Dirty digital dollars

Originally published in Fraud Magazine (July/August 2016), a publication of the Association of Certified Fraud Examiners, Austin, TX, © 2016 John Bandler and ACFE.

Money-laundering case shows how cybercriminals used digital currencyJuly/August 2016

By **John Bandler, Esq., CFE, CISSP, GCIH**

Cybercrime and identity theft have evolved into a sophisticated global economy. Perpetrators use the anonymity provided by digital currency and the internet to hide themselves, their criminal acts and their gains. This nine-year cybercrime investigation case illustrates one of the few law enforcement successes in fighting these crimes.

In early 2005, I was a junior prosecutor at the New York County District Attorney's Office. In addition to my usual duties prosecuting street crimes, I was assigned to the identity theft unit, which famed DA Robert M. Morgenthau had recently formed. I received a complaint, which alleged that a victim's credit card had been used without authorization at an online retailer to ship merchandise to a Manhattan address.

My fellow investigators and I followed the money trail of the online participants in this theft, and we found ourselves looking at a digital currency exchanger in Manhattan called Western Express International Inc.

By outward appearances, Western Express was acting as a check casher and money transmitter for a Russian-speaking clientele based in Eastern Europe but earning money within the U.S. However, the company wasn't licensed by the state to cash checks or transmit money, so we successfully obtained an indictment against them for these crimes in 2006.

Our analysis of computers and records seized from the company revealed that many of their digital currency exchange customers were elite cybercriminals and identity thieves, and the company knowingly was facilitating their crimes and laundering their illegal profits.

Ultimately, Western Express and some of their customers were then indicted again for a variety of charges, including money laundering (of digital currency) and charges related to trafficking in stolen credit card data and other stolen personally identifiable information (PII).

Let's recount the detailed investigation that led to all these indictments and convictions.

They didn't know their customers and didn't care

When we were investigating the initial report of credit card fraud, the online retailer said that other fraudulent orders were placed with additional credit card numbers to be shipped to the same Manhattan address. So we checked with other online merchants and quickly identified about 100 fraud orders placed with that same "ship to" address.

If we're to understand digital currency money laundering, we must recognize its global nature."
The fraud orders weren't being shipped to a master identity thief but merely to a participant in a reselling scheme — a variant on the reshipping scheme. In a reshipping scheme, a cybercriminal recruits a "drop" (e.g. a sucker) to unwittingly receive merchandise purchased with stolen credit card account information and then reship it to an address controlled by the cybercriminal — typically in another country. Here, the individual at the Manhattan address receiving the fraudulently purchased shipments resold them online for a profit.

The reseller was using Egold digital currency to pay the fraudster who was then moving some of that Egold through Western Express. At that time I knew almost nothing about Egold, digital currency, cybercrime, carders, Internet Protocol (IP) addresses and money laundering.

Egold was popular with cybercriminals, identity thieves, child pornographers, Ponzi schemers and those who believed in the "gold standard" and not in government-backed currencies. Egold also was at the forefront of a digital currency movement that has become more mainstream.

About $4 million of Western Express' business over four years consisted of receiving and depositing checks on behalf of their customers and transmitting those funds overseas. However, they were unlicensed to do that, so they violated New York's banking laws. We had evidence for indictment No. 1.

Money transmitting laws are the first steps toward trying to keep our financial systems clean and preventing them from becoming conduits for illicit activity and proceeds. Individuals and companies who move money are supposed to be regulated and must follow anti-money laundering procedures that include know-your-customer protocols and reporting of suspicious activity to the government.

Western Express' transgressions demonstrated why those laws are important. The company didn't take any steps to know its customers but instead allowed them to cash checks made out to obviously fictitious names. Western Express would then remit the money to the customer as he or she chose — such as to overseas accounts or via digital currency or Western Union. Western Express used this low-tech payment method to

allow those living overseas to anonymously receive funds processed through the U.S. banking system.

Western Express also offered a variety of other services, many of which it designed to allow customers to anonymously transfer or spend funds. The company issued money orders, facilitated payments through other money transmitters and resold gift cards.

Western Express' services were expensive for traditional financial services, such as check cashing, money orders, gift cards or digital currency exchange. But customers were willing to pay a high premium for anonymity.

So when you're evaluating a customer base, review the costs of services and ease of use. Many advocates say businesses save money and time when they use digital currencies compared with traditional bank wires or Western Union or MoneyGram. They're correct to a point. But you must evaluate the full cost of using a digital currency because it costs money to cash in and to cash out. For example, Western Express customers based in the U.S. paid about a 5 percent commission to convert cash (e.g. money orders) into digital currency, which they then used to pay overseas criminals. At the other end, overseas criminals paid a commission (sometimes to other exchangers) to convert one digital currency into another or to convert it into traditional (fiat) currency.

Moving digital currency out of a country

We spent more than a year analyzing Western Express' records to fully understand its digital currency exchange business and to prove that it was a financial hub of cybercrime data trafficking. In four years, $35 million in digital currency flowed through the corporation. To paraphrase DA Morgenthau: If any of that money was legitimate, it was probably by pure accident. The second indictment of Western Express — for money laundering and related crimes — identified about $2 million as the proceeds of criminal activity.

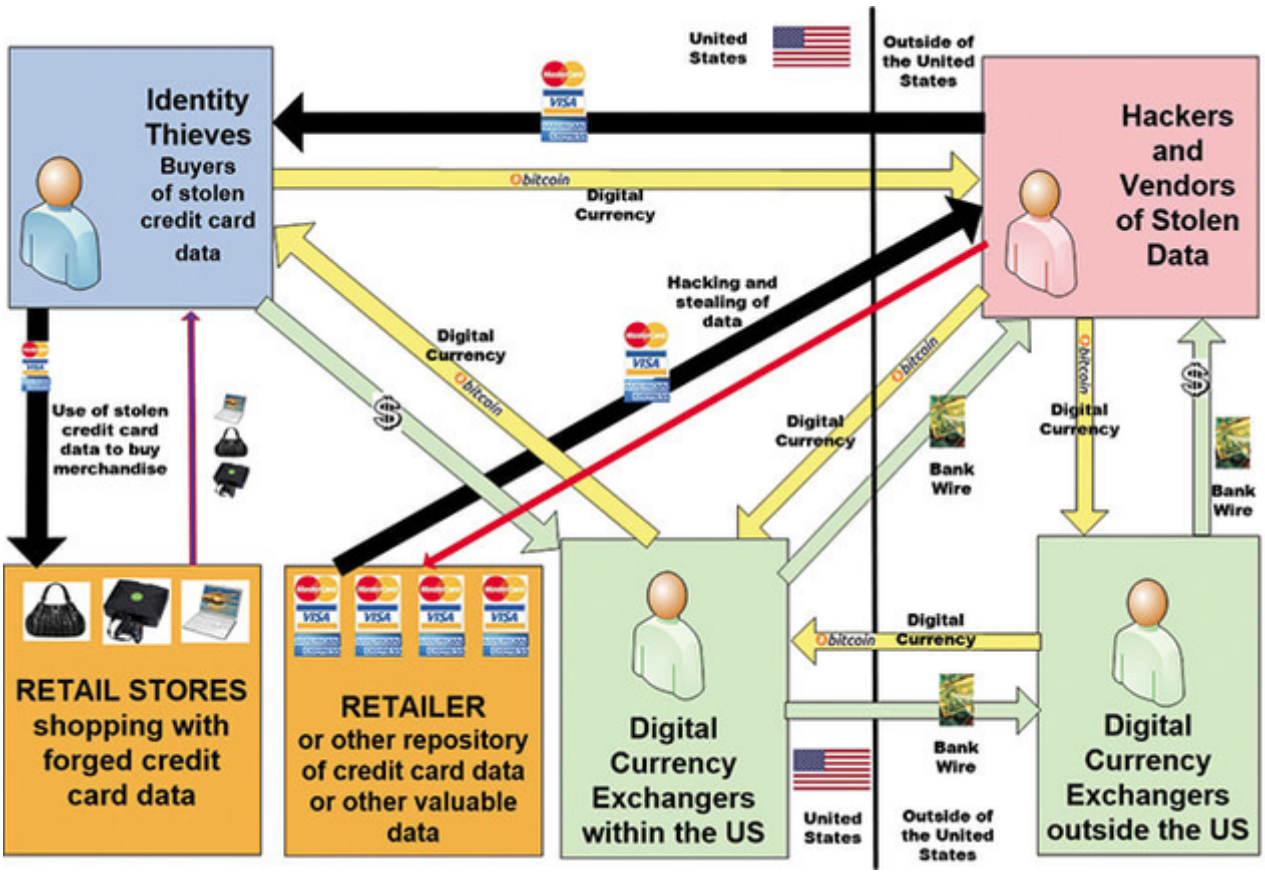

Figure: The flow of digital currency, stolen data and traditional funds.

Anti-money laundering training and procedures often focus on the risks posed by cash transactions, but the industry probably hasn't fully realized the digital currency money laundering threat. Cash is a great tool for in-person criminal transactions such as selling drugs. As the TV series "Breaking Bad" illustrated so well, successful drug dealers quickly realize they have to solve the problem of how to use their cash without violating financial regulations and raising suspicions about its source. They can't use it to buy a house, boat or car without risking some serious and unpleasant attention. They must devise methods and schemes to get cash into the financial system without detection so they can buy the things they want.

Digital currency money laundering has a slightly different flow. The criminals amass their illicit profits via cybercrime, but they still need to conceal them. They must follow several steps to convert the money into laundered proceeds that can be spent. With the emergence and popularity of bitcoin, cyberfraudsters have easier outlets through which they can launder their criminal proceeds. Critically, it's no longer essential that they first convert their illicit funds to traditional fiat currency before buying the products they want.

If we're to understand digital currency money laundering we must recognize its global nature, its resemblance to other international trade models and its interconnection with the conventional financial system. The diagram on page 28 illustrates the flow of digital currency, stolen data and traditional funds. The main takeaway is that cybercriminals outside of the U.S. regularly use methods like these to get illicit funds — generated by victimizing U.S. residents — out of the country.

Comfortable long-distant criminals indicted

The second indictment charged 18 defendants with participating in Western Express' cybercrime money laundering and data trafficking scheme. Five of these defendants were well-known international cybercriminals who resided comfortably overseas while they stole from U.S. victims.

While many in the U.S. law enforcement and financial communities doubt the effectiveness of pursuing cybercriminals acting from outside our borders, authorities had remarkable success indicting and extraditing international defendants in this case. Two defendants (Russian and Moldovan nationals) were arrested in the Czech Republic, extradited to New York and ultimately pleaded guilty in 2010.

Another defendant, Ukrainian national Egor Shevelev, was arrested while vacationing in Greece, extradited to New York and was convicted after trial in 2013. Shevelev was one of the world's most prolific vendors of stolen credit card data on the cyber black market.

The Russian and Moldovan nationals operated a sophisticated version of the reseller/reshipper scheme discussed earlier. In their triangulation scheme, they recruited partners to advertise merchandise for sale online. Once a bona fide purchaser paid for the merchandise, the cybercriminals used stolen credit card information to order the merchandise from an ecommerce site and ship it directly to the purchaser.

One of the international defendants, Dzmitry Burak, remains a fugitive on the Western Express charges and a subsequent federal indictment. He sold stolen credit card data and forged identifications (such as passports) online.

Oleg Covelin also remains a fugitive on the Western Express charges and a subsequent federal indictment. While laundering funds through Western Express, he was learning the cybercrime trade and became very good at it. As the subsequent federal indictment showed, he was an elite hacker capable of very sophisticated cybercrime.

I'm fascinated when I examine the basic transactions among cybercriminals and identity thieves, and how they communicate, pay each other and traffic stolen data. In the end, it's all about profit, and this form of crime is indeed a very profitable occupation. It also requires intelligence and patience — skills that identity thieves and cybercriminals develop and master over years through study and practice.

Though criminals carefully study ways to anonymize themselves and evade law enforcement detection, we were able to pierce their veil of anonymity in this case. Our fraud examination process involved an exhaustive review of evidence, including financial records and emails — seized with search warrants in Kiev, Ukraine; Manhattan; and New Jersey — and in web postings, paper documents, financial records, data within cell phones and computers, and chat messages.

During the pendency of the litigation, the amount of work was overwhelming, and the case seemed as though it might never end. The prospect of preparing proof for a trial of this magnitude was daunting. The jury sat through two months of testimony and evidence, including more than 50 witnesses and a mountain of paper records, electronic data and other evidence.

We brought down Western Express only because of a partnership with the U.S. Secret Service (which had spent years developing anti-cybercrime expertise); the investment my supervisors and Morgenthau made in the investigation team and me; and the hard work of analysts, investigators, special agents and many others in law enforcement and financial sectors. It was a true team effort.

Governments, banks have to crack down

Criminal justice sectors around the world are trying to combat cybercrime and identity theft, which have grown to epic proportions with varying levels of success. The theft of PII and the use of digital currencies have been a part of the cybercrime economy since the early 2000s.

Cybercriminals are bombarding individuals and corporations with ingenious types of attacks. Governments need to play larger roles in helping to protect its citizens' PII and apprehending those responsible for compromising it. Corporations also need to protect their data, customers and employees.

Good cybersecurity is important, but the solution to this problem can't lie with transforming corporations into cybersecurity fortresses that are impervious to repeated attacks and employees into cybercrime experts, who ideally are alert to endless variations of scams and social engineering schemes.

Law enforcement agencies need to do better in apprehending more cybercriminals — thus deterring those who face a minimal risk of apprehension and penalties — by thoughtfully investing in people and cases. Cybercrime prosecutors, investigators, analysts and agents take years to develop — as do cases.

Financial institutions also must do better in preventing and detecting cybercrime because they're the main

conduits through which illicit profits are both generated and transferred internationally for delivery to cybercriminals. Financial institutions can't simply rely on "minimum standard" checkboxes of regulations or account-holder contracts for due diligence to prevent fraud, theft and money laundering. Banks have to find better ways to ensure that international wires aren't simply black holes through which nothing can be recovered. They must look at the problem holistically and attempt to combat it.

We're now dealing with new crooks, digital currencies and websites. But the problem remains, and solutions are urgently needed. Success stories such as the Western Express case help show the way forward to bringing more of the world's cybercriminals to justice.

This article is an adaptation of the author's conference paper that accompanied his session at the 27th Annual ACFE Global Fraud Conference in June. — ed.

***John Bandler Esq., CFE, CISSP, GCIH**, operates a legal and consulting practice to help corporations and individuals with cybersecurity, data privacy, investigations and anti-money laundering. Bandler has 20 years of government experience, including 13 as a prosecutor at the New York County District Attorney's Office.*