the bank for unusual or suspicious activity.
- Product features and limits on usage.

²²⁰ Refer to "[Recommended Practices for Anti-Money Laundering Compliance for U.S.-Based Prepaid Card Programs](#)," February 28, 2008.

Third-Party Service Providers

A bank's Customer Due Diligence (CDD) program should provide for a risk assessment of all third parties involved in offering, managing, distributing, processing, or otherwise implementing the prepaid access program, considering all relevant factors, including, as appropriate:

- A review of such party's BSA/AML compliance program.
- Systems integrity and BSA/AML monitoring capabilities.
- The policies on outsourcing should include processes for (1) documenting in writing the roles and responsibilities of the parties, (2) maintaining the confidentiality of customer information, and (3) maintaining the necessary access to information. The policies should include the right to audit the third party to monitor its performance.
- The BSA/AML and OFAC obligations of third parties.
- On-site audits.
- Corporate documentation, licenses, references (including independent reporting services), and, if appropriate, documentation on principal owners.
- An understanding of the third party's overall compliance culture.

Product Features and Distribution

Product features can provide important mitigation to the BSA/AML risks inherent in prepaid access and prepaid card relationships and transactions and may include:

- Limits or prohibitions on cash loads, access, or redemption, particularly where holder information is not on file.
- Limits or prohibitions on amounts of loads and number of loads/reloads within a specific time frame (load velocity limits).
- Controls on the number of cards purchased by one individual or the number of cards that can access the same card account.
- Controls on the ability to transfer or co-mingle funds.
- Maximum dollar thresholds on ATM withdrawals and on the number of withdrawals within a specific time frame (ATM velocity limits).
- Maximum dollar thresholds on Point of Sale (POS) transactions for individuals and transactions within a preset time period (i.e., daily or monthly); and on the number of withdrawals within a specific time frame (POS velocity limits).
- Limits or prohibitions on certain usage (e.g., merchant type) and on geographic usage, such as outside the United States.
- The ability to reverse transactions.

- Limits on aggregate card values.

Other features that mitigate risks in this area include:

- The identity and location of all third parties involved in selling or distributing the prepaid access program, including any subagents.
- The type, purpose, and anticipated activity of the prepaid access program.

Customers/Prepaid Users

Customer due diligence regarding the purchaser and/or the user(s) of the prepaid product can also be important BSA/AML risk mitigant and may include:

- Whether the source of funds is known and trusted (such as corporate or government loads, vs. loads by individuals).
- The nature of the third parties' businesses and the markets and customer bases served.
- The information collected to identify and verify the holders' identity.
- The nature and duration of the bank's relationship with third parties who are the source of funds in the prepaid access program.
- The company requesting payroll funding and the source of payroll funding.
- The ability to monitor and track loads, transactions and velocity.

As part of their system of internal controls, banks should establish a means for monitoring, identifying, and reporting suspicious activity related to prepaid access programs. This reporting obligation extends to all transactions by, at, or through the bank, including those in an aggregated form. Banks may need to establish protocols to regularly obtain transaction information from processors or other third parties. Monitoring systems should have the ability to identify foreign activity, bulk purchases made by one individual, and multiple purchases made by related parties. In addition, procedures should include monitoring for unusual activity patterns, such as:

- cash loads followed immediately by withdrawals of the full amount from another location, or
- multiple unrelated funds transfers onto the prepaid access product, such as in tax refund fraud situations where multiple tax refunds are loaded onto one card.

Various management information system reports (MIS) may be useful for detecting unusual activity on higher-risk accounts. Those reports include ATM activity reports (focusing on foreign transactions), funds transfer reports, new account activity reports, change of Internet address reports, Internet Protocol (IP) address reports, and reports to identify related or linked accounts (e.g., common addresses, phone numbers, e-mail addresses, and taxpayer identification numbers).