TECHNOLOGY IN THE FIGHT AGAINST MONEY LAUNDERING IN THE NEW DIGITAL CURRENCY AGE

WHITE PAPER

CLEAR
June 2013

THOMSON REUTERS™

SUMMARY

Drugs, prostitution, illegal gaming, fraud, extortion – where there's money tied to a criminal activity, there's a crook who wants to "clean" it or legitimize the money so it can be moved throughout the world's financial system, no questions asked.

Like many illegal activities, money laundering is undergoing a revolution of sorts. That's because technology, from online casinos and social media websites to the introduction of digital currencies, is offering alternative pathways for criminals to launder illegal profits. In spite of significant regulations designed to deter money laundering in the U.S. financial system, instituted shortly after the tragic events of Sept. 11, 2001, law enforcement agencies and financial institutions remain in a race to keep ahead of criminals.

This white paper, brought to you by Thomson Reuters, explores the changes occurring in illegal money-laundering activities, and what financial institutions and law enforcement agencies are doing to combat this growing threat to the stability of the world's financial system through the use of new strategies, regulations and technology.

CONTRIBUTIONS

Thomson Reuters would like to thank the following people for their contributions to this white paper:

Cindy Williamson, CFE, CAMS, enforcement analyst III, National White Collar Crime Center (nw3c.org)

Jason Vazquez, senior vice president and BSA/AML compliance officer, Provident Bank (providentbanking.com)

Jason Thomas, senior strategic analyst, Thomson Reuters

Katherine Sagona-Stophel, government analyst, Thomson Reuters

DEFINING THE PROBLEM

On May 28, 2013, U.S. prosecutors indicted seven people in a cyber-crime operation involving an online bank that allegedly handled more than $6 billion for drug dealers, child pornographers, identity thieves, hackers and other criminals, all connected through the anonymous exchange of digital currency. According to U.S. officials, it was the largest money-laundering bust in U.S. history.

At the center of the alleged cyber-money laundering operation is Liberty Reserve, a Costa Rica-based currency transfer and payment processing company. According to Reuters, Liberty Reserve processed around 12 million transactions per year since 2006. The company allowed account holders to set up anonymous accounts and convert real money into anonymous, untraceable digital currency called LR.

The Liberty Reserve case represents a sea change in the fight against money laundering, which is the practice of processing money and assets gained through illegal means into legal (clean) status. Money laundering is often a secondary process – preceded by an illegal activity, such as drug trafficking or an online scam. In some cases, money laundering may be used by terrorist organizations to threaten and/or carry out attacks based upon a philosophical agenda. A key element of the process is maintaining anonymity and avoiding transparency throughout the process. Where money launderers were once limited to physical currency, the advent of digital currency has compounded the complexity of the global fight against this activity.

The Financial Action Task Force (FATF), an inter-governmental organization comprising 36 countries, estimates money laundering at 2 to 5 percent of global annual GDP or gross world product, which amounts to an estimated $1.38 trillion to $3.45 trillion. But because the problem is so widespread, the FATF notes that there is no way to estimate how much money is actually laundered through the world's legal and illegal financial systems.

REUTERS/Kacper Pempel

"Money laundering and the financing of terrorism are financial crimes with economic effects," said Min Zhu, deputy managing director of the International Monetary Fund (IMF) in a 2013 *IMF Alert*. "They [money launderers] can threaten the stability of a country's financial sector or its external stability more generally. Effective anti-money laundering and combating the financing of terrorism regimes are essential to protect the integrity of markets and of the global financial framework as they help mitigate the factors that facilitate financial abuse. Action to prevent and combat money laundering and the financing of terrorism thus responds not only to a moral imperative, but also to an economic need."

The fight against money laundering took on greater urgency following the tragic events in the United States on September 11, 2001 (9/11). The U.S. government, the IMF and other government bodies around the world intensified their anti-money laundering efforts after it became clear that the terrorist

organization al-Qaida used money-laundering techniques to successfully fund the 9/11 attacks. It appears, based on a 2005 PBS Frontline investigation, that money raised through Islamic charities in Europe and the United States was laundered through the European banking system to support the planning of 9/11 and other terrorist operations.

"Effective anti-money laundering and combating the financing of terrorism regimes are essential to protect the integrity of markets and of the global financial framework."

Today, more than 10 years after 9/11, money laundering in the digital age has taken on even greater urgency because of the potential it may have in destabilizing the financial health of countries. Money laundering has flourished in countries with ineffective or intentionally loose financial controls, allowing organized crime and/or terrorist groups to easily move funds without being detected. The concern, as some governments such as Germany have publicly expressed about the financial stability of Cypress (in the context of the financial struggles of the European Union), is the cancer-like impact money laundering can have on broader financial systems.

The growing problem of money laundering prompted the announcement by the U.S. Treasury Department in November 2012 of the formation of a new anti-money-laundering task force, according to a Reuters news report by Brett Wolff (Nov. 12, 2012). David Cohen, the U.S. Treasury's Under Secretary for Terrorism and Financial Intelligence, said the primary reason behind the formation of the task force is the "remarkable change" occurring in the financial industry, driven by technological and financial innovation.

"Money-laundering schemes themselves are also becoming increasingly sophisticated and international in nature," Cohen said in the Reuters report. "The same hugely beneficial technological and financial advancements have had the unfortunate side effect of amplifying potential AML [anti-money-laundering] risk."

According to a sampling of documented, prosecuted investigations compiled by the Internal Revenue Service (IRS) for 2010-11, money laundering occurs regularly every day throughout the United States, from major metropolitan areas to small towns in middle America. Examples of money laundering include:

- On May 14, 2013, the U.S. Department of Homeland Security served a court order to Dwolla, a popular mobile payment service, requiring it to cease all account activities with the Mt. Gox (mtgox.com) digital currency (Bitcoin) exchange, citing the fact that Mt. Gox and its subsidiary, Mutum Sigillum LLC, a Delaware corporation, were not licensed to transmit money. The action has been widely perceived in the growing world of digital currency as a first strike by the U.S. federal government in regulating Bitcoin, a fast-growing digital currency favored by money launderers.

- *Gambling News* (April 10, 2013) reported the indictment of 34 individuals and 23 companies connected to Legendz Sports (a.k.a. Legands Sports), an online sports betting operator accused of "racketeering, money laundering and illegal gambling."

- On Aug. 1, 2012, the FBI's Los Angeles Division announced that U.S. and Australian officials secured court orders to recover more than $24 million in assets from e-Bullion.com, which federal prosecutors accused of operating as an illegal money-transmitting business. "Through the e-Bullion.com website,

individuals opened accounts with real money, which they used to purchase virtual e-currency. The FBI contends that e-Bullion allowed individuals engaging in fraud to move money around the world while remaining virtually anonymous and avoiding many global banking reporting requirements."

- On Aug. 26, 2011, Joy Edison, a resident of Elkton, Md., was sentenced to 70 months in prison for conspiring to launder more than $400,000 in drug proceeds. Over seven years Edison and a group of co-conspirators laundered the proceeds of heroin sales through Las Vegas casinos, Maryland lottery tickets, a used-car business, and properties purchased by Edison through a front company, J. Edison Properties.

- In July 2006, Arthur Budovsky and Vladimir Kats were indicted by the state of New York on charges of operating an illegal money transmittal business, GoldAge, Inc., from their Brooklyn apartments. The defendants transmitted at least $30 million to digital currency accounts worldwide. Source: *National Drug Intelligence Center*, June 2008.

- Hector Dominguez-Gabriel, an international narcotics trafficker and money launderer based in Mexico, was sentenced to 240 months in prison on Aug. 12, 2011, on narcotics importation and money-laundering charges. Dominguez-Gabriel laundered millions of dollars in narcotics proceeds back to Mexico through a systematic process of small, structured deposits into bank accounts throughout the United States.

- Reuters reported that the FBI was investigating Second Life's virtual casinos in April 2007 for potential illegal activity related to the 1970 Illegal Gambling Business Act or the Unlawful Internet Gambling Enforcement Act. In its *2011 National Gang*

REUTERS/Fernando Donasci

Threat Assessment: Emerging Trends, the National Gang Intelligence Center noted the viability of Second Life as a source for criminals to commit a wide range of illegal activities.

- According to the *FBI Intelligence Assessment* (April 24, 2012), "organized criminal groups (as of June 2011) were using an online role-playing game to facilitate money laundering by purchasing virtual game currency with the proceeds of criminal activity. The virtual game currency was used to purchase in-game virtual items that were then sold to other players for clean money."

In its most simple form, money laundering is a process, according to a Rand Corporation monograph, *Cyber Payments and Money Laundering*, that exists simply because money – paper bills and coins – is bulky and heavy to transport in large quantities, making it difficult to move around from one person or organization to another, or from state to state, or from country to country.

Besides U.S. financial institutions, other financial structures that are typically used by money launderers include:

- Overseas and offshore bank accounts located in countries that have secrecy laws protecting the identity of the individuals or corporations that open accounts in their countries.

- Shell corporations, which are used to funnel money through "legitimate" businesses.

- Parallel or underground banking systems, which exist in countries such as India, Pakistan, China and other parts of Asia, and are typically enforced by organized criminal groups or gang alliances.

- Trade-based money laundering (TBML), which involves the laundering of funds through the trade of goods and services. In 2006, the FATF noted the growing use of TBML by criminal organizations and terrorist groups as various governments throughout the world tighten anti-money-laundering rules and regulations. However, TBML remains an overlooked aspect of money laundering to this day.

- Prepaid cards, often referred to as gift cards, and readily available throughout the country at gas stations, drug store chains and discount retailers, have become so popular among money launderers that the Financial Crimes Enforcement Network (FinCEN) within the U.S. Treasury Department is exploring new rules that would require travelers to declare prepaid cards in excess of $10,000 to customs officials, according to *Personal Finance Digest* magazine (April 4, 2013).

From a law enforcement perspective, Cindy Williamson, a certified anti-money-laundering specialist with the National White Collar Crime Center (NW3C), believes the key to building a solid case is linking money laundering to a specific illegal act, such as

mortgage fraud, drug trafficking or mail fraud. While federal laws regarding money laundering are extensive, money-laundering laws from state to state are inconsistent, explained Williamson.

"Because criminal groups are so much more sophisticated in their use of technology to commit their crimes and hide the proceeds of their activities, law enforcement has to work more strategically to identify criminal activities and collect intelligence and evidence," Williamson said.

> *"Many within the law enforcement community are concerned about the frightening levels of technology that criminals have at their fingertips."*

"Many within the law enforcement community are concerned about the frightening levels of technology that criminals have at their fingertips," she added.

One reason Williamson believes that technology-based crimes are growing is that it's safer for criminals.

"Why risk getting killed or enduring a long prison sentence for drug trafficking when you can make money faster with less risk (convictions for white-collar crimes tend to receive less prison time) by participating in activities such as mortgage fraud or healthcare fraud?" Williamson said. "Along these lines, investments in technology allow criminal groups to launder money faster and more safely."

The bottom line: Criminals are investing in technology to launder money; financial institutions and law enforcement agencies need to invest in technology as well.

MONEY LAUNDERING IN THE DIGITAL AGE

One of the latest trends in money laundering involves digital currency. Many Americans are only beginning to learn about the growing use of independent virtual cryptocurrency, such as Bitcoins, Litecoins, Zen and Namecoins. But the reality is, online and alternative currencies exist in many places, from Linden Dollars used in the online game Second Life, and Justice Points in World of Warcraft, to Berkshares, an alternative currency created by five banks to promote local business in the Berkshire region of western Massachusetts. And where there are opportunities to exchange real money for online money, there money laundering can also exist.

iStockphoto.com

Bitcoin is an encrypted virtual currency that is completely anonymous, unlike a credit card transaction or personal check, which can be tied to a specific person or entity. Launched in 2009, Bitcoins are not like dollars, yen or euros because there is no government or central regulatory agency that regulates the value or the use of virtual currency, which is exchanged freely and anonymously on peer-to-peer networks worldwide.

Because some virtual currencies can be freely exchanged without being traced, they have gained prominence in the underbelly of the Internet, also known as the Deep Web, which organized crime groups, terrorist cells and other shadowy figures, from child pornography enthusiasts to human traffickers, call home. In a nutshell, the Deep Web is that invisible portion of the Web that "cannot be indexed by search engines – a place where Google does not go," note writers Pablo Albarracin and Christopher Holloway in their Dec. 17, 2012, story about the Deep Web for *Worldcrunch.com*. "Offering anonymity and freedom, the Deep Web has transformed over the years into a deep (some say it represents 90 percent of the content available on the Internet), almost inhospitable, little-explored repository that can host anything from the most innocent to the most ruthless and unthinkable."

While the anonymous nature of the Deep Web has been critical to people fighting against repressive regimes around the world and to hacktivist movements such as Anonymous, the Deep Web is more closely associated with drug trafficking, arms trafficking, terrorism and child pornography. For example, some websites have become online retailers for illegal transactions of drugs, illegal weapons or child pornography, allowing criminals to use digital currency as their preferred source of payment.

FRAUD EXAMINERS CONCERNED ABOUT DIGITAL CURRENCY

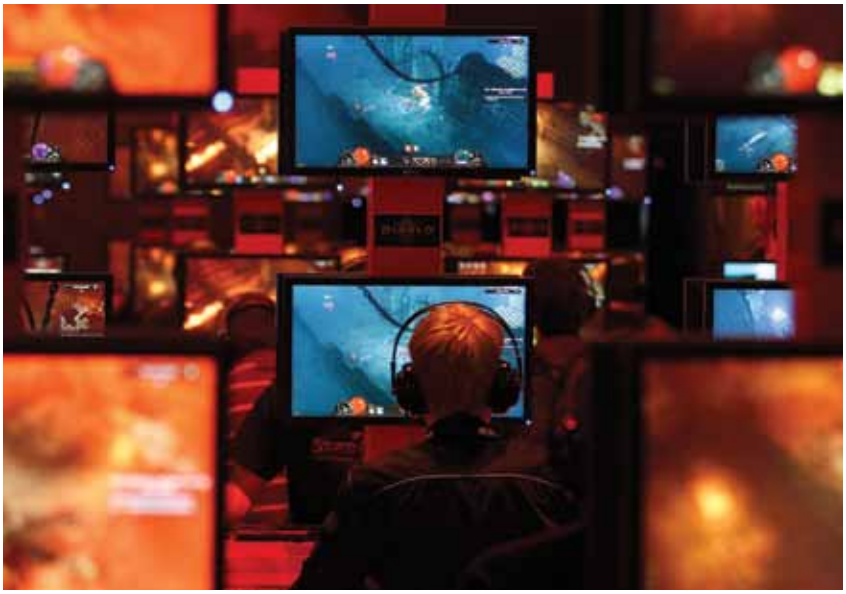
PERCENT OF CERTIFIED FRAUD EXAMINERS WHO HAVE WORKED ON A FRAUD CASE INVOLVING DIGITAL CURRENCIES:

PERCENT OF CERTIFIED FRAUD EXAMINERS WHO FEEL DIGITAL CURRENCIES WILL CHANGE THE WAY THEY CONDUCT FUTURE FRAUD INVESTIGATIONS:

Source: Thomson Reuters-ACFE Survey, April 2013

And yet, you don't have to go into the underworld of the Deep Web to load up on virtual currency. Anyone, from a curious soccer mom to a seasoned drug dealer, can buy Bitcoins or similar virtual currencies through eBay or Craigslist. And that's what worries law enforcement officials.

Because of the growing interest in them, FinCEN announced new money-laundering rules on virtual currencies in March 2013. According to a *Wall Street Journal* report by Jeffrey Sparshott (March 21, 2013), "firms that issue or exchange the increasingly popular online cash will now be regulated in a similar manner as traditional money-order providers such as Western Union Co. They would have new bookkeeping requirements and mandatory reporting for transactions of more than $10,000. However, the new rules don't apply to individuals who simply use virtual currencies to purchase real or virtual goods."



REUTERS/Ina Fassbender

That leaves room for virtual worlds that use or offer online currency, allowing multiplayer online games to serve as unregulated channels for money launderers, according to Jason Thomas, a senior strategic analyst with Thomson Reuters.

"Money laundering through these massive multiplayer online games has largely gone ignored by law enforcement for a long time because it was perceived as being too complex," Thomas noted. "These online games, and the Deep Web in general, can be very intimidating. It's not only the strange subcultures, but the size of it all can feel overwhelming. With trillions of transactions, many in the law enforcement community can't imagine even where to start."

While the relationship between digital currencies and money laundering may just be emerging, it's appearing on the radar screen of law enforcement and financial institutions.

In an April 2013 Thomson Reuters-Association of Certified Fraud Examiners (ACFE) survey of more than 800 certified fraud examiners, 10 percent report working on a fraud case involving digital currency, with 61 percent forecasting that the growing prevalence of digital currencies will change the way they conduct future fraud examinations.

"Another factor is that some in the law enforcement community are very cautious to act in the presence of new technology with the fear that they may become involved in a precedent-setting case," Thomas added.

MONEY LAUNDERING AND COMPLIANCE

While you might expect money laundering to occur in the shadows of our world, like the Deep Web, in many cases, it can occur in plain sight, within the mainstream of the American financial system. On Dec. 11, 2012, HSBC Holdings Plc (HSBC), one of the world's largest financial institutions, agreed to pay a record $1.92 billion fine to the U.S. Justice Department, based on its role in allowing the laundering of millions of dollars by Mexico's Sinaloa and Colombia's Norte del Valle drug cartels through the bank's Mexican and U.S. banking units, according to Reuters (Dec. 11, 2012).

The settlement, according to Reuters, represented the third time in 10 years that HSBC has been penalized for lax controls. "Compliance [at HSBC] was 'woefully inadequate,'" noted Loretta Lynch, the U.S. attorney in Brooklyn.

Thomas said the big challenge for financial institutions is knowing your customer and red-flagging transactions that appear suspicious.

REUTERS/Yuriko Nakao

"The technology exists through providers such as CLEAR and World-Check to identify known bad guys," Thomas said. "And with additional data-mining technology, we can take that information and link a person of suspicion to other people who may be supporting related criminal activity."

In addition, noted Thomas, "the technology exists for financial institutions to identify other money laundering techniques, such as opening up an account in a deceased person's name."

The key to monitoring money-laundering activity is to identify unusual patterns within the transfer and flow of illegal money into the legal money supply. Often times, the tip-off is the change in velocity of the particular incoming and outgoing flow of funds.

"The best money launderers understand the system. They're patient. They move money through the world's financial systems slowly and in smaller, less suspicious amounts," said Thomas. "Money launderers who get caught are impatient – they want to move large amounts of funds through the system fast."

"The problem is that as we build better mouse traps, the mice keep getting smarter," commented Jason Vazquez, senior vice president and BSA/AML compliance officer for Provident Bank, a 120-year-old bank based in Montebello, N.Y., with more than $3.7 billion in assets under management.

Before 9/11, Vazquez explains, most banks throughout the U.S. followed a general list of activities to comply with the Bank Secrecy Act (BSA), a bill signed into law in 1970 that launched a reporting system for financial transactions exceeding $10,000 – a significant step in monitoring the flow of criminally obtained proceeds. While important, maintaining a BSA program wasn't a focal point for many banks or examinations conducted by state or federal regulators.

The key to monitoring money-laundering activity is to identify unusual patterns within the transfer and flow of illegal money into the legal money supply. Often times, the tip-off is the change in velocity of the particular incoming and outgoing flow of funds.

But 9/11, and subsequently the USA Patriot Act, changed the landscape significantly, imposing stiffer rules and regulations on U.S. financial institutions in monitoring financial transactions and money-laundering activities that may offer links to the funding of terrorist activities.

"The Patriot Act raised the bar and put everyone, including non-depository financial institutions, on the same page," said Vazquez. "But at the same time, it imposed new challenges. In many areas, the Patriot Act doesn't tell you explicitly what to do. So we, like many banks, not only have to keep up with the growing sophistication of money-launderers and terrorists but also the growing expectations of regulators, and have dramatically increased our investments in technology and people."

More than violating the law, most banks don't want to be known as the next bank that missed the banking activities of a terrorist group. "The bad PR would be devastating to the reputation and trust of a financial institution – and aside from complying with regulations, it is a key driver behind our money-laundering investments – to protect a reputation that Provident Bank has built over 120 years," Vazquez said.

Advanced technology is allowing financial institutions, such as Provident Bank, to be more consistent in screening the identity of a customer and monitoring for potentially suspicious customer banking activities. In addition, sophisticated behavioral analytics allow banks to create risk profiles for customers and employees, which can be useful in the monitoring process. To complement his internal efforts, Vazquez looks to the best practices established by organizations such as the ACFE for information and ongoing training.

One tool that Vazquez uses is a powerful data-mining software suite that allows his organization to explore public

records associated with a customer whose transactions raise red flags. This software also allows the bank to identify associations with other individuals who may be supporting a money-laundering ring.

"Before this technology, an internal investigation would involve the analysis of hundreds or thousands of pieces of paper," said Vazquez. "Now, data-mining tools allow us to explore a hypothesis within hours or even minutes, giving us a clearer picture of the people linked to transaction anomalies.

"Because of 9/11, the goal posts are always moving," he added. "Regulators increase their expectations from year to year. They're expecting you to become more effective, efficient and more sophisticated. And the truth is, we have to because the money launderers and terrorists are continuously pushing the edges as well."

Determining the ROI on technology investments is difficult for any organization. While preparing for a board meeting in the past, Vazquez faced that exact question: "What is the value of investing in technology to track money-laundering activities based on the best practices in the industry versus the cost of complying at the minimal level based on BSA and Patriot Act rules?"

With just hours before the start of the board meeting at which Vazquez needed to address that question, a news report broke that listed the names of several regional banks that were being investigated by federal authorities for not catching the money-laundering activities of an organized crime ring linked to terrorism.

"Our bank was not in the article because our systems caught it," said Vazquez. "To me, that's the best kind of ROI – maintaining your company's reputation."

IDENTIFYING AND INVESTIGATING MONEY LAUNDERING

As local, county, state and federal law enforcement officials fight the seemingly uphill battle against money laundering, images may come to mind of who is actually involved in these types of criminal activities. You may think of the lone drug dealer, the pimp, or even the geeky kid who got in over his head by moving money around in an online game.

The truth is, money laundering today is as organized and disciplined as the operations of a major company. And oftentimes, it's linked to a growing number of sophisticated cybercrime operations that avoid the dirty and bloody world of the streets.

According to Keith Mularski, an FBI special agent who works from offices of the National Cyber-Forensics and Training Alliance, organized crime groups around the world are engineering widespread cybercrime rings using some of the most sophisticated technology imaginable. In a 2011 *Guardian* profile about Mularski, author Dominic Rushe wrote: "And it is serious criminals who are doing it. Traditional organized-crime activities such as racketeering or prostitution are not going away, Mularski [said], but the new generation of criminals are as excited about online growth as their legitimate business rivals."

In other words, if you're thinking of a young Matthew Broderick hacking into a government website in the movie War Games, you would be seriously mistaken.

To combat the problem, financial institutions and law enforcement agencies across the country, at all levels, recognize the need to invest in technology that allows these organizations to more quickly identify suspicious transactions and more efficiently gather information about persons of interest. As noted in the FinCEN's

Money Services Guide to Money Laundering Prevention, "Federal action to curtail money-laundering activities once focused heavily on identification and documentation of large currency transactions. More recently, anti-money-laundering efforts have focused on the use of money transfers, through both the bank and non-bank money transfer systems, and other means of moving funds. Today, as money launderers become more sophisticated, all types of financial transactions are facing greater scrutiny."

"The biggest barrier in the fight against money laundering is the data," added Thomas. "It's a Big Data problem. There are literally trillions of transactions going through the world's financial systems. That's where technology will help in this fight."

REUTERS/Kacper Pempel

Searches through county courthouses for public records have been replaced with powerful data-mining tools that allow law enforcement agencies to drill down deeper and more broadly to obtain information about suspicious criminal activities and persons of interest. This is critical because sophisticated money launderers understand how to move many small transactions through the world's financial systems in their effort to avoid detection. Lots of small transactions, however, add up to a mountain of data through which to sort.

"As a financial analyst with the National White Collar Crime Center, and formerly with the Henrico County [Virginia] Police Department, it would take me months to obtain and sift through paper records" said Williamson. "Today, with tools like CLEAR, we have the means to obtain volumes of data within minutes or hours. And, we have the power to sort through it to get to the information that really matters."

David Thomas (no relation to Jason Thomas) recommends that financial institutions consider using general profiling technology to improve their understanding of money launderers, and the approaches to stopping them, in his 2012 white paper "The Practice of Profiling," for Thomson Reuters Accelus™ group.

"Some law enforcement agencies have analyzed the use of money launderers in closed cases in order to identify common profiles, such as criminal associates; ethnic, familial, geographic roots; preferences in methods; and so on. The results are used to populate general intelligence databases, sometimes to generate fresh investigations to use in court cases as evidence of association."

While smaller local and county agencies may have the technology they need to identify and investigate money laundering and related cybercrimes, they do not always have the training required to make full use of that technology, noted Williamson. This lack of training is due to several reasons.

"One of the issues is the cost associated with specialized training," Williamson said. "It often costs between $3,000 and $5,000 for a week of technology training, and then additional funds are needed to purchase the software and tools required to successfully carry out ongoing investigations."

To assist law enforcement agencies that struggle with finding the funds for anti-money-laundering training, the NW3C offers free training to member agencies across the country. Last year, NW3C provided training to more than 6,500 sworn personnel (and more than 50,000 sworn personnel since 1996). In addition, NW3C assists law enforcement agencies by offering no-cost investigative tools such as Microsoft® COFEE (Computer Online Forensic Evidence Extractor); PerpHound™ (a forensic tool that enables investigators to analyze call detail records from cell phone companies); and NW3C TUX4N6™ (a bootable CD that allows law enforcement to preview a hard drive without writing to or altering data on the system).

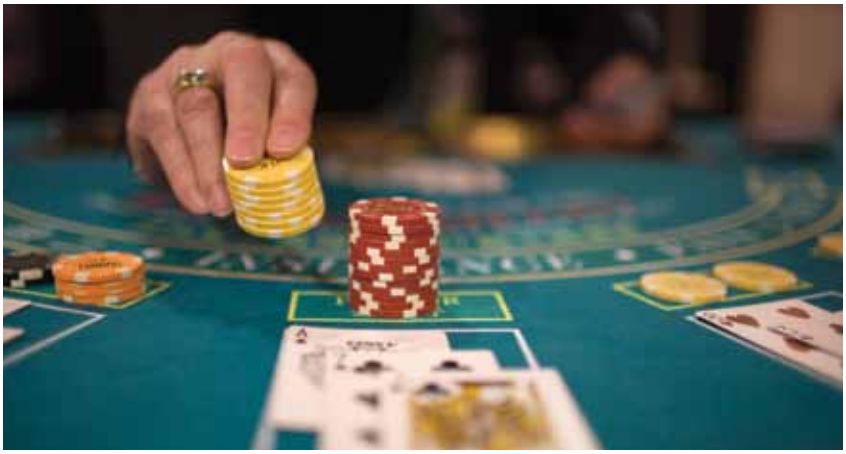
CHALLENGES AND OPPORTUNITIES

In the world of money laundering, the battle between criminals and financial institutions and law enforcement agencies looks like a chess game. A move is met by a countermove. One side attempts to sidestep the other. As traps are laid and sprung, the opponent learns and develops new skills and strategies.

Through regulation and the desire to avoid losing the trust of its customers, banks are investing heavily in technology to monitor transactions and gain knowledge about customers. Likewise, federal law enforcement agencies and, to some extent, state and local law enforcement agencies, are complementing those investments with predictive policing and legal investigation technology that enable them to see beyond individuals to entire networks and businesses that may be involved in money laundering and other criminal activity.

If financial systems continue to increase the controls on their transaction systems, criminal organizations will, in a reaction equal to or greater than those tighter controls, seek alternative systems to launder their cash. However, it seems that many of these alternative systems don't offer the efficiency in processing large amounts of cash as traditional or online banks offer.

And those that come close to offering the efficiency of banks, such as casinos, are evolving in their anti-money-laundering controls. In late January 2013, the Las Vegas Sands Corp. announced that it had ceased international money transfers and was overhauling its compliance procedures, according to the *Wall Street Journal* (Kate O'Keefe, Jan. 24, 2013), as part of its negotiations with federal authorities to resolve allegations of money laundering. The FATF has called for additional anti-money-laundering controls for casinos, especially in known money-laundering hotspots such as the Philippines and Macau (which has become an offshore haven for Chinese money launderers).



REUTERS/Victor Fraile

Processing cash with online games or with digital currency may offer alternatives at this time, but they come with risks. In the 2007 case of E-Gold Ltd., a digital currency provider that offered an anonymous-based payment system backed by gold and silver reserves, the U.S. government demonstrated its willingness to move against a digital-currency issuer that it suspected, and proved in court, was being used as a worldwide vehicle of money launderers. The E-Gold case demonstrated that criminals are constantly looking for sources to store and move money, but in the end, they still want their money in a trusted, widely used, sovereign-based currency like U.S. dollars or euros.

If currency is the critical point in the back–and-forth battle between criminal elements and law enforcement, it would seem that criminal elements would swarm to safer digital currencies as they're introduced in the years to come. Sweden, the first country to introduce paper banknotes in 1661, is moving toward a cashless society. And last year (August 2012), the Royal Bank of Canada introduced the MintChip, the digital equivalent of its paper currency.

It stands to reason that if sovereign governments move toward issuing digital currency, then competition may overwhelm private

currency such as Bitcoin or future currencies. However, if sovereign currencies could potentially be traced for anti-money laundering or even tax purposes, the reality is, based on history, the market for private cryptocurrencies will continue to exist and grow.

The shift within these private cryptocurrencies then moves to maintaining anonymity between individuals and organizations. For example, if drug dealers are open to accepting digital currency in payment for a bag of heroin through a cellphone or via a website, both parties, the dealer and the buyer, would like to ensure their online anonymity, even if digital currency could potentially be tracked based on encrypted coding.

From that viewpoint, the biggest hurdle regulators and law enforcement may face is the growing body of privacy laws created to meet the demands of a digital world. If a drug trafficker chooses to go around controlled environments such as banks, which are obligated to "know your customer," according to David W. Blass, chief counsel at the Division of Trading and Markets of the Securities and Exchange Commission (SEC) in his March 2012 *Securities Technology Monitor* article, "Past and Future of Fighting Money Laundering," at what point can state or federal governments intervene to discover the online identities of individuals?

As financial institutions, government agencies and law enforcement grapple with how to fight money laundering effectively and efficiently, other related issues may emerge in the years ahead as organized crime groups grow more sophisticated in moving money in a digital world. These issues include:

Education – NW3C's Williamson believes that many law enforcement agencies are unprepared to deal with the new reality of cybercrime and the sophisticated methods organized-crime groups use for money laundering. Extensive training and education at all levels are needed, including small-town and rural county police departments. Training can help overcome apprehensions

of confronting new technology and the overwhelming amounts of data that are typical in money-laundering cases.

Red-flagging – Along similar lines, banks and other financial institutions need to continue to invest in Red Flags training for front-line personnel who handle funds or open accounts to recognize the signs of money laundering on a day-to-day basis. As noted by Jennifer Shasky Calvery, director of FinCEN, in her Feb. 27, 2013, remarks to the Securities Industry and Financial Markets Association (SIFMA), "while FinCEN may be designing the defense, it is the financial institutions that must build and execute it on a daily basis."

Alternative currencies – According to the FBI, if Bitcoin and other digital currencies continue to grow in popularity, they will attract more elements of the criminal underground that want to avoid traditional financial systems to transfer money. As long as Bitcoin can continue to maintain its anonymity, while at the same time becoming more mainstream (easy to acquire through simple, real-money transfers), law enforcement will find it increasingly difficult to trace Bitcoin exchanges.

Unpredictable role of hacktivists – The activities of Anonymous and other hacktivist movements within the Deep Web represent a wild card in money-laundering monitoring and investigation, based on other incidents and issues in which Anonymous has inserted itself. At some point, will these groups intervene to assist law enforcement in identifying criminal groups, or based on their belief systems, will they thwart law enforcement agencies in the name of privacy freedom?

Sharing information – To fight the ongoing threat of money laundering and terrorism financing, it's critical for federal, state and local law enforcement agencies and financial institutions to

partner and work closely together. Sharing information quickly and efficiently is the key to stopping the rise in money laundering. Government agencies will need to continue to invest in information technology to increase access. FinCEN Query, which launched in September 2012, is a step in the right direction, according to Calvery. This technology gives law enforcement access to BSA data for the past 11 years. To close the loop, law enforcement agencies must invest in investigative technology that allows them to drill deep and broadly into this data to optimize their investigative systems.

Privacy rights – Law enforcement agencies and elected officials can expect to receive significant challenges from privacy-rights advocates who are concerned about how far law enforcement can go in online surveillance and in demanding data from Internet providers in their pursuit of criminal organizations and money launderers.

Adequately budgeting for technology and people – To fight money laundering effectively, it's critical that law enforcement and corporate risk officers have the firepower to monitor and investigate suspicious activity. However, when many law enforcement agencies face mounting pressure to maintain or cut existing budgets, agencies may be forced to compromise on investments in technology and personnel who are specifically trained to use technology to investigate money-laundering incidents.

Avoid denial – SEC's Blass noted in a recent *Security Technology Monitor* article that it's not enough for financial institutions to put anti-money-laundering programs in place. Individuals must be trained to come forward when they suspect suspicious behavior, even if that means the potential loss of a profitable account.

MILESTONES IN THE FIGHT ON MONEY LAUNDERING

1970 – The Bank Secrecy Act (BSA) becomes law and leads to the creation of a reporting system for financial transactions exceeding $10,000 as a step in monitoring the flow of criminally obtained proceeds. Source: Westlaw.

1970 – The Racketeer Influenced and Corrupt Organizations (RICO) Act identifies money laundering as a predicate offense that represents racketeering activity. Source: Westlaw.

1986 – The Money Laundering Control Act amends the BSA, and identifies money-laundering as a federal felony. Source: Westlaw.

1988 – The Anti-Drug Abuse Act raises penalties and sanctions for money laundering crimes, amending money laundering provisions tied to attempted tax evasion and filing false tax returns. Source: Westlaw.

1989 – The International Monetary Fund (IMF) forms the Financial Action Task Force on Money Laundering (FATF), a 36-member international governmental body established by the G-7 Summit in Paris to develop a worldwide standard for anti-money laundering and combating the financing of terrorism (CFT).

1992 – The Annunzio-Wylie Anti-Money Laundering Act strengthens the BSA, requiring verification and recordkeeping of wire transfers. Source: Westlaw.

1994 – The Money Laundering Suppression Act requires banks to develop anti-money-laundering examination procedures and requires the registration of money services businesses (MSBs). The act makes it a federal crime to operate an unregistered MSB.

1998 – The Money Laundering and Financial Crimes Strategy Act requires the Secretary of the Treasury to implement a national plan to address money laundering. Source: Westlaw.

2001 – The USA Patriot Act establishes new rules to prevent, detect and prosecute terrorism and international money laundering through businesses and financial institutions. The Act requires banks to monitor transactions and increases both civil and criminal penalties for money laundering. Source: Westlaw.

2002 – U.S. Department of Treasury issues the National Money Laundering Strategy focused on addressing the role of money laundering in the war on terrorism.

2004 – The Bank Secrecy Act (BSA) was amended with the passage of the Intelligence Reform and Terrorism Prevention Act of 2004, which establishes regulations requiring certain financial institutions to report cross-border electronic transmittals of funds. Source: Westlaw.

2005 – The Drug Enforcement Agency (DEA) completes Operation Mallorca, a milestone money-laundering investigation of the Colombian Black Market Peso Exchange. The operation led to the arrests of 36 individuals, the seizure of $7.2 million, more than 21,500 pounds of marijuana, 947 kilograms of cocaine and 7 kilograms of heroin. Source: NW3C.

SOURCES

Interview, Williamson, Cindy, CFE, CAMS, enforcement analyst III, National White Collar Crime Center (NW3C), April 2013.

"Fitch: More Banks Facing U.S. Anti-Money Laundering Scrutiny," Fitch (news release), April 5, 2013.

"The IMF and the Fight Against Money Laundering and the Financing of Terrorism," International Monetary Fund, March 31, 2013.

Interview, Vazquez, Jason, senior vice president and BSA/AML compliance officer, Provident Bank, March 2013.

Interview, Thomas, Jason, senior strategic analyst, Thomson Reuters, March 2013.

Interview, Sagona-Stophel, Katherine, government analyst, Thomson Reuters, March 2013.

"Web Money Gets Laundering Rule," Sparshott, Jeffrey, *Wall Street Journal*, March 21, 2013.

"Eye on Digital Currency: Amazon Sellers Get Bitcoin Option; Hackers Steal Bitcoins," *Digital Transactions*, March 11, 2013.

"History of Anti-Money Laundering Laws," Financial Crimes Enforcement Network, United States Department of Treasury, 2013.

"Bitcoin Looks Primed for Money Laundering," Sanati, Cyrus, *Fortune.com/CNNMoney.com*, Dec. 18, 2012.

"HSBC to pay $1.9 billion U.S. fine in money-laundering case," Wiswanatha, Aruna and Wolf, Brett, Reuters.com, Dec. 11, 2012.

"Welcome to the Deep Web: The Internet's Dark and Scary Underbelly," Albarracin, Pablo and Holloway, Christopher, *Worldcrunch.com*, Nov. 17, 2012.

"U.S. Treasury to Lead Review of Anti-Money Laundering Rules," Wolf, Brett, Reuters, Nov. 12, 2012.

"Minting the Digital Currency of the Future," Wolman, David, *Wired.com*, May 7, 2012.

"Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity," *Intelligence Assessment*, Federal Bureau of Investigation, April 24, 2012.

"Money Laundering and Asset Forfeiture: Taking the Profit Out of Crime," Leff, Douglas, J.D., FBI *Law Enforcement Bulletin*, April 2012.

"New Payment Methods and Financial Crimes Risk," Thomas, David, Thomson Reuters Accelus, Jan. 2012.

"General Questions: What Is Money Laundering?" Financial Action Task Force (FATF), 2012.

"The Practice of Profiling, Part 3," Thomas, David, Thomson Reuters Accelus, 2012.

"Examples of Money Laundering Investigations, Fiscal Year 2011," Internal Revenue Service (IRS), 2011.

"Alternative Currencies Grow in Popularity," Schwartz, Judith D., *TIME Magazine*, Dec. 14, 2008.

"Money Laundering," National White Collar Crime Center, May 2006.

LEARN MORE

For more information about CLEAR, visit clear.thomsonreuters.com.

ABOUT THOMSON REUTERS

Thomson Reuters is the world's leading source of intelligent information for businesses and professionals. We combine industry expertise with innovative technology to deliver critical information to leading decision makers in the financial and risk, legal, tax and accounting, intellectual property and science and media markets, powered by the world's most trusted news organization. With headquarters in New York and major operations in London and Eagan, Minnesota, Thomson Reuters employs approximately 60,000 people and operates in over 100 countries. For more information, go to thomsonreuters.com.

ABOUT FRAUD PREVENTION AND INVESTIGATION SOLUTIONS FROM THOMSON REUTERS

For professionals seeking information about individuals and companies, Fraud Prevention and Investigation Solutions from Thomson Reuters offer public and proprietary records with tools for fast, immediately usable results.

CLEAR® is a next-generation online investigative platform from Thomson Reuters with a robust collection of both public and proprietary records to make investigative work easier, such as: real-time incarceration and arrest records, expanded criminal coverage, work affiliations data and alerting functionality. Web Analytics, a feature within CLEAR, instantly searches and categorizes social network sites, blogs, news sites and watch lists within the Deep Web, while you run your public records search. Link charts and Google Maps™ allow you to visualize data connections. CLEAR offers various platform options designed and developed for you to meet your specific investigative needs.

Thomson Reuters public and proprietary records can be integrated into your systems or searched via online platforms designed around how you conduct your investigation. Large-volume batch capabilities and batch alerting functionality save time and provide you with the information you need in a usable format.

For questions on purchasing CLEAR or more product information, please contact us at 1.800.262.0602 or clear@thomsonreuters.com.

THOMSON REUTERS™

THOMSON REUTERS™