moneylaundering.com
PREMIUM
The world's leading authority on money laundering news, guidance, and analysis

May 2006

One company's approach to mitigating prepaid card risks

By PETER ZIVERTS and JEREMY KUIPER

The Money Laundering Threat Assessment, released in December 2005 by the U.S. government, described stored-value, or prepaid, cards as the elephant in the room no one wanted to acknowledge.

As the report stated, prepaid card programs that "lack customer identification procedures and systems to monitor transactions for suspicious activity present significant money laundering vulnerabilities, particularly if there are liberal limits or no limits on the amount of cash that can be prepaid into the card account or accessed through ATMs."

The government's core issues with prepaid cards are the lack of a clear anti-money laundering (AML) regulatory framework and inconsistent AML oversight by issuers.

But, in pointing out many shortfalls with the cards, the report also implied important solutions to three of the government's primary concerns: anonymity, transaction limits and suspicious activity reporting.

The prepaid bandwagon

Nearly everyone is jumping on the prepaid bandwagon, including banks, with widely accessible open system offerings, and retailers — even car washes — with closed system cards that are redeemable only within a designated retail chain or network.

Western Union markets the Western Union Prepaid MasterCard Card, which is issued by BankFirst as a general use debit card, and as a means of earning a greater share of wallet among its U.S. money transfer consumer base, though it doesn't market its card as a remittance vehicle.

The Western Union Prepaid MasterCard program includes an AML compliance process with features other prepaid card issuers could emulate.

Eliminating anonymity

The prepaid debit program can address the issue of anonymity from the point of enrollment, which incorporates a multi-step process.

Consumers can enroll for the service at an agent location, via Internet or telephone. Enrollment requires basic information: name, address, telephone number, date of birth and Social Security number. For non-U.S. customers, a passport (number and country of issuance), permanent resident card or other government-issued photo ID and country of issuance are required.

After enrollment, the issuer bank (in this case study, Bank First) verifies the consumer information and runs it on a monthly basis through an Office of Foreign Assets Control (OFAC) check. Once background information is verified, a personalized, embossed card is mailed to the consumer's address – P.O. boxes are not accepted unless an accompanying street address is on file.

Card reloads must be done in-person with the card present at agent locations in the United States only. Subsequent OFAC checks are repeated with each load, and every 30 days among the entire cardholder base. Direct deposit loads from a single employer also are permitted.

For employers, the bank conducts a low due diligence review, obtains their tax ID and runs OFAC and Better Business Bureau checks. It also checks with the state the employers operate in to make sure they are registered with the state.

Agents engaged in enrolling consumers and reloading prepaid cards must have in place a documented Bank Secrecy Act/AML compliance program. Western Union reviews all of its agents' AML compliance programs — including suspicious activity monitoring and reporting — on a periodic, risk-assessed basis.

In this part of the program it's important to remember compliance's interaction with marketing: prepaid card providers should not oversell such card attributes as anonymity. Most consumers are reasonable people and understand the need to balance privacy and transparency to ensure the safety of the financial system. A marketing pitch based entirely on anonymity is bound to attract the wrong element.

Transaction limits

Transaction limits promote proper intended use and provide multiple touch points for transaction monitoring. The limits are subject to review and change, but in Western Union's case currently include:

- Two-year card lifespan
- $950 maximum load per 24 hour period
- $2,500 balance limit
- $9,500 aggregate monthly load limit
- Maximum of 10 loads per month

In this case, the program does not allow dual card accounts — one account with two cards to take money out of it — which are becoming a popular means of remitting funds. That type of program calls for much stronger measures to verify the identity

of and exercise control over the remote user.

Transaction monitoring, reporting

In the money services business (MSB) world, transaction monitoring is generally the best way to "know your customer." That's because MSB/consumer relationships are more often transaction- rather than account-based. With money transfer transactions, for example, knowledge of consumer transaction patterns fills the void that the absence of more detailed account information creates.

In Western Union's case, the prepaid card load activity is subject to monitoring at certain thresholds and according to other criteria, including: daily and 30-day activity, principal activity by band, and frequency of purchases and loads. Monitoring facilitates suspicious activity reporting on the aggregate network level, which supplements such reporting at the agent level.

Primary MSBs and their agents each have a responsibility to monitor and report suspicious activity. Agents do it subjectively on the transaction level through direct consumer contact. Primary MSBs have an entire network view and conduct objective, data-driven analysis of aggregate transaction volume.

This dual view to transaction monitoring provides a comprehensive system for understanding consumer activity and identifying suspicious activity, which is the backbone of meaningful reporting.

In addition to monitoring load activity, Western Union receives a monthly file of end user activity to facilitate additional monitoring and reporting of consumer card purchases according to certain business rules. This supplements monitoring and suspicious activity reporting (SAR) reporting conducted by the issuer bank, BankFirst, that monitors certain types of merchants (car rental, airline, etc.) and foreign transaction activity.

Regulation and reasonable promises

Still, critics might say that such AML programs, despite their rigor, don't provide ultimate control over the end user of a prepaid card. That might be true, but only to a small extent. And, it could be said that the same is true with other payment mechanisms, including credit cards, checks and certainly cold, hard cash.

True, some clarity on regulation and oversight is sorely needed. Proper regulation should acknowledge the high-tech nature of prepaid cards and not strive for a lowest common denominator solution that meets the "needs" of tech-challenged, low cost providers. AML compliance is, by necessity, a high-tech business, and regulation should support the creation of tech-based programs that have the ability to enforce transaction limits, and identify and report suspicious behavior.

Experienced issuers understand these challenges and start from the basis of

mandating clear and comprehensive AML compliance controls. And, when issuers and their partners have a shared view of the risks and responsibilities associated with prepaid cards, the AML programs are likely to be highly responsive to government concerns.

Going forward, controlling the risk associated with prepaid cards will require identifying best practices that can be molded into effective, enforceable regulation.

By Peter Ziverts, vice president, External Partnerships/AML Compliance, Western Union Financial Services Inc., and Jeremy Kuiper, managing director, Stored Value Solutions, BankFirst (Sioux Falls, South Dakota, USA).