paybefore.com
• The industry resource for prepaid and stored value cards •

Prepaid from the Perspective of Law Enforcement: Do the Feds Have a Point?

By Don Semesky, President, Financial Operations Consultants, LLC

"I've already had a million dollars on this card." Sounds incredible, but, believe it or not, these words were spoken by a prepaid card company owner to an undercover agent.

Whether the owner was stating a fact, or just puffing, given the context of the conversation, it was certainly clear that he was using this as a selling point in offering the prepaid card as a money laundering instrument.

The problem is, statements like this reinforce law enforcement's theory that prepaid cards and other prepaid instruments pose an innovative and dangerous money laundering threat. Likewise, an example like this would serve as the industry's worst nightmare, i.e., as a catalyst for reputational harm and greater regulatory scrutiny.

As is often the case, many good people get punished for the sins of a few. Unfortunately, in a post-9/11 world, the sins of a few can have a devastating effect globally, so, overreaction has become the norm out of necessity.

The Age of Technology

If timing is everything, then the prepaid industry has it all—almost. People are increasingly reliant on technology to perform almost every type of financial transaction. The prepaid industry has an ever-expanding piece of this market, and the profit potential is enormous. With this potential, however, comes a corresponding responsibility to make sure that prepaid instruments are not abused by criminals, either to defraud or to cause physical harm to the citizens and businesses of this country. To think that it's solely law enforcement's responsibility is like parents thinking their children's educations rest solely on teachers.

So far, what has damaged prepaid's reputation among law enforcement has been based on a handful of prosecutions, which have been, rightly or wrongly, extrapolated into hypothetical worst case criminal money laundering scenarios. For example, could criminal organizations load prepaid cards and take them out of the United States to launder tens, or even hundreds, of millions of dollars? From a purely technological standpoint, the answer is yes. However, from a factual standpoint, is this really happening? The answer is, we don't really know. And, while both law enforcement and the prepaid industry have vested interests in the answer, neither has done a very good job of figuring it out.

In a recent industry survey conducted by the Network Branded Prepaid Card Association (NBPCA) among its members, ATM transactions conducted outside of the United States using domestic-issued prepaid cards amounted to less than 0.02 percent of both industry volume and transactions. Based on these figures, even if all of the money withdrawn overseas using

In Viewpoint, prepaid and stored value professionals share their thoughts and perspectives on the industry. These are not necessarily the viewpoints of Paybefore.

Don Semesky spent 35 years in federal law enforcement: 30 years in various positions with IRS-Criminal Investigation (IRS-CI), including three years as the Anti- Money Laundering Policy Advisor to the Office of National Drug Control Policy (ONDCP), and five years with the United States Drug Enforcement Administration (DEA) as chief of the Office of Financial Operations, where he oversaw DEA's global AML efforts. He can be reached at dsemesky.foc@gmail.com.

prepaid cards represented criminal proceeds, the amount wouldn't constitute a viable money laundering threat.

Here's the problem though: The response to NBPCA's poll covered only a little more than 50 percent of the association's members' dollar volume. To the extent that the sample is representative of the industry as a whole, then it is valuable insight into the use of open-loop or network branded prepaid cards. Although this information is reassuring and a good start, it's not definitive. Additional work—statistically valid and covering prepaid companies outside of the NBPCA and closed-loop cards—would go a long way toward understanding the prepaid industry as a whole and how cards issued in the United States are being used outside of this country's borders.

> *"So far, what has damaged prepaid's reputation among law enforcement has been based on a handful of prosecutions, which have been, rightly or wrongly, extrapolated into hypothetical worst case criminal money laundering scenarios."*
>
> *—Don Semesky, Financial Operations Consultants, LLC*

ATMs and AML

From a drug-money laundering perspective in the United States, the primary threat presented by prepaid cards to date has involved rogue companies that issue unbranded cards with access to one or more ATM networks. When a company can control virtually all of the services that are needed to issue, load, monitor and process a prepaid card, it's a recipe for disaster. One bad actor can exploit this situation to launder untold millions of dollars until either his activity comes to the attention of law enforcement through an unrelated investigation or a bank's anti-money laundering (AML) software flags the company's operating account(s) for further examination.

A prime example of this type of threat is the case of Moola Zoola and its owner, Robert P. Arbuckle. In a November 2006 federal indictment in Dallas, Arbuckle was charged with using Moola Zoola prepaid cards to launder money, stolen by fraudsters from unsuspecting victims through an identity theft scam using eBay and PayPal in Europe and North Carolina. After receiving the victims' money, the fraudsters gave it to Arbuckle, who placed the stolen funds in his Moola Zoola accounts to load prepaid cards carrying the names of people whose identities had been stolen. Then, according to the indictment, Arbuckle transferred the money from one card to another to hide the money trail. He sent some of the cards outside of the United States to Russian nationals who had stolen the money using the PayPal scheme. These criminals, in turn, used the cards to withdraw cash from ATMs in Moscow and Uzbekistan.

Among the items seized during the search of Arbuckle's home were $164,000 in cash, how-to books on identity theft and money laundering, and 55 *boxes* of Moola Zoola prepaid cards. Arbuckle, who had declared bankruptcy in 1998, profited nicely from his venture. At the time of the take-down of the investigation, he was living in a $970,000 home, driving a new Lexus and had more than $130,000 in the bank. He subsequently pled guilty but now is appealing his conviction. The investigation tied Moola Zoola to drug, fraud and child pornography criminal organizations. Support from the financial community on this investigation was outstanding.

Drug Currency

Most of the documented prepaid card abuse seen in drug investigations thus far, however, has been more in the line of payment for drugs by drug abusers and payment for facilitating expenses by drug trafficking organizations (DTOs), than for money laundering.

A good example of how a DTO can exploit a prepaid card was seen in a recent DEA investigation in Baltimore, Md., of the Black Guerilla Family (BGF) gang, a violent inner-city gang, with roots in Southern California. In a press release following the takedown of the case, the U.S. Attorney's Office in Baltimore indicated that the indictment and search warrant affidavit alleged that BGF members used violence and threats to coerce prisoners to pay protection money to the BGF. BGF members would supply the extorted inmate with a prepaid card number and direct the inmate to have family members or friends place money on the card. The card would then be held by a BGF-affiliated corrections officer or BGF member on the street. Court documents also indicate that prepaid cards were used by BGF members as currency for selling illegal drugs and other contraband in prisons.

The BGF gang was able to exploit prepaid cards issued by a company that

has a robust AML program. That company, by the way, has been cooperating with the DEA in the investigation.

The point is: No facet of the financial services industry is impermeable to criminal proceeds. For politicians or law enforcement officials to demand this or for the industry to represent that it is, is completely unrealistic. It is just as unrealistic to believe that criminal organizations will not exploit a financial service whose participants are not vigilant against the infusion of illicit proceeds.

Following the Electronic Trail

In investigations like the BGF, the abuse involving prepaid instruments is difficult to detect and usually discoverable only through some type of unrelated enforcement activity such as an arrest or a search warrant.

In these cases, the tables turn, and the criminal organization's use of the prepaid instrument can come back to bite them. Unlike cash, prepaid transactions leave an electronic audit trail for the investigator. Working in partnership, law enforcement and the prepaid provider can identify co-conspirators in drug organizations, corrupt public officials who possibly were paid with these cards, possible corrupt agents who are selling the cards in bulk, the purchase of forfeitable assets as well as identify other leads to events and activities that can be used as evidence of the criminal conspiracy.

Key learning points for investigators are understanding how to identify the prepaid instrument, its use and limitations, and then knowing how and where to retrieve the information. Unlike a bank account, there are many parties associated with the issuance, loading and monitoring of a prepaid product. There is going to be a learning curve for the investigators to understand how to gather this evidence. Likewise, there have to be record-keeping requirements that will allow for these transactions, and all of the identifying information, to be easily located and retrieved.

Non-drug criminal activity associated with prepaid cards identified thus far, as evident from the Moola Zoola case, has primarily entailed scenarios where fraudsters have used prepaid cards in the layering process to conceal and move the proceeds of their fraudulent activities outside of U.S. borders.

> *"Some of the most sophisticated money laundering schemes are now being identified and broken with the information that modern technology is bringing to the financial services industry."*
>
> *—Don Semesky, Financial Operations Consultants, LLC*

Bank Secrets and Bad Guys

The philosopher George Santayana told us: "Those who cannot remember the past are doomed to repeat it."

With that in mind, let's examine law enforcement's relationship with the banking industry. Historically, when the matter involves a robbery or fraud, where the bank is a victim, there is a very close working relationship between the bank and law enforcement.

Why? Because they have the same goal: "Catch the bad guy" and try to make the victim whole.

Now, let's switch the scenario to a Bank Secrecy Act (BSA)/AML matter. For years, this too often became an adversarial dance, with banks thinking law enforcement was costing them money through time and expenses associated with regulatory compliance and the loss of revenue-generating accounts. Law enforcement, on the other hand, questioned the motives of banks in domiciling the account of the suspect under investigation.

Years ago, at a banking conference in Miami, I was asked by a banker from an offshore center, "Why does the U.S. government harass us with all your laws and regulations, when all we're trying to do is make a buck?" The guy was a poster child for bad corporate citizenship. What we tend to forget is that when Congress passed the Currency and Foreign Transaction Reporting Act in 1970, the intent was to create a way for the financial community and law enforcement to work together to identify and "catch the bad guys" through the large amounts of currency their crimes were generating. It has literally, and embarrassingly, taken decades, but, for the most part, I think we are there with the bank/law enforcement relationship. Whenever I have encountered a scenario within a bank where the business interest dominates and overrules compliance for the sake of "making a buck," that bank has ended up in either regulatory or criminal hot water.

What's important now is to not squander the lessons learned and build

the relationship between the prepaid industry and law enforcement from the outset.

Partnering with Law Enforcement

So what then is the best workable solution? The answer is developing a *partnership* between law enforcement and the prepaid industry.

Right now there is a lot of misunderstanding on both sides. From the prepaid industry's side, the need is to raise the comfort level of law enforcement that there are enough controls in place to deter abuse of the products. From the law enforcement side, the need is to understand and accept that prepaid is an advancing technology that is going to become part of the fabric of the financial services industry, so we need to adapt and "investigate" the industry to discover how it works and how we can work with it.

I would stress not to wait for an invitation but to reach out to law enforcement to educate them on the products in the marketplace, how they work, the AML controls that are being put in place for these products and the type of information that is gathered from customers when they purchase these products. In return, law enforcement needs to share money laundering methodologies it is seeing in investigations and assist the industry in building a set of risk factors or red flags that can be incorporated into AML software monitoring programs.

The prepaid industry is built on cutting edge technology, which translates into information. Information is the key ingredient that law enforcement needs in tracking illicit money around the globe. Some of the most sophisticated money laundering schemes are now being identified and broken with the information that modern technology is bringing to the financial services industry. Working in partnership, law enforcement can learn what information the prepaid industry has to offer, and the prepaid industry can learn what types of scenarios are being encountered and what information law enforcement needs.

Protecting Your Assets

A quote I use in describing law enforcement's efforts in combating the drug problem is, "We can win any battle; it's the war that's killing us." The same could be said about fraud and other crimes where, for some, the reward often outweighs the risk and social responsibility. In other words, law enforcement, at all levels, does not have enough resources to address the entire crime problem. We have to prioritize our focus and leverage resources to maximize our impact on the criminal organizations that pose the biggest threats. And, law enforcement needs the private sector's help to address the problem.

On the AML front, what this means is compliance and partnership. Every minute law enforcement spends investigating a financial institution for noncompliance is precious time taken from investigating the real bad guys who threaten our safety and security. A good compliance program discourages criminals from using your products, which, in turn, reduces your risk and your exposure to sanctions. Another benefit of a good compliance program is it also reduces the likelihood of internal and external fraud.

The NBPCA has drafted model BSA/AML compliance protocols and red flags that could indicate unlawful exploitation of a prepaid product. If you're looking for a starting point, I would recommend you look there. A good compliance program will have as its cornerstone thorough customer identification and verification, and controlled and reasonable load limits. When these are coupled with a good monitoring software and competent analytical follow-up, your company should not only be protected, but also be a credit to the industry.

To paraphrase a line from the gun lobby, "Prepaid cards don't launder money, people launder money." However, just like a gun makes it easier to kill people, prepaid cards can certainly make it easier to launder money. The prepaid industry well understands the outstanding business potential for their products. Now, it has to jealously protect those products from being abused by the people who will attempt to exploit them for their illicit gain—and, in turn, cause reputational and financial harm to the industry. This can be accomplished through a balancing of business interests with good corporate citizenship, practiced through responsible AML compliance and a continuing open dialogue and partnership with law enforcement.