Board of Governors of the Federal Reserve
Federal Deposit Insurance Corporation
National Credit Union Administration
Office of the Comptroller of the Currency
Financial Crimes Enforcement Network

Interagency Guidance to Issuing Banks on Applying Customer Identification Program Requirements to Holders of Prepaid Cards

March 21, 2016

The Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) (collectively, the Agencies), are publishing this guidance to issuing banks[1] on the application of the joint regulations implementing the customer identification program (CIP) requirements set forth in Section 326 of the USA PATRIOT Act[2] (referred to in this guidance as the "CIP rule")[3] to their prepaid cards. Prepaid cards include those that are sold and distributed by third-party program managers, [4] as well as cards that are used to provide employee wages, healthcare, and government benefits. The guidance clarifies that a bank should apply its CIP to the cardholders of certain prepaid cards issued by the bank.[5]

[1] The term "issuing bank" used in this guidance means the bank that authorizes use of the prepaid card. Usually the issuing bank is the bank that has its name printed on the back of a prepaid card. A bank includes any commercial bank, savings association, or credit union, and branch of a foreign bank. See 31 CFR 1010.100(d).

[2] 31 USC 5318(l).

[3] 68 *Federal Register* (FR) 25090 (May 9, 2003) codified at 31 CFR 1020.220 (Treasury); 12 CFR 21.21 (OCC); 12 CFR 208.62(b)(2) and 211.24(j)(2) (FRB); 12 CFR 326 (FDIC); and 12 CFR 748.2 (NCUA).

[4] For purposes of this guidance, a third-party program manager is a company that designs, manages and operates a prepaid card program and contracts with a bank to issue prepaid cards under the program and to process transactions conducted using those cards. The third-party program manager also provides customer service and card distribution (sales). The third-party program manager may also be a "provider of prepaid access" under FinCEN's rule. See 31 CFR 1010.100(ff)(4). However, an issuing bank's responsibilities described in this guidance are separate from any Bank Secrecy Act requirements that are otherwise applicable to third-party program managers, or any other party in the prepaid payment chain.

[5] This guidance specifically refers to prepaid cards, but also is applicable to other prepaid access products, that meet the criteria described in this guidance. Such examples include certain prepaid access products offered through mobile phones or Internet sites that are used to access funds.

I. Introduction

Prepaid cards have become mainstream financial products, widely used by individuals, corporations, and other private sector entities, as well as state, federal and local governments.[6] General purpose prepaid cards can be used at multiple, unaffiliated merchants and can allow cardholders to perform a variety of functions, including those that have traditionally been conducted using other payment mechanisms, such as checks, debit cards tied to bank accounts, or credit cards.[7] These functions include withdrawing cash at automated teller machines (ATMs), paying bills, purchasing goods and services, and transferring funds to other cardholders and receiving funds transfers. Employers use prepaid cards to provide wages and other compensation or benefits, such as pre-tax flexible spending arrangements for healthcare expenses or dependent care. State, federal, and local governments use these financial products to distribute government benefits and tax refunds.

Prepaid cards can be purchased online and from a variety of physical locations, such as local bank branches, retail stores and supermarkets. A growing number of third-party program managers are selling prepaid cards online and at physical locations, in addition to managing prepaid card programs, processing transactions, and providing customer support.

Functionalities that make prepaid cards attractive to consumers also pose risks for banks that issue prepaid cards and process prepaid card transactions. For example, easy access to prepaid cards, the ability to use them anonymously, and the potential for relatively high volumes of funds to flow through pooled prepaid access accounts, make prepaid cards potentially vulnerable to criminal abuse.

The Agencies have made clear that the money laundering and other financial crime risks faced by banks that issue prepaid cards and process prepaid card transactions require the implementation of strong and effective mitigating controls.[8] Controls put in place by issuing banks and the prepaid card industry, such as limits on card value and the frequency and amount of transfers, as well as appropriate due diligence on third parties and cardholders, have helped mitigate these risks. However, questions have arisen regarding the application of the CIP rule to prepaid cards issued by banks, including with respect to prepaid cards issued by banks under arrangements with third-party program managers.

---

[6] For further information, see the 2013 Federal Reserve Payments Study, available at https://www.frbservices.org/files/communications/pdf/research/2013_payments_study_summary.pdf.and the 2013 FDIC National Survey of Unbanked and Underbanked Households, available at https://www.fdic.gov/householdsurvey/. The survey noted a year over year increase in the use of prepaid cards with transactions focused largely on bill payment.

[7] By contrast, closed-loop prepaid cards, which are redeemable only at a single merchant or service provider, or a group of affiliated merchants or service providers, are generally not issued by banks and do not establish relationships that resemble formal banking relationships. Cardholders of closed-loop prepaid cards may only use the prepaid card to purchase goods or services from the merchant or service provider to which the cardholder or a third party has provided funds to load or reload the card.

[8] See the *FFIEC BSA/AML Examination Manual*, "Prepaid Access–Overview" (2014), p. 227, available at http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_061.htm.

II. CIP Rule Overview

In 2003, the Agencies issued the CIP rule that requires a bank to obtain information sufficient to form a reasonable belief regarding the identity of each "customer" opening a new "account."[9] The bank's CIP must include risk-based procedures for verifying its customers' identities to the extent reasonable and practicable. In particular, the CIP rule requires banks to implement a CIP that includes certain minimum requirements. First, a bank's CIP must include procedures for opening an account that, at a minimum, must include obtaining a name, date of birth, address, and identification number from a customer who is an individual.[10] Second, a bank's CIP must also include identity verification procedures that describe when and how the bank will verify the customer's identity using documentary or non-documentary methods.[11] Finally, the CIP rule has specific account recordkeeping and notice requirements.[12]

This guidance clarifies that certain prepaid cards issued by a bank should be subject to the bank's CIP, including when a bank issues prepaid cards under arrangements with third-party program managers that sell, distribute, promote, or market the prepaid cards issued by the bank. This may be the only relationship that the cardholder has with the bank.

In order to determine if CIP requirements apply to purchasers of prepaid cards, the bank should first determine whether the issuance of a prepaid card to a purchaser results in the creation of an account; and if so, ascertain the identity of the bank's customer. As discussed below, these determinations depend on the functionalities of the prepaid card issued.

III. Determining the Existence of an 'Account'

An "account" is defined in the CIP rule as "a formal banking relationship established to provide or engage in services, dealings, or other financial transactions, including a deposit account, a transaction or asset account, a credit account or other extension of credit." An account also includes "a relationship established to provide a safety deposit box or other safekeeping services or to provide cash management, custodian, or trust services."[13] An account does not include "products and services for which a formal banking relationship is not generally established with a person, such as check cashing, wire transfer, or the sale of a check or money order." For CIP purposes, an account does not include any account that the bank acquires, or accounts opened, to participate in an employee benefit plan established under the Employee Retirement Income Security Act of 1974.[14]

---

[9] 31 CFR 1020.100(c), (a).

[10] 31 CFR 1020.220(a)(2)(i).

[11] 31 CFR 1020.220(a)(2)(ii).

[12] 31 CFR 1020.220(a)(3) and (a)(5).

[13] 31 CFR 1020.100 (a)(1).

[14] 31 CFR 1020.100(a)(2).

Certain prepaid cards exhibit characteristics that are analogous to deposit accounts, such as checking or other types of transactional accounts.[15] Some of these cards are linked to, and permit use of, funds held by a bank, even though the funds may be managed by, or distributed through, a third-party program manager.[16] As described below, for purposes of the CIP rule, prepaid cards that provide a cardholder with (1) the ability to reload funds or (2) access to credit or overdraft features should be treated as accounts.

a. General Purpose Prepaid Cards With the Ability to Reload Funds

General purpose prepaid cards may be reloaded by the cardholder or another party on behalf of the cardholder in a manner that is similar to the way in which funds can be added to a traditional deposit, asset, or transaction account. Therefore, the Agencies believe that issuing a general purpose prepaid card with those features creates a formal banking relationship and is equivalent to opening an account for purposes of the CIP rule.

By contrast, the issuance of a general purpose prepaid card that, under the program's terms, cannot be reloaded by a cardholder or another party on behalf of the cardholder, does not establish an account for CIP purposes. These cards do not bear the characteristics of a typical deposit, transaction, or asset account because they do not permit the cardholder or other party on behalf of the cardholder to reload funds. Therefore, the Agencies believe these cards do not create a formal banking relationship.

b. General Purpose Prepaid Cards With Access to Credit or Overdraft Features

General purpose prepaid cards may permit withdrawals in excess of the card balance and also may provide the cardholder with access to an overdraft line or an established line of credit similar to a lender/borrower or credit card relationship. The Agencies believe that a card that permits either functionality constitutes a formal banking relationship with the issuing bank and is an account for purposes of the CIP rule.

c. Activation of General Purpose Cards

In some cases, general purpose prepaid cards may be sold without the reloadable functionalities activated or credit or overdraft features enabled. A purchaser or subsequent transferee of these cards generally may activate any one of those features only if they contact the issuing bank or the

---

[15] General purpose prepaid cards may include features that permit the cardholder to make and receive payments or transfers by non-card means, such as by Automated Clearing House (ACH) , wire, check, or mobile phone message, activities that are also conducted through an account. For example, a cardholder may be able to pay a bill by logging on to the issuing bank's Web site and initiating an ACH payment to the biller. A cardholder also may be permitted to make and receive payments using a prepaid card, such as through a cardholder-to-cardholder transfer, a transfer to the cardholder's savings account, or a transfer to another person's transaction account at the issuing bank. If these features could result in the reloading of the general purpose prepaid card, then the card should be treated as an "account."

[16] Generally, credit unions may only serve individuals and entities within their approved field of membership. Therefore, the threshold question for any credit union contemplating entering into an account relationship involving holders of prepaid cards sold and distributed by third parties is whether the customer with whom it intends to establish the relationship is within the field of membership it is authorized to serve.

third-party program manager. In such cases, for purposes of the CIP rule, the Agencies believe that an account is not established until a reload, credit, or overdraft feature is activated by cardholder registration.

IV. Identifying the Customer

Once an account has been established, the bank must identify the customer for purposes of the CIP rule. Under the CIP rule, a person that opens a new account is deemed a customer.[17] To verify the identity of the person opening the account, the final CIP rule's preamble explains that a bank need only verify the identity of the named accountholder.[18] The following describes how these principles should apply to different types of prepaid cards.

a. Prepaid Cardholders and Third Parties

When a general purpose prepaid card issued by a bank allows the cardholder to conduct transactions evidencing a formal banking relationship, such as by adding monetary value or accessing credit, the cardholder should be considered to have established an account with the bank for purposes of the CIP rule. Further, the cardholder should be treated as the bank's customer for purposes of the CIP rule, even if the cardholder is not the named accountholder, but has obtained the card from an intermediary who uses a pooled account with the bank to fund bank-issued cards.

As a general matter, third-party program managers should be treated as agents of the bank for purposes of the CIP rule, rather than as the bank's customer. The preamble to the final CIP rule makes clear that the rule does not affect a bank's authority to contract for services to be performed by a third party either on or off the bank's premises, nor does it alter a bank's authority to use an agent to perform services on its behalf. However, as with any other activity performed on behalf of the bank, the bank ultimately is responsible for compliance with the requirements of the bank's CIP rule as performed by that agent or other contracted third party.[19]

Third-party program managers may establish pooled accounts in their names for the purpose of holding funds "on behalf of" or "in trust for" cardholders or processing transactions on behalf of other issuing banks. However, the fact that these funds are held in a pooled account should not affect the status of the cardholder as a bank customer, assuming the cardholder has established an account with the bank by activating the reloadable functionalities of a general purpose prepaid card, or its credit or overdraft features.

In the case of non-reloadable general purpose prepaid cards without credit or overdraft features, or other prepaid cards that do not have the identified features that establish an account for purposes of the CIP rule, such as closed-loop prepaid cards, the third-party program manager in

---

[17] 31 CFR 1020.100(c)(1)(i).

[18] 68 FR 25090, 25094 (May 9, 2003).

[19] See 68 FR 25090, 25104 (May 9, 2003). See also *Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act*, FAQs Final CIP Rule (April 28, 2005), at p. 5, available at http://www.fincen.gov/statutes_regs/guidance/pdf/faqsfinalciprule.pdf.

whose name the pooled account has been established should be considered to be the only customer of the issuing bank and should be subject to requirements of the bank's CIP policies and procedures. In these cases, the issuing bank need not "look through" the pooled account to verify the identity of each cardholder.

i. ***Payroll Cards***

Payroll cards are cards that enable an employee to access funds in accounts that are established directly or indirectly by an employer and to which the employer (or a third party acting on the employer's behalf) is able to transfer the employee's wages, salary, bonuses, travel reimbursements, or other compensation. Typically, the employer (or the employer's agent) opens an account with a bank and provides each of its employees with a card that can be used to access the employee's share of the account. The employer (or the employer's agent) then transfers the employee's wages, salaries, or other compensation into the account or subaccount, rather than distributing a check to the employee.

If the employer (or the employer's agent) is the only person that may deposit funds into the payroll card account, the employer should be considered the bank's customer for purposes of the CIP rule. In that case, the bank need not apply its CIP to each employee. The employer should be considered to be the customer even if there are subaccounts that are attributable to each employee. By contrast, if the employee is permitted to access credit through the card, or reload the payroll card account from sources other than the employer, the employee should be the customer of the bank and the bank should apply its CIP to the employee.

ii. ***Government Benefit Cards***

Government benefit cards (also referred to as Electronic Benefit Transfer Cards) are cards issued under government benefit programs to distribute government benefits or other payments. Government benefit programs vary as to whether beneficiary-cardholders are permitted to load funds unconnected to the government benefit program onto the card, and whether they provide access to credit. If the government benefits card program permits only government funds to be loaded onto the card and does not provide access to credit, no customer relationship is established between the bank and the beneficiary-cardholder for purposes of the CIP rule. In addition, since the term "customer" does not include a department or agency of the United States, of any state, or any political subdivision of any state, a bank that issues such a government benefit card is not required to apply its CIP to the government agency establishing the benefit card account. If, however, the card allows non-government funds to be loaded onto the card or provides access to credit, then a customer relationship is established between the bank and the beneficiary-cardholder and the bank should collect CIP information from the beneficiary-cardholder.

iii. ***Health Benefit Cards***

Prepaid cards can also be used to access funds in a Health Savings Account (HSA), or accounts established as part of a Flexible Spending Arrangement (FSA) or Health Reimbursement Arrangement (HRA). While HSAs, FSAs, and HRAs are all used to set aside tax-exempt funds

for certain medical expenses, these arrangements may differ with respect to who may establish the account, deposit funds into the account, or access funds in the account. Therefore, the person or entity that should be considered to be the issuing bank's customer for CIP purposes will differ.

> **Health Savings Accounts** are accounts established by an employee to pay or obtain reimbursement for qualifying medical expenses. Such reimbursement may be issued on a prepaid card. The employee establishing the account or the employer may contribute to the HSA. Because the employee establishes the account, the employee is the issuing bank's customer for purposes of the CIP rule.
>
> **Flexible Spending Arrangements and Health Reimbursement Arrangements** are established by an employer and funded by either voluntary withholdings from an employee's salary (in the case of FSAs only) or through direct employer contributions (in the case of FSAs and HRAs). The employee may use a debit card, credit card, or prepaid card for certain qualified medical expenses. Because no person other than the employer (or employer's agent) establishes an FSA or HRA, makes deposits into the FSA or HRA, and distributes funds from the FSA or HRA, the employer should be the issuing bank's customer for purposes of the CIP rule.

V. Contracts with Third-Party Program Managers

The issuing bank should enter into well-constructed, enforceable contracts with third-party program managers that clearly define the expectations, duties, rights, and obligations of each party in a manner consistent with this guidance.[20] For example, a binding contract or agreement should, at a minimum:

a. outline CIP obligations of the parties;

b. ensure the right of the issuing bank to transfer, store, or otherwise obtain immediate access to all CIP information collected by the third-party program manager on cardholders;

c. provide for the issuing bank's right to audit the third-party program manager and to monitor its performance (generally, banks need to ensure that periodic independent internal and external audits are conducted to ensure prudent operations and compliance with applicable laws and regulations); and

d. if applicable, indicate that, pursuant to the Bank Service Company Act (BSCA) or other appropriate legal authority, the relevant regulatory body has the right to examine the third-party program manager.[21]

---

[20] For further information, see *FFIEC Information Technology Examination Handbook*, "Outsourcing Technology Booklet," available at http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx. Other guidance issued by the Agencies may also be applicable.

[21] For example see, OCC Bulletin 2011-27, "Pre-Paid Access Programs: Risk Management Guidance and Sound Practices" (June 28, 2011). The BSCA does not confer authority to the NCUA. However, federally insured credit unions may refer to Letter to Credit Unions 07-CU-13 and associated enclosures for relevant guidance in addition to the *FFIEC Information Technology Examination Handbook*.