CORRECTION: TWO RUSSIAN NATIONALS SENTENCED TO PRISON FOR MASSIVE DATA BREACH CONSPIRACY

USDOJ-Office of Public Affairs to me 11:25 AM

THE UNITED STATES DEPARTMENT of JUSTICE

FOR IMMEDIATE RELEASE
THURSDAY, FEBRUARY 15, 2018

NOTE: The below is a corrected press release from a previous version that was issued.

TWO RUSSIAN NATIONALS SENTENCED TO PRISON FOR MASSIVE DATA BREACH CONSPIRACY

Hackers Targeted Major Payment Processors, Retailers and Financial Institutions Around the World

WASHINGTON – Two Russian nationals were sentenced yesterday to federal prison terms for their respective roles in a worldwide hacking and data breach scheme that targeted major corporate networks, compromised 160 million credit card numbers and resulted in hundreds of millions of dollars in losses – one of the largest such schemes ever prosecuted in the United States.

The sentences were announced by Acting Assistant Attorney General John P. Cronan of the Justice Department's Criminal Division, First Assistant U.S. Attorney William E. Fitzpatrick of the District of New Jersey and Director Randolph D. Alles of the U.S. Secret Service.

Vladimir Drinkman, 37, of Syktyvkar and Moscow, Russia, was sentenced to 144 months in prison. Drinkman previously pleaded guilty before U.S. District Judge Jerome B. Simandle of the District of New Jersey to one count of conspiracy to commit unauthorized access of protected computers and one count of conspiracy to commit wire fraud in a manner affecting a financial institution. Dmitriy Smilianets, 34, of Moscow, previously pleaded guilty to conspiracy to commit wire fraud in a manner affecting a financial institution and was sentenced to 51 months and 21 days in prison. Both men pleaded guilty in September 2015 before Judge Simandle, who imposed the sentences yesterday in Camden, New Jersey federal court. In addition to the prison terms, Judge Simandle sentenced Drinkman to three years of supervised release and Smilianets to five years of supervised release.

Drinkman and Smilianets were arrested in the Netherlands on June 28, 2012. Drinkman was extradited to the District of New Jersey on Feb. 17, 2015, and Smilianets was extradited on Sept. 7, 2012.

"Drinkman and Smilianets not only stole over 160 million credit card numbers from credit card processors, banks, retailers, and other corporate victims, they also used their bounty to fuel a robust underground market for hacked information," said Acting Assistant Attorney General Cronan. "While mega breaches like these continue to affect millions of individuals around the world, hackers and would-be hackers should know that the Department of Justice will use all available tools to identify, arrest, and prosecute anyone who attacks the networks on which businesses and their customers rely."

"These defendants operated at the highest levels of illegal hacking and trafficking of stolen identities," First Assistant U.S. Attorney Fitzpatrick. "They used their sophisticated computer skills to infiltrate computer networks, steal information and sell it for a profit. Perpetrators of some of the largest data breaches in history, these defendants posed a real threat to our economy, privacy and national security, and cannot be tolerated."

"This case demonstrates the investigative capabilities of the U.S. Secret Service and the collaborative efforts of our law enforcement partners, specifically the U.S. Attorney's Office for the District of New Jersey, and the Dutch Ministry of Security and Justice," Special Agent in Charge McKevitt said. "The Secret Service will continue to develop innovative ways to protect the financial infrastructure of the United States and bring to justice cyber criminals who use emerging technologies to conduct business."

According to documents filed in this case and statements made in court:

Drinkman and Smilianets admitted to their roles in a conspiracy with three co-defendants to hack into the networks of corporate victims engaged in financial transactions, retailers that received and transmitted financial data and other institutions with information that the conspirators could exploit for profit, including the computer networks of NASDAQ, 7-Eleven, Carrefour, JCP, Hannaford, Heartland, Wet Seal, Commidea, Dexia, JetBlue, Dow Jones, Euronet, Visa Jordan, Global Payment, Diners Singapore and Ingenicard.

According to the indictment in this case and statements made in court, the five defendants each played specific roles in the scheme. Drinkman and Alexandr Kalinin, 31, of St. Petersburg, Russia, allegedly specialized in penetrating network security and gaining access to the corporate victims' systems. Drinkman and Roman Kotov, 36, of Moscow, allegedly specialized in mining the networks to steal valuable data. The hackers hid their activities using anonymous web-hosting services allegedly provided by Mikhail Rytikov, 30, of Odessa, Ukraine. Smilianets sold the information stolen by the other conspirators and distributed the proceeds of the scheme to the participants.

Drinkman and Kalinin were previously charged in New Jersey as "Hacker 2" and "Hacker 1" in a 2009 indictment charging Albert Gonzalez, 34, of Miami, Florida, in connection with five corporate data breaches – including the breach of Heartland Payment Systems Inc., which at the time was the largest ever reported. Gonzalez is currently serving 20 years in federal prison for those offenses. Kalinin is also charged in two federal indictments in the Southern District of New York: the first

charges Kalinin in connection with hacking certain computer servers used by NASDAQ and the second charges him and another Russian hacker, Nikolay Nasenkov, with an international scheme to steal bank account information from U.S.-based financial institutions. Rytikov was previously charged in the Eastern District of Virginia with an unrelated scheme.

Kalinin, Kotov and Rytikov remain at large.

The Attacks

According to documents filed in this case and statements made in court, the five defendants allegedly penetrated the computer networks of corporate victims and stole user names and passwords, means of identification, credit and debit card numbers and other corresponding personal identification information of cardholders, acquiring more than 160 million card numbers through hacking.

The initial entry was often gained using a "SQL injection attack." SQL, or Structured Query Language, is a type of programing language designed to manage data held in particular types of databases; the hackers allegedly identified vulnerabilities in SQL databases and used those vulnerabilities to infiltrate a computer network. Once the network was infiltrated, the defendants allegedly placed malicious code, or malware, in the system. This malware created a "back door," leaving the system vulnerable and helping the defendants maintain access to the network. In some cases, the defendants lost access to the system due to companies' security efforts, but were allegedly able to regain access through persistent attacks.

Instant message chats obtained by law enforcement revealed the defendants allegedly often targeted the victim companies for many months, waiting patiently as their efforts to bypass security were underway. The defendants had malware implanted in multiple companies' servers for more than a year.

The defendants allegedly used their access to the networks to install "sniffers," which were programs designed to identify, collect and steal data from the victims' computer networks. The defendants then allegedly used an array of computers located around the world to store the stolen data and ultimately sell it to others.

Selling the Data

According to documents filed in the case and statements made in court, after acquiring the card numbers and associated data – which they referred to as "dumps" – the conspirators sold it to resellers around the world. The buyers then sold the dumps through online forums or directly to individuals and organizations. Smilianets was in charge of sales, selling the data only to trusted identity theft wholesalers. He charged approximately $10 for each stolen American credit card number and associated data, approximately $50 for each European credit card number and associated data and approximately $15 for each Canadian credit card number and associated data – offering discounted pricing to bulk and repeat customers. Ultimately, the end users encoded each dump onto the magnetic strip of a blank plastic card and cashed out the value of the dump by withdrawing money from ATMs or making purchases with the cards.

Covering Their Tracks

According to documents filed in the case and statements made in court, the defendants allegedly used a number of methods to conceal the scheme. Unlike traditional Internet service providers, Rytikov allowed his clients to hack with the knowledge he would never keep records of their online activities or share information with law enforcement.

Over the course of the conspiracy, the defendants allegedly communicated through private and encrypted communications channels to avoid detection. Fearing law enforcement would intercept even those communications, some of the conspirators attempted to meet in person.

To protect against detection by the victim companies, the defendants allegedly altered the settings on victim company networks to disable security mechanisms from logging their actions. The defendants also worked to evade existing protections by security software.

As a result of the scheme, financial institutions, credit card companies and consumers suffered hundreds of millions in losses – including more than $300 million in losses reported by just three of the corporate victims – and immeasurable losses to the identity theft victims in costs associated with stolen identities and false charges. The charges and allegations contained in indictments against the remaining defendants are merely accusations and the defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

The case was investigated by special agents of the U.S. Secret Service, Newark Field Office and Criminal Investigative Division. The case is being prosecuted by by Trial Attorneys Andrew S. Pak and Richard Green and Deputy Chief of Litigation James Silver of the Criminal Division's Computer Crime and Intellectual Property Section, and Assistant U.S. Attorney Justin Herring of the Computer Hacking and Intellectual Property Section of the Economic Crimes Unit and the Justice Department's Office of International Affairs. The Criminal Division's Office of International Affairs also provided substantial assistance in this case.

Acting Assistant Attorney General John P. Cronan and U.S. Attorney Carpenito thanked public prosecutors with the Dutch Ministry of Security and Justice and the National High Tech Crime Unit of the Dutch National Police. They also credited the special agents of the U.S. Secret Service, Newark Field Office, under the direction of Special Agent in Charge Mark McKevitt, and the Criminal Investigative Division, under the direction of Special Agent in Charge Michael D'Ambrosio, for the ongoing investigation leading to yesterday's sentencings.

# # #

CRM

18-187

Follow us: