Hal Berghel

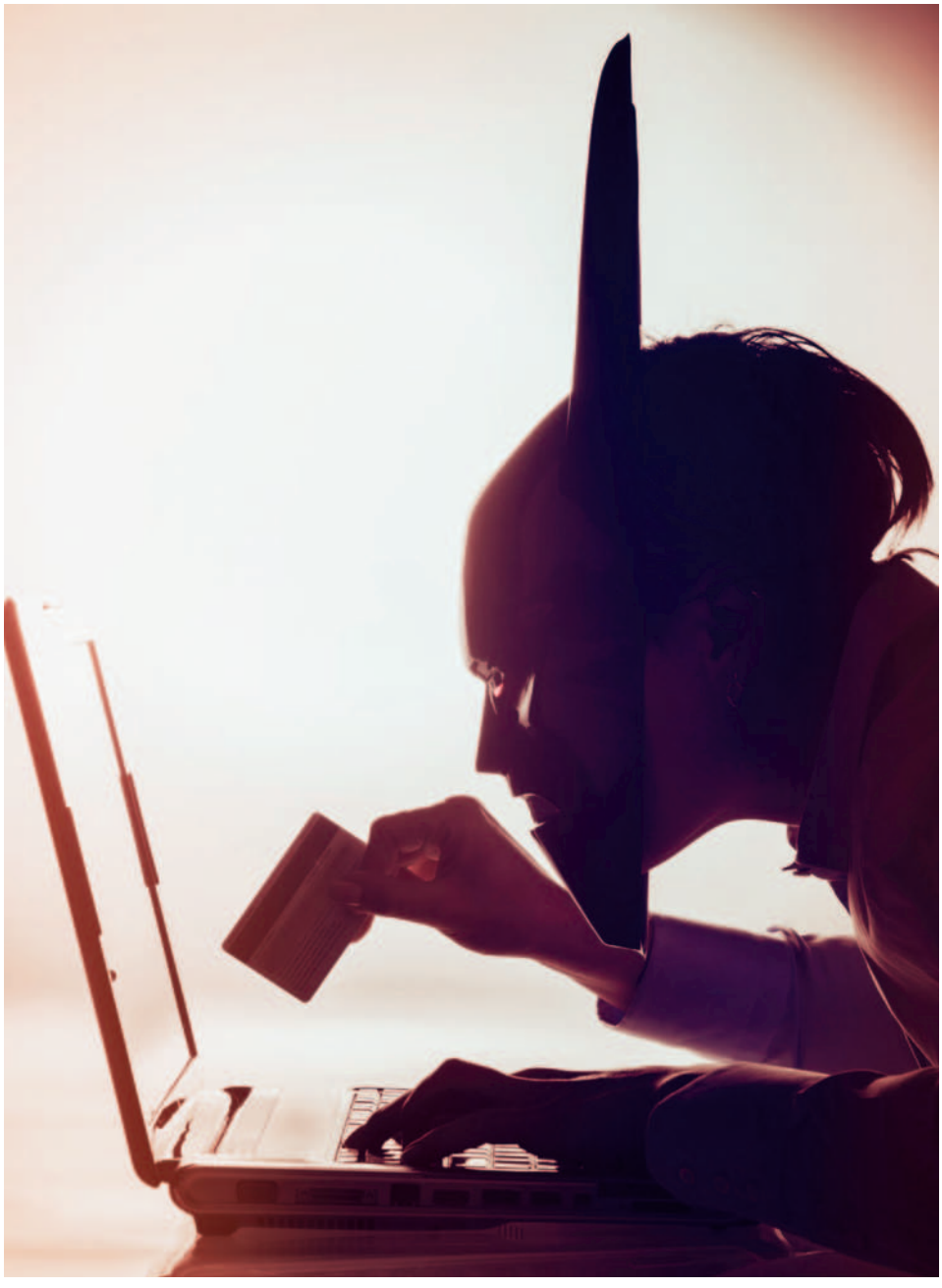
THE 2012 ANTI-MONEY LAUNDERING AND FINANCIAL CRIME CONFERENCE

Aria Las Vegas, October 1-3, 2012

I've gone a good part of my adult life holding the view that spending three days at a conference with bankers would be about as pleasant as having a root canal. But due to the diligence and dedication of today's crooks and criminals (I'm referring here to those outside the financial community) today's bankers actually have some interesting issues to discuss. This conference, sponsored by ACAMS, the Association of Certified Anti-Money Laundering Specialists, drew 1,500 attendees to Las Vegas the first three days of October, 2012. From what I could tell, a pleasant time was had by all.

My interest in AML derives from my work with identity theft and financial fraud (itf-froc.org) over the past decade or so. As it turned out, identity theft and money laundering are appealing to the same groups these days: narco-traffickers, terrorists, gangs, and a motley crew of politicians and Ponzi schemers. This conference brings together AML specialists from what has become the first line of defense: the financial community. As one of the speakers in a spinout session on counter-terrorism financing put it: financial intelligence has become a full and equal partner to signals intelligence and human intelligence in the war on money laundering. But I'm getting ahead of myself.

The conference opened with a keynote address from the head of the criminal investigation unit of the IRS. From my experience keynote addresses from senior bureaucrats is usually a mistake as they all tend to be predictable and formulaic: acknowledge hard work of employees, explain how well the organization is run, document a few



Courtesy of iStock

recent successes, and predict a rosy future. This speaker did not disabuse me of my predilection. It was followed by a plenary session entitled "How to Succeed in AML Without Really Trying", which was a skit about a hypothetical AML challenge in a bank. The role-playing involves a half-dozen certified AML practitioners. I guess this is a banker's idea of reality TV. The plot, such that it was, involved a bank that was exposed as an inadvertent participant on a Ponzi scheme. The actors took on the roles of CEO, legal counsel, AML officer, prosecutor, Ponzi schemer, and public relations officer took the audience through the creation of communication strategy plan, disclosure to regulators, remediation plan, internal and external investigations, and the need to satisfy different objectives working at cross purposes quickly. The parallels between AML readiness in the financial community, SOX, and GCB compliance in the gaming industry should not be overlooked. As the faux general counsel explained the need for preservation and archiving of all documentations, I couldn't help thinking about Arthur Andersen's attorney recommending that the Enron staff revisit the document retention policy in the middle of a Justice Department investigation. I think the word's out that messing with the evidence can get the regulators and prosecutors more irritated than the original breach. Qua skit, I'm not sure about the effectiveness of the delivery method – no one was drawn into a world of make believe as far as I could tell – but it was a smooth transition to lunch.

The real value of this conference, in my view, is in the spinout or concurrent sessions. One noteworthy example was a panel entitled "Mastering the Digital World: Exposing Fraud in Nontraditional Payments," that brought together executives from VISA and MasterCard, and the head of the Finance and Proceeds of Crime Unit of Homeland Security Investigations. The moderator was able to keep the panelists on point for the most part as they discussed the bank card industry vs. law enforcement interests

Courtesy of iStock

in financial cards that aren't strictly debit/credit oriented. Prepaid cards are a good illustration.

The context of the discussion is the use of criminals and terrorists to make use of financial products as soon as they become available. Since 2000, financial institutions were required to file suspicious activity reports (SARs) under the Bank Secrecy Act (BSA), and since 2002-3 this requirement was extended to casinos and card clubs including those located on tribal lands. These regulations created some problems for money launderers of all stripes who have historically used these institutions to launder, store, transfer and withdraw cash earnings. The BSA and Patriot Act made the conversion of physical deposits to electronic deposits more transparent and easier to detect. This inspired those on the dark side to look for alternatives.

Enter the prepaid product. I first became aware of the use of prepaid cards by criminal organizations through my work with law enforcement some years back when criminal organizations began using prepaid gift cards for trans-border money transfers. At that time, law enforcement was ill-equipped to deal with the problem because they had no way of discerning the value represented by the card. In the past year, AML regulations have made this venue less convenient for the criminals because U.S. Treasury regulations through FinCEN require at least a designated point of contact for prepaid cards. Thus, there is presumably a risk manager in some financial institution somewhere reachable by electronic means that can handle law enforcement enquiries, prepaid cards are coming out of the shadows.

This sets the stage for the natural tension between the prepaid card vendors and merchants on the one side, and law enforcement and the regulators on the other. The former wants unfettered access to the data under the promise that they will be responsible stewards, while the prepaid industry emphasizes the legitimate use of prepaid

The holy grail of the prepay criminals at the moment is apparently the closed loop, one-time card with both cash access and online capabilities. In this way the card is maximally liquid: once the card is loaded, the value can float around the Internet without regard of the physical location of the card.

cards by the community of people who don't use banks. In fact, in 2013, prepaid cards will be the only option for Social Security recipients who don't have bank accounts that accept direct deposit, because the U.S. Treasury will stop printing Social Security checks. This contention over the privacy of the prepaid card data is unlikely to go away any time soon and well-illustrates the battle ground where law enforcement's "need to know" assaults personal privacy. It will be interesting to see whether the financial industry will be able to hold any ground regarding prepaid cards.

The discussion of criminal tactics in the use and abuse of prepaid cards was very interesting. There are several ways of characterizing prepaid products. One orthogonal characterizations is closed loop vs. open loop and one time vs. reloadable. This is important because different controls are required to regulate different products. From the criminal's perspective, closed loop cards are particularly attractive because at the moment no "KYC" (know your customer in bank-speak) is typically required by the banks. They share this characteristic with throw-away cell phone merchants. This modus operandi is similar to the gift card exploits that I first became aware of several years ago – just a few tweaks here and there. The holy grail of the prepay criminals at the moment is apparently the closed loop, one-time card with both cash access and online capabilities. In this way the card is maximally liquid: once the card is loaded, the value can float around the Internet without regard of the physical location of the card. One of the speakers mentioned that it is not uncommon to have the cash moved from confiscated prepaid cards while they are in the evidence locker.

There were several sessions that dealt with new-wave money laundering and fraud. An entire suite of facilitation tools is in use by these post-modern crooks when using banks and bank products:

- Internet
- Credit/debit cards
- Stored value cards
- NGOs/charities
- Illegal money remitters
- Informal value transfer systems
- Shell/Front companies
- Off-shore havens
- Correspondent banking
- Money services businesses
- Trade-Based Money Laundering
- Trans-national bulk cash movement
- Wire transfers
- Mobile Phones

It's clear from this list that the crooks are pushing the envelope on many fronts.

A recent buzzword in counter-cyber-terrorism is "threat financing." As it turns out, the terrorists among us rely on the financial community to support their derring-do as much as the traditional criminals. They use fraud, money laundering, extortion, kidnapping, drug smuggling, and the familiar cache of revenue-generating exploits to their advantage as well. As such they rely on the same financial industry to help them raise, move, store and spend their revenue as the crooks. Their goals are the same: isolation from the source of funds and any criminal activity that produced them. They also share the same tactics of placement, layering and integration of the funds.

In all there were about fifty of these spinout sessions in seven categories spread over the two days, augmented by two keynotes and six seminars. The categories included case study analysis, audits, AML knowledge sessions, AML program development (two concurrent each period) and multi-industry interactive training (two concurrent each period) – about what you would expect of a conference run by an accrediting association. I would think anyone interested in AML would be hard pressed not to be able to fill up the two days with interesting sessions.

While I didn't see many representatives from the gaming and entertainment industry represented, that should change with time as AML due diligence is expected in the industry. The CTR-C, and Form 8300 compliance requirements alone justify sending the AML compliance officer, and a few additional staff each year.

This was a successful, well-attended, and well organized conference. I recommend it for your consideration.

Hal Berghel is Director of both the UNLV School of Informatics and the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). His consultancy, Berghel.Net, provides security and management services to government and industry.