William Noonan

Deputy Special Agent in Charge
United States Secret Service
Criminal Investigative Division
Cyber Operations Branch

Prepared Testimony

Before the
United States Senate
Committee on Banking, Housing, and Urban Affairs

December 10, 2014

Good morning Chairman Johnson, Ranking Member Crapo, and distinguished Members of the Committee. Thank you for the opportunity to testify on the ongoing challenge of cyber crime impacting our Nation's financial system. The U.S. Secret Service (Secret Service) has decades of experience investigating large-scale criminal cyber intrusions, in addition to other crimes that impact our Nation's financial payment systems. Based on this investigative experience, I hope to provide this Committee insight into the continued trend of transnational cyber criminals targeting our Nation's financial system for their illicit gain.

The Role of the Secret Service

The Secret Service was founded in 1865 to protect the U.S. financial system from the counterfeiting of our national currency. As the Nation's financial system evolved from paper to plastic to electronic transactions, so too has the Secret Service's investigative mission. Today, our modern financial system depends heavily on information technology for convenience and efficiency. Accordingly, criminals have adapted their methods and are increasingly using cyberspace to exploit our Nation's financial payment system by engaging in fraud and other illicit activities. This is not a new trend; criminals have been committing cyber enabled financial crimes since at least 1970.[1]

Congress established 18 USC §§ 1029-1030 as part of the Comprehensive Crime Control Act of 1984[2] and explicitly assigned the Secret Service authority to investigate these criminal violations.[3] These statutes first established as specific Federal crimes unauthorized access to computers[4] and the fraudulent use, or trafficking of, access devices[5]—defined as any piece of information or tangible item that is a means of account access that can be used to obtain money, goods, services, or other thing of value.[6]

Secret Service investigations have resulted in the arrest and successful prosecution of cyber criminals involved in the largest known data breaches, including those of TJ Maxx, Dave & Buster's, Heartland Payment Systems, and others. Over the past five years Secret Service cyber crime investigations have resulted in over 5,940 arrests, associated with approximately $1.53 billion in fraud losses and the prevention of over $11.71 billion in potential fraud losses. Through our work with our partners at the U.S. Department of Justice (DOJ), in particular local U.S. Attorney's Offices, the Computer Crime and Intellectual Property Section (CCIPS), the International Organized Crime Intelligence and Operations Center (IOC-2), the Federal Bureau of Investigations (FBI) and others, we will continue to bring major cyber criminals to justice.

[1] Beginning in 1970, and over the course of three years, the chief teller at the Park Avenue branch of New York's Union Dime Savings Bank manipulated the account information on the bank's computer system to embezzle over $1.5 million from hundreds of customer accounts. This early example of cyber crime not only illustrates the long history of cyber crime, but the difficulty companies have in identifying and stopping cyber criminals in a timely manner—a trend that continues today.
[2] Pub. L. 98-473, §§ 1602(a) and 2102(a), 98 Stat. 1837, 2183 and 2190.
[3] 18 U.S.C. §§ 1029(d) & 1030(d)(1)
[4] 18 U.S.C. § 1030
[5] 18 U.S.C. § 1029
[6] 18 U.S.C. § 1029(e)(1)

The Transnational Cyber Crime Threat

Advances in computer technology and greater access to personally identifiable information (PII) via the Internet have created online marketplaces for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity, and complexity of cyber crimes targeting private industry and critical infrastructure. These crimes include network intrusions, hacking attacks, malicious software, and account takeovers leading to significant data breaches affecting every sector of the world economy. The recently reported payment card data breaches are examples of the decade-long trend of major data breaches perpetrated by transnational cyber criminals who are intent on targeting our Nation's financial payment system for their illicit gain.

The growing collaboration amongst cyber-criminals allows them to compartmentalize their operations, greatly increasing the sophistication of their criminal endeavors as they develop expert specialization. These specialties raise both the complexity of investigating these cases, as well as the level of potential harm to companies and individuals. For example, illicit underground cyber crime marketplaces allow criminals to buy, sell, and trade malicious software, access to sensitive networks, spamming services, payment card data, PII, bank account information, brokerage account information, hacking services, and counterfeit identity documents. These illicit digital marketplaces vary in size, with some of the more popular sites boasting membership of approximately 80,000 users. These digital marketplaces often use various digital currencies, and cyber criminals have made extensive use of digital currencies to pay for criminal goods and services or launder illicit proceeds.

Secret Service Strategy for Combating this Threat

The Secret Service proactively investigates cyber crime using a variety of investigative means to infiltrate these transnational cyber criminal groups. As a result of these proactive investigations, the Secret Service is often the first to learn of planned or ongoing data breaches and is quick to notify financial institutions and the victim companies with actionable information to mitigate the damage from the data breach and terminate the criminal's unauthorized access to their networks. One of the most poorly understood facts regarding data breaches is that it is rarely the victim company that first discovers the criminal's unauthorized access to their network; rather it is law enforcement, financial institutions, or other third parties that identify and notify the likely victim company of the data breach.

A trusted relationship with the victim is essential for confirming the crime, remediating the situation, beginning a criminal investigation, and collecting evidence. The Secret Service's growing global network of 37 Electronic Crimes Task Forces (ECTF), located within our field offices, are essential for building and maintaining these trusted relationships, along with the Secret Service's commitment to protecting victim privacy. The Secret Service routinely discovers data breaches through our proactive investigations and notifies victim companies with actionable information. For example, as a result of information discovered this year through just one of our ongoing cyber crime investigations, the Secret Service notified hundreds of U.S. entities of cyber criminal activity targeting their organizations.

Additionally, as the Secret Service investigates cyber crime, we discover current criminal methods and share this cybersecurity information broadly to enable other organizations to secure their networks. The Secret Service does this through contributing to leading industry annual reports such as the Verizon Data Breach Investigations Report and the Trustwave Global Security Report, and through more immediate reports, including joint Malware Initial Findings Reports (MIFRs).

This year, UPS Stores Inc. used information published in a joint report by the Secret Service, National Cybersecurity and Communications Integration Center, United States Computer Emergency Readiness Team (NCCIC/US-CERT), and the Financial Services Information Sharing and Analysis Center (FS-ISAC) on the Back-Off malware to protect itself and its customers from cyber criminal activity.[7] The information in this report was derived from a Secret Service investigation of a network intrusion at a small retailer in Syracuse, New York. The Secret Service publically shared actionable cybersecurity information derived from this investigation to help numerous other organizations while still safeguarding sensitive information. As a result, UPS Stores, Inc. was able to identify 51 stores in 24 states that had been impacted, and then were able to contain and mitigate this cyber incident before it developed into a major data breach.[8]

As we share cybersecurity information discovered in the course of our criminal investigation, we also continue our investigation in order to apprehend and bring to justice those involved. Due to the inherent challenges in investigating transnational crime, particularly the lack of cooperation of some countries with law enforcement investigations, it can take years to finally apprehend the top tier criminals responsible. For example, even after a 2011 indictment, Secret Service agents were not able to arrest Roman Seleznev of Vladivostok, Russia, in an international law enforcement operation until just recently. Mr. Seleznev has been charged in Seattle in a 40-count superseding indictment for allegedly being involved in the theft and sale of financial information of millions of customers. Seleznev is also charged in a separate indictment with participating in a racketeer influenced corrupt organization (RICO) and conspiracy related to possession of counterfeit and unauthorized access devices.[9] This investigation was lead by the Secret Service's Seattle Electronic Crimes Task Force.

In another case, the Secret Service, as part of a joint investigation with U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI) and the Global Illicit Financial Team, hosted by IRS-Criminal Investigations, shut down the digital currency provider Liberty Reserve, which was allegedly widely used by criminals worldwide to store, transfer, and launder the proceeds of a variety of illicit activities. Liberty Reserve had more than one million users, who conducted approximately 55 million transactions through its system totaling more than $6 billion in funds. The alleged founder of Liberty Reserve, Arthur Budovsky, was recently extradited from Spain to the United States. Mr. Budovsky is among seven individuals charged in the indictment. Four co-defendants – Vladimir Kats, Azzeddine el Amine, Mark Marmilev, and Maxim Chukharev – have pleaded guilty and await sentencing. Charges against Liberty Reserve

[7] *See* http://www.us-cert.gov/security-publications/Backoff-Point-Sale-Malware
[8] *See* UPS Store's press release *available at* http://www.theupsstore.com/about/media-room/Pages/The-ups-store-notifies-customers.aspx.
[9] *See* http://www.justice.gov/usao/waw/press/2014/October/seleznev.html

and two individual defendants, who have not been apprehended, remain pending. This investigation was lead by the Secret Service's New York Electronic Crimes Task Force.

Legislative Action to Combat Data Breaches

While there is no single solution to prevent data breaches of U.S. customer information, legislative action could help to improve the Nation's cybersecurity, reduce regulatory costs on U.S. companies, and strengthen law enforcement's ability to conduct effective investigations. The Administration has proposed various pieces of cybersecurity legislation, including law enforcement provisions related to computer security, and continues to urge Congress to pass legislation that will strengthen government and private sector cybersecurity capabilities. In particular, we urge Congress to act on legislation that will allow us to keep pace with the rapidly-evolving threats of cyber crime.[10]

Conclusion

The Secret Service is committed to continuing to safeguard the Nation's financial payment systems by defeating cyber criminal organizations. Responding to the growth in these types of crimes, and the level of sophistication these criminals employ, requires significant resources and substantial collaboration among law enforcement and its public and private sector partners. Accordingly, the Secret Service dedicates significant resources to improving investigative techniques, providing training for law enforcement partners, and sharing information on cyber threats. The Secret Service will continue to coordinate and collaborate with other government agencies and the private sector as we develop new methods to combating cyber crime. Thank you for your continued commitment to protecting our Nation's financial system from cyber crime.

[10] This proposal is available at: http://www.whitehouse.gov/omb/legislative_letters/