INFORMATION LAW JOURNAL

A Publication of the Information Security and EDDE Committees
ABA Section of Science & Technology Law

AUTUMN 2016 VOLUME 7 ISSUE 4 EDITOR/FOUNDER: THOMAS J. SHAW, ESQ.

Cybercrime and Digital Currency

By John Bandler

Cybercrime-for-profit has become an enormous industry, and is the cause of most of our internet and information security problems. In order to combat cybercrime, we need to understand how cybercriminals are paid and how they launder their proceeds, and realize that they make heavy use of digital *Read more*

Understanding Information Security: Containing a Potential Oil Spill

By John Jorgensen and Charly Shugg

Information is a sensitive aspect of most businesses, but especially law firms. Law firm electronic information is not only about the law firm's business operations but also client information, case information, litigation strategy and status, escrow accounts and potentially sensitive client personnel information. Electronically *Read more*

The Internet of Things and Air Law: LSA Purchase Agreements

By Jacob Tewes

The proliferation of the Internet of Things ("IoT") is rapidly outpacing the tectonic evolution of common law. This phenomenon is nowhere close to new, but it continues to accelerate. A hundred years after the Wright brothers tackled their own seismic hurdle, the makers of a new breed of aircraft pushed the limits of *Read more*

Avoiding eDisaster in eDiscovery: A Canadian Perspective on Cybersecurity

By Michael Darcy and Nicholas Johnston

Earlier this year, a Russian cybercriminal named "Oleras" tried to hack into nearly 50 of the largest law firms in the United States. That same month, the Wall Street Journal reported that legal giants Cravath, Saine & Moore LLP and Weil Gotshal & Manges LLP, along with a number of unnamed firms, had all suffered data *Read more*

Cyber Security – The Indian Paradigm

By Jayesh H, Arunabh Choudhary, and Aditi Bagri

In the past decade, India has been a significant contributor to the growth of information technology, in India and abroad. This has primarily been in terms of the number of professionals working in the IT/ITeS sector who are of Indian origin and the people who keep getting added to it year on year. While globally there are *Read more*

The More Things Change, the More They Stay the Same

By Alejandro Barrientos, Alexander B. Hastings, and Edward H. Rippey

The *ILJ* recently outlined the 2015 amendments to the scope of discovery in Federal Rule of Civil Procedure 26(b)(1) and the prescription of e-discovery sanctions in Rule 37(e).[1] Those amendments have inspired hope that courts will rein in the costs of e-discovery and the unpredictability of e-discovery sanctions. *Read more*

Cybercrime and Digital Currency

By John Bandler

Cybercrime-for-profit has become an enormous industry, and is the cause of most of our internet and information security problems. In order to combat cybercrime, we need to understand how cybercriminals are paid and how they launder their proceeds, and realize that they make heavy use of digital currencies. Thus, we must understand digital currencies and other digital payment methods, and how they can be misused for criminal purposes. If you have clients that exchange digital currency, or accept digital currency as payment, then they should be aware of the risks of being used a conduit for cybercrime digital currency proceeds, so that they don't unwittingly assist the criminals in their crimes. This will help your clients mitigate reputational, regulatory, and legal risks.

When crime is done for profit, some criminals eventually become very good at what they do. They become successful, and are able to evade detection and "earn" a lot of money. They have a fascinating problem, which is how to transmit, conceal, and ultimately use their abundant illicit profits without attracting unwanted attention. That is where money laundering comes in. With enormous illicit profits come resources, and criminals have the opportunity to engage corrupt accountants, lawyers, bankers, and businesspeople to further their goals.

Crime motivated by profit presents law enforcement with significant challenges as well as significant opportunities. Though successful criminals have become good at evading detection, they also provide an extensive flow of funds that law enforcement can use to trace them. Further, their constant criminal activity provides for abundant evidence and abundant criminal charges - once law enforcement has identified the perpetrators. A single, isolated crime might be difficult or impossible to solve, but repeated criminal activities make for a lucrative prosecution target.

Based upon my time spent studying the cybercrime and identity theft economy, it is clear to me that digital currency is an important pillar of that economy. However this article is not an indictment of digital currencies. First, digital currency is not unique for being used by criminals - it could also be said that cash is an important pillar of the street crime economy, and that illicit proceeds move through conventional financial institutions every day, despite efforts to detect it. All traditional financial payment methods have been used by criminals, including cash, wire transfers, money transfers, bank accounts, payment cards, credit cards and more. Indeed, cybercriminals are adept at engineering successive bank wires through our conventional banking system, wires that eventually leave the United States and then become unrecoverable. Further, the payment method we all take for granted - the credit card - has provided cybercriminals and identity thieves with lucrative opportunities. In sum,

money laundering criminal activity has been around a long time, and it is no surprise that criminals would also use digital currencies to further their purposes.

Further, my experience with digital currencies is viewed through the lens of a former law enforcement veteran, who for twenty years focused only on crime. There is definitely room for research and analysis about what percentage of digital currency transactions are for criminal purposes, and what percentage is for legitimate purposes. That said, the indisputable fact is that digital currency has been used by criminals, and will continue to be used by criminals. The challenge is to get better at tracking and reducing their use of it. Another fact is that cybercrime-for-profit is of epidemic proportions, and law enforcement is simply not keeping up. Cybercrime is committed with impunity by actors outside of our borders. One part of our solution in combatting cybercrime will lie with stemming the flow of illegal profits out of our country. Stemming the flow of the illicit profits, even illicit profits that flow via digital currency, requires better understanding of how conventional funds are transmitted.

Thus, this article is not intended to be an indictment of digital currencies, but merely to generate awareness of the criminal risks. If the risks are managed properly, digital currencies might have great promise, and there is no reason that the status quo for conventional payment mechanisms cannot be improved upon.

What is a Digital Currency?

Digital currencies have been around since the nineties, but have only recently come into mainstream awareness with the rise of Bitcoin after 2009. Most regulators use the term "virtual currencies".[1] Personally, I feel the use of the "virtual" terminology downplays the importance of digital currencies, because the value the currencies can transfer is real, not "virtual" or pretend. However, regulators have chosen the term "virtual" because to them, it is not a "real" currency, since it was not issued by a government, like fiat currency is. In the end, the value is real, so long as people are willing to pay with it, accept it as payment, or exchange it.

Generally, a digital currency could be centralized or decentralized. Centralized means there is an entity overseeing it and administering it, and examples of this have included Egold, Liberty Reserve, WebMoney, PerfectMoney, and others. A decentralized currency doesn't have any entity overseeing it, and that's a unique concept pioneered by Bitcoin, and now emulated by many others.

The centralized or decentralized distinction becomes particularly important if the government is trying to hold someone responsible for activity within a digital currency platform. If a centralized digital currency is not complying with laws, or is knowingly facilitating criminal conduct, the entity and its officers may be held to account for compliance with licensing, regulatory, and criminal statutes. In

[1] See https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf, http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

contrast, a truly decentralized digital currency has no one that is supervising or overseeing the currency, so the government can only go after individual users or exchangers, rather than a central authority.

All digital currencies (whether centralized or decentralized) require exchangers - businesses or individuals that perform the service of exchanging digital currency for fiat currency (or vice-versa), or exchanging one digital currency for another digital currency. Sometimes the digital currency administrator acts as an exchanger as well. These exchangers may be required to be licensed, comply with anti-money laundering regulations and criminal statutes, and can be held legally accountable.

A Brief History of Digital Currency and Cybercrime

For cybercriminals and identity thieves, they don't care how the blockchain ledger technology works, how bitcoin are mined, or whether it is a good investment vehicle. Their need is to send and receive payments through the internet, using a method that is irreversible and anonymous. It should also be reliable, but that is only required for the short term, since criminals are adaptable and if the payment method stops working, they will try a different method. Digital currency companies and technology may change, but the underlying need remains the same.

Law enforcement has conducted various digital currency related prosecutions over the years. Sometimes they have targeted the centralized digital currency itself, for failing to comply with money transmitting laws or for knowingly laundering criminal proceeds.[2] Sometimes, they have targeted digital currency exchangers, who failed to comply with money transmitting laws, or for money laundering.[3] And sometimes they have targeted criminal businesses that use digital currency as a form of payment.[4]

The first main digital currency was Egold, a centralized digital currency that was created in the mid-1990s. I didn't hear about it until 2005, at which time I was a prosecutor at the New York County District Attorney's Office working under District Attorney Morgenthau. I was assigned to the newly formed Identity Theft Unit, investigating a credit card fraud identity theft case. This case led me to Egold, and Egold led me to a cybercrime investigation and prosecution that spanned nearly a decade.

Egold was innovative - it provided a method for one person to pay anyone else, anywhere in the world, and through the internet. Egold appealed to a certain demographic because it stated that all Egold was backed by real gold. Some felt that a gold backed currency is more secure and reliable than a currency backed by a government, especially since most governments have left the gold standard. But Egold

---

[2] See infra, U.S. v. Egold Ltd; et al, and U.S. v. Liberty Reserve et al.
[3] See infra, People of the State of NY vs. Western Express Int'l Inc. et al, and People of the State of NY vs. Gold Age et al.
[4] See U.S. v. Ross Ulbricht, and DOJ press release dated February 4, 2014, at https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-indictment-ross-ulbricht-creator-and-owner-silk-road.

also appealed to another demographic - cybercriminals, identity thieves, and other criminals - because it was an anonymous, instant, and irreversible internet payment method.

To use Egold, first one created an Egold account, and essentially all the account holder needed for this was a working email address. Once the Egold account was created, the account could accept incoming payments, whether it was from a customer paying for a service, or from an exchanger who the account holder had paid to fund their Egold account. When a person created their Egold account, personal information like name, address, and phone number was entered, but none of it was verified. The only information that needed to be accurate about the account holder was the email address, since this was the method used to contact the account holder. With the rise of free email accounts that meant Egold accounts were practically anonymous. Together with Egold's rise in popularity came the rise of the cybercrime and identity theft economy.

Western Express I

My credit card fraud case involving one stolen credit card account led me to fraud involving about one hundred credit accounts and about $40,000 worth of fraud, which was a big case for a junior prosecutor, but nothing like what was to come. This fraud brought me to Egold, because that's what the participants were using to pay each other, and Egold led me to Western Express International, Inc., a digital currency exchanger located in Manhattan. Among its digital currency and many other services, it engaged in an illegal check cashing and money transmitting scheme for Eastern European clientele, so we obtained an indictment for this activity in February 2006.[5] This activity was just a small part of the company's criminality, and analysis of their records, with the partnership of the United States Secret Service, resulted in a second indictment a year and a half later that would charge the company and its customers for its digital currency money laundering activities. More on that in a moment.

Gold Age

In July of 2006, another unit in the Manhattan DA's office charged Gold Age, a Brooklyn digital currency exchanger and its principals Arthur Budovsky and Vladimir Kats with operating as an unlicensed money transmitter by conducting Egold exchange.[6] They would eventually plead guilty on these charges, but then leave the United States and create their own centralized digital currency called Liberty Reserve - more on this later.

---

[5] See People of the State of NY vs. Western Express Int'l Inc. *et al*, and DA's press release of February 22, 2006, archived via https://web.archive.org/web/20060607220821/ http://www.manhattanda.org/whatsnew/index.htm.

[6] See People of the State of NY vs. Gold Age et al, and DA's press release of July 27, 2006 archived at https://web.archive.org/web/ 20071101071314/ http://www.manhattanda.org/whatsnew/press/2006-07-27.html.

Egold

In the meantime, federal authorities had been investigating Egold and criminality on that platform. Egold's corporate location was less than clear - it claimed to be a corporation of Saint Kitts and Nevis, it used attorneys in Bermuda, but its employees and computers were in Florida. This seemed designed to create ambiguity over whether Egold was subject to U.S. law, however Egold's creators and owners - who were within the U.S. - took no steps to hide their role in the company. In April of 2007, Egold and its corporate officers were charged by federal authorities with unlicensed money transmitting and conspiracy to commit money laundering.[7] This effectively put an end to Egold as a digital currency. In July of 2008, Egold pleaded guilty to conspiracy to commit money laundering and conspiracy to operate an unlicensed money transmitter.[8]

Western Express II

Following our 2006 search of the offices of Western Express, we reviewed evidence and expanded our investigation of their customers. Through our investigation of identity thieves, cybercriminals, and the trafficking of stolen data, a pattern became clear. U.S. based identity thieves sent U.S. funds to an Egold exchanger, and the Egold exchanger funded the identity thief's Egold account. Then the identity thief paid Egold to an Eastern European cybercriminal, in exchange for stolen data. This stolen data might include stolen credit card information, internet financial account login information, or complete pedigree about a victim, including name, address, date of birth, social security number, and more. Then the Eastern European cybercriminal needed to convert their Egold criminal profits into something else, and the Egold was returned to the United States, exchanged for either another digital currency, or for U.S. funds. This pattern was relatively simple. Next, there was a wholesale exchange of digital currency and U.S. funds that occurred between exchangers in various countries to "repatriate" the digital currency back to the U.S. The net result of all of this was theft from U.S. individuals, corporations, and financial institutions, and stolen profits funneled out of the U.S. And even if digital currency was a part of the transactions, the net result was conventional bank wires sent from the U.S. to Eastern Europe, a fact that seemed to be unknown to every financial institution involved.

A part of this exchange was WebMoney, another centralized digital currency that became popular in the early 2000s, and is still around today. Whereas Egold was a platform designed for English speaking users, and had a significant US customer base, WebMoney was geared towards Eastern Europeans, and at first their website was exclusively in Russian. The popularity of these two digital currencies, coupled with their distinct demographics of each, provided us with a unique view into the cybercrime and identity theft industry.

---

[7] See U.S. v. Egold Ltd; et al, and DOJ press release dated April 27, 2007 available at https://www.justice.gov/archive/opa/pr/2007/April/07_crm_301.html.

[8] See id, and DOJ press release dated July 21, 2008, available at https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html.

In August 2007 we obtained an indictment that charged Western Express and fourteen of their customers with digital currency money laundering, and trafficking in stolen data and resulting cybercrime and identity theft crimes. It took years to extradite some of the overseas cybercriminals, and the case successfully culminated in a two and a half month trial with guilty verdicts.[9] Through this long process, I was able to review hundreds of thousands of criminal transactions and interactions, payments, and communications, which helped shed light on the needs of individuals and the general economy.

Liberty Reserve

After Egold exchanger Gold Age and their founders Arthur Budovsky and Vladimir Kats pleaded guilty in New York State Court, they left the U.S. and created their own digital currency, Liberty Reserve, in Costa Rica. The Liberty Reserve platform eventually became well used by cybercriminals and identity thieves. In May of 2013, the federal government indicted Liberty Reserve, its founders and others for money laundering and unlicensed money transmission.[10] They tried to stay out of reach of U.S. law enforcement, but were unsuccessful, and ultimately pleaded guilty and were sentenced in 2016 to significant prison time.[11]

The Rise of Bitcoin

Bitcoin was created in 2009 and pioneered the technology that allows for a decentralized currency - a distributed ledger system and "blockchain technology". Though Bitcoin may be the digital currency that has received the most publicity, it is important to note it was not the first digital currency, and will not be the last, and there are many cryptocurrencies that have been created in its likeness. The names may change, the methods may change, but the uses are the same.

The ledger system is a way for a group of users to record and keep track of transactions, without one person or entity being in charge. Thus there is no central authority overseeing the transactions, but rather a ledger system that is publicly available and can be viewed by all, and modified by the group in a safe and reliable manner. It's a fascinating concept and innovation.

Bitcoin received much press and hype, and brought government and regulator attention to digital currencies. Bitcoin's distributed ledger system uses what is called "blockchain technology" to record transactions, and once transactions are recorded and verified, they are embedded into the blockchain, are available for public inspection, and are safe from tampering. This distributed ledger blockchain

---

[9] See DA's press release dated August 8, 2013, available at http://www.manhattanda.org/press-release/western-express-cybercriminals-convicted-trial-sentenced-significant-state-prison-time.

[10] See DOJ press released dated May 28, 2013, available at https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-liberty-reserve-one-world-s-largest.

[11] See DOJ press release dated May 6, 2016, available at https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years, and http://www.law360.com/articles/796315/liberty-reserve-co-founder-slapped-with-10-year-sentence.

technology has the potential for many uses outside of digital currency, since it could simplify record keeping and enable "smart contracts".[12] Bitcoin has also been seen by some as an investment vehicle.

The term "cryptocurrency" generally means it relies upon cryptographic programs and completion of mathematical problems to record and maintain a ledger of all transactions, which settles payments and determines account balances. In order to incentivize individuals to devote computer resources to verify transactions and work on the distributed ledger, bitcoin "miners" can earn bitcoin through solving the cryptographic problems.

Silk Road

Meanwhile, an online platform called "Silk Road" was created to facilitate internet transactions between buyers and sellers for contraband like drugs. It utilized an internet technology called TOR, or The Onion Router, designed to mask a person's true internet location (Internet Protocol address). Silk Road was like eBay, except the merchandise was contraband, and users paid in Bitcoin instead of PayPal. Then the contraband merchandise would then be shipped by the seller. In February of 2014, federal prosecutors charged Ross Ulbricht, the creator of Silk Road with various crimes.[13] He was eventually convicted after trial and sentenced to life in prison.[14] The Silk Road case involved the use of Bitcoin digital currency to purchase primarily brick-and-mortar contraband, so it doesn't fully fit within the economic model of cybercriminals, identity thieves, digital currency and stolen data that we are discussing here. The Silk Road website resulted in several investigations, some of which were conducted by corrupt federal agents, whose crimes were eventually discovered and they were prosecuted and sent to prison.[15]

That is just a short synopsis on some major developments in digital currency over the years. There are many cryptocurrencies similar to Bitcoin, and there are many other decentralized and centralized digital currencies. The important takeaway is that while the names may change, many of the aspects remain the same.

---

[12] For an example of the use of the blockchain technology that is not related to digital currency, see symbiont.io. For an example of the use of blockchain technology that has both a smart contract and a digital currency aspect see ethereum.org. For an example of using blockchain technology to make payments between financial institutions, see ripple.com.

[13] See U.S. v. Ross Ulbricht, and DOJ press release dated February 4, 2014, at https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-indictment-ross-ulbricht-creator-and-owner-silk-road.

[14] See DOJ press release dated May 29, 2015, available at https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison.

[15] See DOJ press release dated October 19, 2015, available at https://www.justice.gov/opa/pr/former-dea-agent-sentenced-extortion-money-laundering-and-obstruction-related-silk-road, and DOJ press release dated December 7, 2015, available at https://www.justice.gov/opa/pr/former-secret-service-agent-sentenced-71-months-scheme-related-silk-road-investigation.

Laws and Regulations

New technology and new payment methods should be viewed within the proper context. Whether or not the letter of the law appears to address certain conduct or technology, the spirit of the law is clear. And the spirit and purposes of the laws are about limiting how criminals use payment methods.

Laws regarding money transmission are the first step towards protecting our financial system from abuse by criminals and money launderers. The federal government and most states have such laws.[16] Generally speaking, money transmission laws seek to narrow the portal through which illicit funds can be transmitted. The laws are designed to ensure that only properly licensed and supervised institutions and businesses can transmit funds on behalf of customers. These licensed and supervised institutions must have proper anti-money laundering procedures, and follow reporting requirements, and if they fall short, they can be penalized and their license revoked. If an unlicensed money transmitter sends funds, they have committed a crime, and can be prosecuted, even if there is no proof that the funds themselves are related to nefarious conduct.

Licenses, regulation, and supervision also apply to all parts of the financial system. This means that financial institutions devote considerable resources to fight money laundering, and if they fall short, the penalties could be significant fines, and even loss of license, and being put completely out of business. This means that thousands of people and billions of dollars are devoted towards anti-money laundering efforts.

Money laundering laws are the next step in protecting our financial system from abuse, and they criminalize the knowing transmission or concealment of criminal proceeds.[17] Thus, criminal penalties, including jail, can attach for individuals who knowingly transmit criminal proceeds. It is a much higher proof threshold than money transmission, because it requires proof that the funds are dirty, and proof that the person knew the funds were dirty.

The spirit of these laws have been clear, but their applicability to digital currency was murky for some time. In 2013, the U.S. Government made clear that digital currency exchangers needed to register as money service businesses.[18] In 2014, New York State's Department of Financial Services conducted hearings and solicited opinions on how the state should treat bitcoin and bitcoin exchangers. They ultimately issued a regulation requiring licensing of "Virtual Currency Business Activity", or a "bitlicense" as New York nicknamed it.[19] It became the first state to create a specific digital currency regulation.

---

[16] See e.g. 18 U.S.C. § 1960, New York State Banking Law Article 13-B, § 640 et seq.

[17] See e.g. 18 U.S.C. §§ 1956 and 1957 and New York State Penal Law § 470.00 et seq.

[18] See FinCEN guidance FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, March 18, 2013), available at https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf, FIN-2014-R012, Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System, October 27, 2014, available at https://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R012.pdf.

[19] See 23 NYCRR Part 200, http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf, http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework_faq.htm.

Most states have money transmitting laws, and they are evolving regarding how digital currency exchangers fit in to that scenario. There is also an effort to standardize their laws.[20] Indeed, even after New York's "bitlicense", there is still ambiguity as to how the "bitlicense" meshes with the money transmitter requirement.[21]

Given the above, it is no surprise that laws have evolved in the last ten years, and will continue to evolve. Regulators and prosecutors may try to adapt existing laws to new fact patterns, and sometimes they are successful, sometimes not. If digital currency users understand the spirit of the money transmitting laws, and understand how digital currency can be misused by criminals, they are in a better position to protect themselves from being used to facilitate criminal activity.

For example, many current regulations carve out a loophole for businesses that simply accept digital currency as a form of payment.[22] Were an individual or business to blindly rely upon such a loophole, and blindly engage with anonymous customers who have seemingly endless supplies of digital currency, they might find themselves in an unfortunate position facing reputational, regulatory, or legal risk. In other words, the digital currency sector and private sector should police itself, and take the lead in identifying criminal conduct, and not wait for government to lead the way.

The Cybercrime Economy and Digital Currency

Digital currency fills a need in the cybercrime and identity theft economy because it allows for payment though the internet instantly, irreversibly, and anonymously. Digital currency advocates might dispute that payments are in fact anonymous, but all should agree that criminals will seek and use a method that provides measures of anonymity.

Cybercrime-for-profit is a new business model. Traditional organized crime was based upon a face-to-face interaction, whether it was drugs, extortion, prostitution, or loansharking. This brick-and-mortar interaction works well with cash payment, and thus cash money laundering techniques were born, designed to integrate and disguise this dirty cash as legitimate income. With this face-to-face interaction, the participants meet each other, and may get to know each other. There is a code among the participants (e.g. no informing) which can be enforced physically if necessary, which helps prevent law enforcement from learning about their activities.

Cybercrime-for-profit relies upon crimes committed through the internet, and there is no need for the participants to get to know each other, other than by online nickname and reputation. Indeed, it is

---

[20] See e.g. National Conference of Committees on Uniform State Laws, Draft Regulation of Virtual Currency Business Act, Feb. 2016, available at http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/2016feb_RVCBA_Mtg%20Draft.pdf.

[21] For example, the NYSDFS website states, "Depending on the specific business activities in which they are engaged some companies may need both a money transmitter license and a BitLicense." http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework_faq.htm

[22] See id.

dangerous to let others know you, because the damage that participants can do to another is "out" someone and disclose their true identity, thus exposing them to law enforcement attention. Thus, cybercriminals and identity thieves work in anonymity, even if they have business relationships that are ongoing. Cybercrime crosses physical boundaries, and it is no longer necessary for a criminal to have a physical presence in the neighborhood where they commit crime. In fact, it is better to reside outside the U.S., make lucrative profits by committing crimes against individuals and businesses in the U.S., and do so with little fear of detection or apprehension.

A cybercriminal in another country needs to get paid, and digital currency is perfect for this. The cybercrime industry is well developed and specialized, each participant can offer a particular service, and digital currency allows each participant to get paid anonymously and instantly. The best illustration of this is the relationship between hackers and identity thieves, which I simplify here for discussion. Suppose there is an enormous data breach of millions of U.S. victims' personal information or credit card information. The hackers who conducted this breach are likely safely in another country, and have covered their tracks well so that law enforcement attempting to solve this single breach in isolation will have little success. These hackers then need to sell the data, and who better to sell it to then identity thieves in the U.S? After all, the best place to impersonate a U.S. victim is within the U.S. That stolen credit card is best used in the victim's home country and city. Thus, thousands of identity thieves need a way to anonymously pay an anonymous cybercriminal for stolen data, and digital currency is perfect for that. Once the digital currency is paid via the internet, the stolen data can be delivered via the internet.

During my examination of cybercrime and identity theft digital currency transactions several things became clear. First, criminals were paying a premium in fees and time for the anonymity of the digital currencies they used. There were traditional payment methods that would have been simpler and cheaper to use, but criminals chose more complicated and expensive payment methods that protected their anonymity. Second, identity thieves in the U.S. were paying cybercriminals in Eastern Europe for stolen, hacked data, which was then used to commit identity theft. Relationships developed that lasted years, even though the individuals did not know each other's true identity. Third, at that time, each demographic had their own digital currency needs. For U.S. identity thieves, they needed to purchase digital currency so they could pay the cybercriminals in Eastern Europe. The cybercriminals in Eastern Europe needed to exchange (launder) the voluminous digital currency they received as payment for the stolen data. Thus, digital currency was repatriated to the United States. All of this required use of the conventional financial system, yet the conventional financial system seemed totally unaware that it was happening.

During the 2000's, it was essentially impossible to spend digital currency for brick-and-mortar merchandise. The rise of popularity of Bitcoin today has changed that. Now, major businesses are accepting digital currency as payment for merchandise. That presents an opportunity for the digital

currency money launderer, and a risk for the business. The business should not simply put their head in the sand.

The analogy of cash money laundering is appropriate. Successful organized street crime organizations might earn millions of dollars in cash, and they need to launder it. Government has tried to choke the entry of dirty cash into the system, thus financial institutions must report large cash deposits, as do jewelers, car dealers, casinos, and others. Still, cash money launderers develop methods to integrate their cash into the financial system without detection, which might include buying businesses or partnering with corrupt businesses.

Digital currency is the same but different. Successful cybercriminals earn millions of dollars in digital currency which needs to be laundered. Although cash can be stored in a mattress or storage locker indefinitely, digital currency is less reliable, and needs to be exchanged into something more stable - they do not want to hold it. In the end, a successful cybercriminal wants all the trappings of a successful street criminal, nice clothes, car, boat, house, and spending money. They will be creative in finding ways to launder their digital currency, just like other criminals are creative in laundering cash.

Conclusion

Digital currency is still evolving, its usage is still not understood fully by many, and government's view towards it is also still evolving. Government is rarely on the forefront, and often is reactive. This reaction time is further delayed, because even if law enforcement observes criminal conduct today, it could be a year or more before a case is brought, and a year or more before that case is resolved. Thus, it is not enough to examine the past cases, but one should examine the principles, and extrapolate for the future.

A business accepting or dealing in digital currency should look towards the spirit of money transmitting and money laundering laws, and look towards reputational risks and long term business needs. This requires an honest analysis of who their customers are, and where the money is coming from, and going to.

A financial institution should also be aware that just because they think none of their customers are involved in digital currency exchange, it is still possible that their systems are being used for something related to digital currency. As the Western Express investigation revealed, millions of dollars were sent via conventional bank wires, and the banks apparently had no idea that it was connected to digital currency exchange. Digital currency requires the use of the conventional financial system, and there remains a lot that financial institutions can do to make digital currency exchange less opaque.

Cybercrime and identity theft is a problem with a clear root cause and motive - profit. Much of the profit flows via digital currency. If we can better understand digital currency, and who uses it, we can help stem the crime, and identify the perpetrators.

John Bandler *founded a legal and consulting practice to bring his experience to the private sector to help corporations and individuals with cybersecurity, data privacy, investigations, and anti-money laundering. John has 20 years of government experience, including thirteen as a prosecutor at the New York County District Attorney's Office, and eight as a Trooper with the New York State Police. He gained unique insights into cybercrime, cybercrime intelligence, digital currency money laundering, and identity theft, and also prosecuted a wide variety of cases from inception through resolution, ranging from global cybercrime data trafficking and money laundering to violent street crime.*

John served as a State Trooper for eight years in one of New York State's busiest stations. He was also a commissioned U.S. Army officer, serving in infantry and military intelligence reserve units. He is licensed to practice law in NY, CT, and DC, and holds various professional certifications in fraud investigation, information security, privacy, anti-money laundering, and information technology, including CISSP, GCIH, GCCC, CAMS, CFE, CIPP/US, Cloud +, Network +, and A +.