Mr. Noonan's Answers to the Questions for the Record

Committee on the Judiciary
Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime

Answers to the Questions for the Record from Chairman Leahy

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

Committee on the Judiciary
United States Senate

"Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime"
February 4, 2014

1. Are there additional legal tools and/or resources that would help the United States Secret Service to investigate and prevent data breaches and other cybercrimes?

On May 12, 2011, the Administration sent Congress a cybersecurity legislative proposal. This proposal includes various provisions that would aid in the investigation and prevention of data breaches. Significantly, the proposal includes a national data breach notification standard that requires victim companies to report to a law enforcement agency with investigative jurisdiction, and allows law enforcement to delay any required public disclosure if this notification would impede an ongoing criminal investigation. It also includes Law Enforcement Provisions Related to Computer Security, which proposes changes to the scope and penalties of violations under 18 USC § 1030, including making these violations RICO predicate offenses, enhancing criminal and civil forfeiture, and providing for stronger penalties.

Given the growing sophistication and transnational nature of cyber crime, the Secret Service recommends amending 18 USC § 1030(a)(6) to criminalize the selling of unauthorized access to computers, including access to botnets, regardless of intent to defraud. The Secret Service also recommends amending 18 USC § 1029 to include criminals who traffic in the payment card data of U.S. financial institutions outside of the United States.

Investigating and preventing cyber crime requires skilled criminal investigators and effective partnerships with federal, state, local and international law enforcement. A constrained budget environment coupled with sequestration has limited the ability of the Secret Service to hire special agents to backfill positions lost through attrition, and to conduct training on cyber crime investigations. With additional resources, the Secret Service could strengthen its capacity to

combat cyber crime by providing special agents with recurring computer forensics and network intrusion training. In addition, increased training for the Secret Service's law enforcement partners through the National Computer Forensics Institute would serve as a force multiplier in defeating transnational organized cyber crime.

2. Given the recent trend of "point of sale" data breaches involving United States retailers and the use of so-called "scraping" malware in some of those data breaches, do you anticipate that there will be an increase in this kind of cybercrime involving payment cards in the future?

Since it was first published in 2008, the annual Verizon Data Breach Investigations Report (DBIR) has identified payment card data as the type of data most often stolen. Of the 621 confirmed data breaches analyzed in the 2013 DBIR, 28% involved the compromise of a "point of sale" (POS) terminal or server. Similarly, the 2013 Trustwave Global Security Report analyzed over 450 cyber incident response investigations conducted by Trustwave in 2012, in response to reports of suspected or confirmed data breaches. Of these, 47% involved the compromise of POS or payment processing systems. Both of these reports also show the substantial role of memory scraping malware to obtain financial information as part of cyber crime activity. The Secret Service contributes to both of these reports.

Over the past decade, cyber criminals have become highly adept at stealing large quantities of payment card data, and have established sophisticated online marketplaces for trafficking in the stolen data. Total annual financial losses to U.S. companies, due to cyber crime involving the fraudulent use of payment card data, are estimated by the Nilson Report to exceed $5 billion in 2012, and to have grown every year since at least 2003. Similarly, the Secret Service has observed an increase in the scale of cyber crime activity that we investigate, with total fraud losses associated with Secret Service cyber crime cases exceeding $200 million each year since 2010. The Secret Service will continue to prioritize its investigative efforts to most effectively suppress this sort of criminal activity, by focusing on the transnational, organized cyber criminals that have demonstrated the greatest ability and desire to inflict substantial financial losses to U.S. merchants and the financial services industry.

Mr. Noonan's Answers to the Questions for the Record

Committee on the Judiciary
Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime

3. Do you anticipate that we will witness an increase in "point of sale" data breaches, given the recent trend of data breaches involving major American retailers?

Data breaches, like the recently reported events, are a frequent occurrence. The 2013 Verizon Data Breach Investigations Report (DBIR) analyzes 621 confirmed data breaches, of which 28% involved the compromise of a "point of sale" (POS) terminal or server, while the 2013 Trustwave Global Security Report found that, of the over 450 cyber incident response investigations that Trustwave conducted in 2012, 47% involved the compromise of POS or payment processing systems. These reports also demonstrate that cyber criminals continue to primarily target retailers and other points of collection and processors of large quantities of payment card data like food and beverage, hospitality, and financial services companies. The Secret Service anticipates that this trend will likely continue.

Increased public awareness through news coverage of major data breaches, like the recently reported events, may result in enhanced scrutiny by companies and the uncovering of additional network intrusions and associated breaches, thereby increasing the number of reported incidents in the near future. The Secret Service is committed to proactively investigating this type of criminal activity, and to preventing and minimizing the financial losses to U.S. companies and the financial services industry from cyber crime.