People v. Western Express et al. was a groundbreaking investigation and criminal prosecution involving digital currency money laundering and payments to facilitate cybercrime and identity theft. A digital currency exchanger located in Manhattan was indicted, as were many of their criminal customers, who included a vendor of stolen data from Ukraine; other Eastern European cybercriminals, hackers and identity thieves; and identity thieves within the United States. Sophisticated investigative and analytical techniques were used to bring these defendants to justice, in a case that culminated with a two and half month trial. This session will explore this case study of a groundbreaking cybercrime investigation from beginning to end.

JOHN BANDLER, CFE, CISSP, CAMS, CIPP/US
Founder/Owner
Bandler Group LLC

John Bandler founded a legal and consulting practice to bring his experience to the private sector to help corporations with cybersecurity, data privacy, investigations and anti-money laundering. In 2002, he was hired by the legendary Robert M. Morgenthau as a prosecutor at the New York County District Attorney’s Office, where he served until 2015. 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.
Cybercrime and identity theft are significant criminal and financial threats to our country and have evolved into a sophisticated global economy. Within the last few years, we have repeatedly heard media coverage about certain aspects of cybercrime like digital currencies (especially Bitcoin) and large retail data breaches. However, the theft of personal data and the use of digital currencies have been a part of the cybercrime economy since the early 2000s.

Cybercrime and identity theft have reached epic proportions and are difficult to combat. The crimes traverse the nation and the world. The perpetrators use the anonymity of the Internet to hide themselves, their criminal acts, and their ill-gotten gains. This case study illustrates one of the few law enforcement successes of fighting this crime. All the lessons of this case remain valid today, though the names of the players have changed.

This presentation will cover:
- How criminals traffic in stolen data
- How criminals use anonymity techniques and how to unmask them
- How criminals use digital currencies to pay each other, launder their criminal proceeds, and how to track these financial activities
- How a successful global investigation occurred, starting with local identity theft and culminating with international extraditions of major cybercriminals
- How a cybercrime investigation and trial unfolds

Cybercrime for profit is a fascinating area for many reasons. It is international in scope, highly lucrative, and relatively risk-free. Successful cybercriminals routinely supply and rely on the black market of stolen identity
information. Because cybercrime is almost exclusively conducted online, it requires participants to maintain anonymity while simultaneously establishing long-term business relationships. The ability to hide in the Internet and the risk-free nature of the business means that the maxim “If at first you don’t succeed, try, try, again” applies. A rookie criminal is free to try a cyber fraud, and if they fail, they can try it again another way. Unlike crime in the brick-and-mortar world, criminals don’t have to worry about being caught.

Digital currency (sometimes called virtual currency, a popular example of which is Bitcoin) allows cybercriminals to pay each other instantly via the Internet and with anonymity. Digital currency is the medium of choice for anything nefarious on the Internet. Whenever criminals interact with each other, there is a considerable amount of mistrust. Consider the analogy of a street transaction involving drugs or guns in which cash is king. When the participants meet in person and decide to exchange a product (drugs) for payment (cash), they want the transaction to be final once the exchange is made and they part ways. Can you imagine if drug dealers were worried about being paid with a forged check, stolen credit card, or if the payment were traceable by law enforcement? No, they would never conduct a drug sale on those terms. Similarly, when criminals interact on the Internet, for example, to purchase stolen credit card data or stolen personal information (name, DOB, SSN, etc.), they want the transaction to be done instantly and irreversibly, and hopefully, untraceably. Cybercriminals also don’t want to be defrauded by other cybercriminals, who make their living with forgery and identity theft.

Digital currency fulfills all the cybercriminal’s needs for anonymity and finality of payment. Remember that the
primary use of any digital currency is as an Internet payment method. That’s it. So don’t be distracted by some of the intricacies of a cryptocurrency like Bitcoin, such as the blockchain technology “mining” of Bitcoin; Bitcoin investment strategies; or all the other things about Bitcoin that make it seem both interesting and confusing. Most people, including cybercriminals, are using a digital currency simply to pay someone on the Internet. So long as it works, and they trust it to work and they feel they won’t be detected, they will use it.

The cybercrime economy has many participants who interact with one another to further their criminal purposes. Some players are U.S.-based thieves who “earn” their living using stolen identity information to carry out a variety of fraud schemes. Their fraud activities require a steady supply of personal information with which to steal money, whether it is credit card account data, other financial account information, or victim names, birth dates, Social Security numbers, and other personal identifying information. Other cybercriminals live and operate outside of the United States, but earn a lot of money by facilitating the fraud committed by local criminals — without ever needing to step foot in the United States. For example, international criminals hack and steal data from the United States, whether it is credit card data or personal identifying information, and then resell that data to identity thieves in the United States or engage in schemes to monetize that data and get the funds out of the United States. These criminals are as a group innovative and creative, working to infiltrate any vulnerability in order to steal.

Although data breaches, the Dark Web, and Bitcoin are now in the media spotlight, the international cybercrime economy has been evolving since 2001 and started taking
off in 2003. By 2003, cybercriminals were using a digital currency called *Egold* to pay each other for stolen data and criminal services and were “meeting” on Web forums to discuss ways to commit cybercrime and identity theft, as well as to find business partners or suppliers.

Simultaneously, as credit card and bank account security compromises became commonplace, we were all getting to know what it was like to be a victim of identity theft.

The case I discuss here spanned nearly a decade and involved some colorful characters. The case began with a routine investigation into a fraudulent purchase made online with a local woman’s credit card when I was a junior prosecutor at the Manhattan District Attorney’s office assigned to the newly created Identity Theft Unit. It progressed to the investigation and indictment of 18 defendants involved in major identity theft crimes and international cyber money laundering and, ultimately, nine years later, ended with the trial of three of those defendants. During the pendency of the litigation, it seemed like the amount of work was overwhelming and that the case might never end. The prospect of preparing proof for a trial of this magnitude was daunting. In a local prosecutor’s office, resources are scarce, even in an office as large as the Manhattan District Attorney’s office. This is not the type of trial where you can prepare the witnesses shortly before their testimony, but rather one that requires detailed analysis and preparation of records and exhibits, months and even years in advance.

In brief summary, the investigation began in early 2005 when I received a complaint about identity theft where a victim’s credit card was used without authorization at an online retailer to ship merchandise to an address in Manhattan. Following the money trail of the online actors
involved in this theft, we found ourselves looking at a digital currency exchanger in Manhattan called Western Express International, Inc., which by outward appearances, was acting as a check casher and money transmitter for Eastern Europeans earning money in the United States. However, the company was not licensed to cash checks or transmit money in New York State, so our first step was to have the company indicted for illegal check cashing and money transmitting. 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 that the company was knowingly facilitating their criminal activity and laundering their criminal profits. The company 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 personal identifying information.

Among the many great successes of the case was the extradition of three major Eastern European cybercriminals to New York on these charges, as well as a trial that resulted in guilty verdicts for the last three remaining defendants, a Ukrainian extradited on this charge who was one of the premier global vendors of stolen credit card data and two of his customers who were identity thieves from Brooklyn.

This case was the result of a partnership with the United States Secret Service, without whom this case could not have been brought, and the hard work of many people, including analysts, investigators, special agents, and many others in law enforcement and the financial sector.
As we investigated the initial report of credit card fraud, the online retailer indicated that there were other fraudulent orders placed with other credit card numbers to be shipped to the same Manhattan address. So we checked with other online merchants and soon we identified about a hundred fraud orders placed with that same ship-to address.

Clearly we had a suspect. At that time I knew just a little about identity theft and was a member of the newly formed Identity Theft Unit created by District Attorney Robert M. Morgenthau, which was led by two innovative assistant district attorneys, one of whom would stay to become the Unit Chief and who supervised and mentored the case and me throughout trial. I knew almost nothing about cybercrime, carders, Internet Protocol addresses, money laundering, or digital currency. The fraud orders were not being shipped to a master identity thief, but merely to a participant in a reselling scheme, a variant on the reshipping scheme. The individual at the Manhattan address receiving the fraudulently purchased shipments resold them online for a profit. It was another fraud I had not heard of at the time.

The reseller was using Egold digital currency to pay the fraudster and, as it turned out, the fraudster was moving some of that Egold through Western Express. I had never heard of Egold or digital currency at the time, nor had most people. However, it was popular with cybercriminals, identity thieves, child pornographers, Ponzi schemers, and gold bugs (people who believe in the gold standard and not in government backed currencies). The Egold was going to Western Express, so the investigation turned its focus to the corporation and what it was doing.
Western Express, by outward appearances, offered a host of financial services aimed towards a Russian-speaking clientele in Eastern Europe. Much of it was based upon transferring value for their customers both in and out of the United States. About $4 million over an equal number of years of their business consisted of receiving and depositing checks on behalf of their customers and transmitting those funds overseas. Since they were not licensed to do so, this constituted a violation of New York’s banking laws and formed the basis of the first indictment.

Money transmitting laws are a first step towards trying to keep our financial systems clean and to keep them from being a conduit for illicit activity and proceeds. People and companies who move money are supposed to be regulated and must follow Anti-Money Laundering (AML) procedures that include Know Your Customer (KYC) protocols and reporting of suspicious activity to the government. Western Express demonstrated why those laws are important. Western Express took no steps to know its customers and instead allowed customers to cash checks made out to obviously fictitious names. Western Express would then remit the money to the customer as they chose, such as to overseas accounts or via Western Union. In so doing, Western Express allowed people living overseas to anonymously receive funds processed through the U.S. banking system with this low-tech payment method.

Western Express also offered a variety of other services, many of which were designed to allow the customer to anonymously transfer funds or spend funds. They issued money orders, facilitated payments through other money transmitters, and resold gift cards.
It is worth noting the cost of many of their services. Cost of services and ease of use are important factors to consider when evaluating the customer base of any payment method. Many advocates of digital currencies point to the ease of use and low cost when compared with the traditional financial system such as sending a bank wire or Western Union or MoneyGram. They are right to a point. But the full cost of using a digital currency must be evaluated, because it costs money to cash in and cash out. Western Express’s services were expensive when compared to traditional financial services, whether it was check cashing, money orders, gift cards, or digital currency exchange. That expensive price reflected a premium for anonymity.

It took over a year to analyze the records of Western Express to fully understand their digital currency exchange business and to prove that they were a financial hub of cybercrime data trafficking. Thirty-five million dollars in digital currency flowed through the corporation over a four year period. To paraphrase Mr. Morgenthau, if any of that money was legitimate, it was probably purely by accident. That said, the second indictment of Western Express—charging money laundering and related crimes—identified about $2 million as the proceeds of criminal activity.

Much anti-money laundering training and procedures are focused on the risks posed by cash transactions, but the industry probably has not fully realized the threat of digital currency money laundering. Cash, as we touched upon earlier, 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 develop the problem of how to use all that cash without violating financial regulations and raising
suspicions about its source. They can’t use cash to buy a house, boat, or car without risking some serious and unpleasant attention, so they need to devise methods and schemes to integrate that cash for everyday use.

Digital currency money laundering has a slightly different flow. Here, the illicit profits are earned through cybercrime, but the profits still need to be concealed. The money still has to take several steps to be converted into “laundered” proceeds that can be spent. With the emergence and popularity of Bitcoin, there now are easier outlets for cyber fraudsters to launder their criminal proceeds. Critically, it is no longer essential that they first convert their illicit funds to traditional fiat currency before buying the products that they want.

Understanding digital currency money laundering requires us to recognize its global nature, its resemblance to other international trade models, and its interconnection with the conventional financial system.

The following diagram illustrates how the flow of digital currency, stolen data, and traditional funds works. The main takeaway is that cybercriminals outside of the United States regularly use methods like these to get illicit funds—generated by victimizing our residents—out of the United States.
The second indictment in the Western Express case charged 18 defendants with participating in Western Express’ cybercrime money laundering scheme. Five of these defendants were well-known international cybercriminals who stole from U.S. victims while comfortably residing overseas. While many in the law enforcement and financial communities doubt the effectiveness of pursuing cybercriminals acting from outside our borders, this case had some remarkable success indicting and extraditing international defendants. One defendant—Egor Shevelev—was a Ukrainian national who was arrested while vacationing in Greece, extradited to New York, and convicted after the trial. At the time, Shevelev was one of the world’s most prolific vendors of stolen credit card data on the cyber black market. Two other defendants (Russian and Moldovan nationals) were arrested in the Czech Republic, extradited to New York, and ultimately pleaded guilty. Two defendants remain fugitives to this day.

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, stolen credit card information was used to order the merchandise from an ecommerce site and ship the merchandise directly to the bona fide purchaser.

One of the international defendants—Dzmitry Burak—remains a fugitive on the Western Express charges as well as a subsequent federal indictment. He sold stolen credit card data as well as forged identifications (such as passports) online. Oleg Covelin also remains a fugitive, both on the Western Express charges as well as on the subsequent federal indictment. During the time he laundered 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.

It is both helpful and fascinating to see and understand the basic transactions among cybercriminals and identity thieves, how they communicate, how they pay each other, and how they traffic the stolen data. In the end, it is all about profit and this form of crime is indeed a very profitable occupation. It also requires intelligence and patience; many skills that identity thieves and cybercriminals develop over the years are mastered only with study and practice.

Though the criminals have carefully studied ways to become anonymous and evade law enforcement detection, this case was successful in piercing that veil of anonymity for some of the cybercriminals and identity thieves using Western Express’ services. This process involved an exhaustive review of evidence, including Web postings, paper documents, financial records, data from cell phones and computers, chat messages, evidence
seized during a search warrant in Kiev, and painstaking computer forensic analysis.

A fantastic team helped put the evidence together throughout the investigation and proved it to the jury’s satisfaction beyond a reasonable doubt at trial. 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 presented records obtained from Russia, the Ukraine, and dozens of U.S. corporations, including financial records and email records. We presented physical evidence seized from search warrants in the Ukraine, Brooklyn, Manhattan, and New Jersey.

Many of the witnesses testified about the hours, weeks, and years of work they spent making this case. Aside from the witnesses, there were many who played a large role in making sure the case happened, including prosecutors, analysts, agents, and investigators who allowed us to bring a few cybercriminals and identity thieves to justice. Few cases like this have been brought, much less made it to trial, and offered such rich insights into today’s cybercrime economy and the threats we face.

Clearly, individuals and corporations in our country are being bombarded with attacks of all types from cybercriminals trying to steal personal and financial information. Our government needs to do a better job at protecting our data and at apprehending those responsible for compromising it. Good cybersecurity is important, but the solution to this problem cannot lie with making every individual and corporation a cybersecurity fortress impervious to the repeated attacks we are suffering. Nor can we make them all cybercrime experts, alert to every endless variation of scam and social engineering scheme.
That approach is simply not realistic. Our law enforcement agencies need to be better at stopping cybercrime, or at least reducing it, by apprehending more of those responsible, and thus creating some deterrence to the criminals who currently face zero risk of apprehension and penalty. For law enforcement to do this there needs to be a thoughtful investment in people and cases.

Financial institutions also need to do better, because they are the main conduit through which cybercrime illicit profits are both generated and how they exit this country for delivery to the cybercriminals. It cannot be enough for our financial institutions to rely on minimum standard checkboxes of regulations or account holder contracts as their standard for due diligence; there must be a better way to ensure that international wires are not simply a black hole through which nothing can be recovered. They too must also look at the problem holistically and attempt to combat it.

The Western Express case illustrates a global problem that exists today. The names have changed, there are new digital currencies, new players, and new websites, but the problem remains, and we need to do better to find a solution. That said, this case is a shining success story and a testament to the many professionals who worked so hard on it to bring justice to a few of the world’s many cybercriminals.