

A guide for law enforcement and financial institutions:

# AML and risk challenges facing financial institutions issuing prepaid cards



*Editor's note:*

*This is part one of a two part series.*

Whether used to provide cost-effective substitutes to traditional paper payments, such as government benefits, rebates and flexible savings accounts, or to provide a financial product to the under-banked or un-banked community, the prepaid card industry is rapidly growing both in the United States and internationally. According to research commissioned by MasterCard, Inc. and conducted by the Boston Consulting Group (BCG), the total value of the branded prepaid card opportunity in the U.S. is expected to surpass \$440 billion by 2017, nearly quadrupling its estimated value of \$120.2 billion in 2009. The study also shows the U.S. market will remain the largest branded prepaid segment in the world, holding 53 percent of the overall market share. India, the UK, Mexico, Italy, the Middle East and Brazil combined, will hold approximately 25 percent of the branded prepaid market by 2017. Brazil alone is expected to expand from \$1.7 billion in 2009 to more than \$17 billion in 2017.<sup>1</sup>

While most may be familiar with the prepaid card products that exist including gift, payroll and general purpose reloadable cards, do you have a good understanding what AML and risk controls financial institutions put into place before issuing or selling prepaid cards? The first part of this two-part series will address AML and risk considerations specifically for issuing financial institutions, followed by the second part which will focus on considerations for those companies wishing to market and sell prepaid card products. An examination of these subject areas provides law enforcement with a knowledge base for present and future investigations pertaining to prepaid cards.

At the end of the day,  
the issuer of the prepaid  
card is completely  
responsible for AML  
compliance on its products

For the most part, only financial institutions can be members of the card associations, meaning all prepaid cards are issued by a financial institution. If you look on the back of a prepaid card you will see the issuer statement. There are two routes financial institutions can take to issuing prepaid cards: (1) develop and issue a prepaid card program to market and sell directly to consumers themselves, or (2) assist third parties in developing prepaid card programs whereby the financial institution is the issuer but the third party is responsible to market and sell to consumers. This is typically referred to as a sponsorship model and is the model preferred by most financial institutions today. The third party is usually referred to as a "program manager" and the financial institution as the "issuer."

Financial institutions delving into the prepaid sponsorship industry, or indeed sponsorship of any bank products including credit cards and other lending products, need to place special emphasis on risk management of their third parties. In the past, "rent-a-charter" situations were troublesome to regulators and even though the industry has put substan-

tial controls in place to avoid this situation, regulators are again taking a hard look at financial institutions' third party risk management practices. In addition to contractual, operational and financial risk considerations, the issuer must consider its AML compliance obligations. At the end of the day, the issuer of the prepaid card is completely responsible for AML compliance on its products the same as any other bank product or service offered. The following are some specific considerations for financial institutions looking to issue prepaid cards.

#### Program manager due diligence

While the issuer is not offering a traditional commercial checking account to the program manager, it is providing access to financial products. The issuer should apply the same, if not more, customer identification program (CIP) and enhanced due diligence (EDD) standards to program managers as would apply to a traditional commercial account. This includes having complete information on the company and ownership structure, including background checks on the company itself and its beneficial owners. Financial statements, data security and disaster recovery policies are also recommended. A good third-party risk program will include a process for risk rating third parties, as well as standards for risk-based monitoring and periodic review of third party relationships. Refer to the regulatory agencies' web sites for further guidance on third party risk management.

#### AML and OFAC risk assessments

The issuer's enterprise-wide AML and OFAC Risk Assessments should encompass issuance of prepaid cards. Not only should the risk assessment include evaluation of the product, customer and geographic risks associated with the new business line, it should

<sup>1</sup>Payment News (2010), MasterCard Releases Prepaid Market Sizing Report, 12 July 2010, [www.paymentsnews.com/2010/07/mastercard-releases-prepaid-market-sizing-report.html](http://www.paymentsnews.com/2010/07/mastercard-releases-prepaid-market-sizing-report.html)

also include assessment of the risks associated with offering the products through third parties. The April 2010 FFIEC BSA/AML Examination Manual provides a good outline of the risk mitigation factors to consider.

### AML policy

In addition to ensuring that its enterprise-wide AML Program covers issuance of prepaid, the issuer should also have documented AML requirements to which its program managers are contractually required to comply. These requirements should include the issuer's expectations for the program manager's AML policy, four pillars and specific requirements for CIP, transaction monitoring, reporting, and OFAC. Depending on the program manager's other business lines, program manager's may or may not be required to have their own AML policy to address applicable AML regulations. In those cases, the sale of prepaid cards and the issuer's requirements should be added to program manager's existing AML policy.

### AML officer

Each program manager should have a designated AML officer. Depending on the size of the company, the officer may hold multiple positions, including but not limited to legal, fraud, risk, finance or operations. In all cases, the program manager's AML officer should have the resources needed to fulfill their responsibilities; however, the AML officer may have limited AML experience depending on the program manager's other business lines. In those cases, it is beneficial if the issuer can provide additional training. Offering the program manager industry training solutions, such as those provided by the Network Branded Prepaid Card Association (NBPCA)<sup>2</sup> or ACAMS, can be beneficial for everyone.

### AML training and retail agents

Program managers should be required to attend initial and annual training on the issuer's AML requirements. The program manager should also be required to provide AML training to their applicable staff and any retail agents. If the program manager is using retail agents to sell or reload prepaid cards, it is crucial for the issuer

Each program manager should have a designated AML officer

to ensure that the retail agent is provided with AML training for sale of its products. How to deliver this training should be a risk-based decision; however, it is recommended the issuer provide direct training to the retail agent when possible, versus using a train the trainer method whereby the program manager delivers the training. The issuer should also have a contractual agreement with each retail agent selling its prepaid cards.

### Independent testing

The issuer should ensure their annual independent audit includes testing of their prepaid card programs and controls. The issuer should also consider applying risk-based requirements for independent testing of its program managers. Independent testing is crucial for the issuer to show their regulator that they are providing appropriate oversight of the program manager, and it can also be used as a performance measurement for the issuer to evaluate the program manager's compliance. In the case of higher-risk program managers, the issuer may require the program manager to obtain an external independent review of their AML program and its adherence to the issuer's requirements. In lower-risk cases, the issuer may opt to do its own review of the program manager's AML program; however the adequacy of this review may be questioned due to the issuer's involvement in setting the standards. One way to solve this is for the

issuer to maintain separate areas or departments, one to develop and train on the AML requirements and one to perform independent testing for compliance.

### Customer Identification Program

One of the most important AML considerations for an issuer is determining how best to apply its Customer Identification Program (CIP). As a regulated financial institution, the issuer's CIP requirements for prepaid cards should be similar to its CIP requirements for traditional deposit products. In most cases, however, CIP on prepaid cardholders is performed in a non-face-to-face environment due to the online nature of the product or data security constraints at retail. Since many program managers will be using non-documentary verification methods such as public database checks, the issuer should consider selecting and approving a few vendors that meet its CIP criteria and work with those vendors to develop a compliant CIP decision model for the program managers to utilize. If the issuer is not involved in approving the verification method, its CIP testing will need to be increased to ensure that program manager compliance. The issuer should also provide the program manager with its requirements for documentary verification, e.g., what documents are acceptable under its CIP. In the case of payroll card programs, the program manager may also request approval to allow the employer to perform CIP verification. The issuer needs to set and provide standards for any third party reliance as well. However the issuer decides to handle CIP, it is crucial to establish a testing process to evaluate the program manager's compliance with the issuer's CIP. Issuers should consider continued exceptions and failure to comply with CIP requirements as a reason for contract termination.

### Currency transaction monitoring and reporting

Cash deposits, or "value-loads," are rarely accepted by either the issuer or the program manager. If cash value loads are accepted, it is usually through a third party "load network," which carries the appropriate money transmission licensing, as well as the

<sup>2</sup>The NBPCA is a trade association open to all companies involved in providing prepaid cards that carry a brand network logo and offers educational resources to both members and non-members. [www.nbpca.org](http://www.nbpca.org).

responsibility to aggregate and report cash transactions. In addition, prepaid card attributes are prohibitive of reportable transactions, as most value loads and withdrawals are limited at \$2,500 per transaction. However, issuers still need to consider the ability to aggregate cash activity between multiple cardholders. Does the issuer obtain the transactional records? If so, how can the issuer aggregate activity if one cardholder has a card with program manager A and another card with program manager B? These aggregation issues remain a challenge for the prepaid card industry.

### Suspicious activity monitoring, reporting and law enforcement needs

Suspicious activity monitoring can be handled one of two ways, depending on the amount of data the issuer receives on its cardholders. If the issuer receives all cardholder information including transactional data, typically referred to as “flat files,” it can monitor activity within its organization. The issuer may use a fraud or AML tool provided by a card association, an internally built system and risk-based rules, or an outside vendor solution. However, few vendor solutions currently available for AML monitoring adequately address the unique characteristics of prepaid card programs. It can also be difficult to justify the cost of a vendor solution when prepaid revenue can be pennies per transaction.

If the issuer is not receiving flat file information, or transactional data, it must provide its program managers with suspicious activity monitoring requirements. Issuers should consider monitoring for such things as multiple cards, cash value loads followed by cash withdrawals, merchant credits without corresponding debits, multiple transfers to and from accounts, deposits in names other than the cardholder and above average value loads. The issuer should also periodically test the program manager’s compliance with the monitoring requirements.

As the regulated financial institution, the issuer also has the responsibility to file SARs on reportable activity. The issuer’s AML requirements should provide the program managers with information such as when

and how to report suspicious activity to the issuer. Issuers should consider whether to have the program manager report all suspicious activity, regardless of the dollar amount, or to report suspicious activity only when it meets the reporting threshold. For instance, if the program manager is only required to report suspicious activity at the reporting threshold, the issuer is unlikely to be aware of suspects with multiple cards conducting suspicious activity that would be reportable when aggregated.

The issuer should complete the SAR with enough detail for law enforcement to understand what transpired. Some law enforcement personnel may have limited experience with prepaid cards, thus it is important to use understandable terminology and explain unique schemes. For instance, the prepaid industry typically uses the term “value load,” which is in effect, a deposit. It is also important for law enforcement to know the source of funds; if a card was loaded by payroll the issuer should provide the name of the employer. Likewise, if a card was loaded by cash, the issuer should provide the loading merchant and location if able. The issuer should also have a process in place to respond to law enforcement requests, both through 314(a), subpoenas and National Security Letters. Very little has been published on actual cases involving prepaid cards; however, one


good source is the FATF report published October 2010 entitled *Money Laundering Using New Payment Methods*.

### OFAC

While technically separate from AML regulations, the issuer should also ensure its program managers are maintaining compliance with OFAC requirements. It is recommended that issuers conduct their own periodic OFAC screening to fulfill their obligations; however, the issuer may not be able to perform the initial OFAC screening prior to the account being opened. In those cases the issuer must rely on its program manager to conduct the initial OFAC screen. The issuer should provide the program manager with requirements on the timing of the check, as well as directions on how to clear a hit and report a match. The issuer should include testing of the program manager’s OFAC process as part of its standard CIP testing. Lastly, while the card associations require blocking of certain OFAC sanctioned countries, it is also a good idea for the issuer to provide its own list of prohibited countries to the program manager.

### Conclusion

Hopefully this brief article provides you with valuable information regarding the AML and risk challenges faced by financial institutions issuing prepaid card programs. While the challenges can be significant, prepaid cards remain a viable product line for financial institutions and a necessary financial product for a significant segment of consumers.

Part two of this article will address AML and risk considerations for companies selling and marketing prepaid products, including some of the AML challenges raised by FinCEN’s Notice of Proposed Rulemaking on *Amendment to the Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Prepaid Access* released June 28, 2010. 

Jani Gode, CAMS, senior AML consultant, SightSpan, Inc. Mooresville, North Carolina, USA, [jgode@sightspan.com](mailto:jgode@sightspan.com)

The issuer should complete the SAR with enough detail for law enforcement to understand what transpired