
*Cybercrime**UNITED STATES V. ROMAN SELEZNEV*

EVERY WEEK, IT SEEMS, A NEW WARNING goes out to consumers: a major corporation or financial institution has been hacked, and your data may have been exposed. These breaches can reveal sensitive information, including names, Social Security numbers, passwords, credit card and account numbers—data valuable to an underground network that packages it for sale to a criminal end user. In an online marketplace where buyers and sellers operate anonymously, it is often a challenge to pin an online breach to a real-life individual. Combating, investigating, and prosecuting these types of crimes can be further complicated if the perpetrators are outside the United States.

This chapter examines the case of *United States v. Roman Seleznev*, one of the largest cybercrime prosecutions. The case involves the hacking of point-of-sale systems used by small businesses to take credit card payments, the packaging and reselling of that credit card information, and a worldwide hunt for the perpetrator. It's also a rare success story of a large-scale cybercriminal being brought to the United States to stand trial. As you read this chapter, think about the international cooperation that was necessary to investigate and prosecute this case, and at what points the lack of cooperation with other jurisdictions hindered the case. Another interesting aspect of this case is attribution: how prosecutors prove that a certain individual is the person who is responsible for anonymous online activities.

THE CRIME

Investigators in the Pacific Northwest got their first introduction to this global cybercrime investigation through a report from a Schlotsky's Deli in

Coeur d'Alene, Idaho. In 2010, the store's owner reported a problem with its point-of-sale system, suspecting it had been targeted by cybercriminals. A Seattle police detective, David Dunn, who was a member of the Secret Service Electronic Crimes Task Force, responded and found that the system was beaming data out to servers in Russia. Soon, the investigation expanded to other restaurants in Washington State—bakeries, restaurants, pizza parlors. In each case, the point-of-sale system contained malicious software that located stored credit card numbers and then sent data overseas. The software appeared to have been installed by an intruder who had scanned the internet for open “ports” that allowed off-site tech support to remotely access a business's computer system for maintenance (Government's Trial Brief, 6).

The credit card information was sent back to collection servers where it was then sorted to determine the value of the data, such as credit card numbers, bank identification numbers, names of account holders, and personal identification numbers (PINs). From there, the data were posted for sale on websites known as “dump shops” and marketed to an underground network of buyers (Second Superseding Indictment, 2014).

These sites were already known to federal investigators. As early as 2005, the US Secret Service sought to identify the individual suspect whose online handle was “nCuX,” a major player on forums where “carders” bought and sold stolen credit card data. “Carding” is the practice of hacking, stealing, and trafficking credit card data (Government's Trial Brief, 2016). Carding forums are marketplaces where carders, hidden behind online aliases, can sell the stolen credit information to users who then make fraudulent purchases. By 2009, investigators were fairly confident that the person going by “nCuX” was Roman Seleznev of Vladivostok, Russia. Federal agents attempted to gain international assistance and met with their Russian counterparts to share what they knew about the suspect and ask for help in apprehending him. This strategy backfired. Within a month, nCuX announced his retirement and disappeared from the internet (Black Hat USA, 2017). Investigators later learned that Seleznev's father was a member of the Russian parliament.

The investigation started over. But almost immediately a new online handle, “2Pac,” appeared in the online carding forums, and the cybercrimes team suspected that it was the same person. Several new “dump shop” websites, including “Track2” and “Bulba,” began trafficking in the same stolen credit card data. The sites even offered a service that would allowed buyers to check that the credit card accounts were still active and a guarantee to replace card numbers that were invalid (Second Superseding Indictment, 2014, p. 8). One

site offered step-by-step tutorials on how to buy and use stolen credit card information for profit, even warning users “Remember this is Illegal way!” (Government’s Sentencing Memorandum, 2017).

While investigating the 2010 breaches in the Pacific Northwest, the agents mapped the route the stolen data took and tracked it to the Track2 and Bulba sites, where the credit card numbers were offered for sale (Government’s Trial Brief, 2016). Detective Dunn and Special Agent Keith Wojcieszek, a Washington, DC–based Secret Service agent, identified the infrastructure that Track2 used—including servers and email accounts. Most of the collection servers that aggregated the stolen credit card data were overseas, but a few were in Virginia and therefore subject to US jurisdiction. Dunn and Wojcieszek obtained search warrants to look for information that would lead to the identity of the site’s operator. One server, known as HopOne, had collected hundreds of thousands of credit card numbers, including the ones in Washington State.

That server also contained a trail of electronic crumbs that led to the intruder. A forensic analysis found remnants of web-browsing history that included travel reservations for Roman Seleznev, including his date of birth, passport number, and the names of his wife, daughter, other family members, and two associates (Government’s Trial Brief, 2016). It also revealed two email accounts that gave the agents a new direction in which to search. Search warrants for the email accounts led to billing statements for other servers, and email traffic confirmed the registration of another site thought to be linked to Seleznev.

One of those email accounts was particularly revealing, producing evidence such as emails to Seleznev from his wife in which she attached pictures of herself and their daughter; other emails addressed to Roman Seleznev; receipts for flower deliveries to Seleznev’s wife at their home address; and an invoice addressed to Roman Seleznev that listed a phone number he was known to use. The emails also revealed usernames and passwords commonly used by Seleznev, further linking him to the intrusion (Government’s Trial Brief, 2016, p. 9). Investigators found a particular Yahoo email address used to register the Track2 website, and obtained a search warrant for that email account. While that search turned up no evidence linked to Seleznev, investigators learned that the account used the username “smaus” and password “ochko.”

Now that investigators had a name to link to the crime, they could go after their suspect. A sealed indictment was filed in March 2011 charging Seleznev with six counts of bank fraud (18 U.S.C. § 1344), eight counts of intentional

damage to a protected computer (18 U.S.C. § 1030(a)(5)(A)), eight counts of obtaining information from a protected computer (18 U.S.C. § 1030(a)(2)), one violation of possessing fifteen or more unauthorized access devices (18 U.S.C. § 1029(a)(3)), two charges of trafficking in unauthorized access devices (18 U.S.C. § 1029(a)(2)), and five counts of aggravated identity theft (18 U.S.C. 1028A(c)). They had an arrest warrant, but Roman Seleznev avoided US jurisdiction. Investigators began stalking him around the globe.

A month after the sealed indictment was filed, Seleznev was severely injured in a terrorist bombing at a restaurant in Morocco (Black Hat USA, 2017). Suffering major head trauma and other wounds, he was airlifted back to Moscow, where he remained in a coma for several weeks and was hospitalized for months. In the meantime, his online business slowed, and his associates asked customers of Track2 and Bulba to be patient while the boss recovered.

Seleznev and his business did eventually bounce back, and the US agents continued to watch for him, but he continued to carefully avoid U.S. jurisdiction. On July 1, 2014, agents learned that he was vacationing in the Maldives, a small chain of islands in the Indian Ocean. The information set off a flurry of activity for those involved in the case (Government's Sentencing Memorandum, 2017, p. 11).

The agents had four days to (1) seek internal US government clearances to conduct a foreign operation; (2) obtain agreement from the Maldives to turn Seleznev over without a formal extradition treaty; (3) mobilize Secret Service agents to the Maldives (an eighteen-hour flight from Hawaii); (4) coordinate the logistics of the apprehension with the local authorities; (5) arrange for private transportation (that is, a private jet with sufficient range to fly many thousands of miles over water) to take Seleznev to the nearest US territory; and (6) take custody of Seleznev.

The United States does not have an extradition treaty with the Maldives, but US officials convinced the authorities there to expel Seleznev from the country to US custody (Black Hat USA, 2017). He was arrested at the airport on July 5, 2014, and taken to Guam, where he had an initial appearance in a US federal court. He pleaded not guilty to all charges.

Seleznev, thirty years old, had genuine health concerns stemming from the 2011 bombing in Morocco, which had left him with a significant head injury. He fought extradition to the United States, claiming he'd been "kidnapped" in violation of international law, and enlisted the Russian government's assistance. He lost that battle, however, and was transported to Seattle to stand trial.

COURT PROCEEDINGS

Roman Seleznev was arraigned in a federal court in Guam on August 8, 2014. He entered a not guilty plea to all charges. Once transported to Seattle, a judge ordered his detention pending trial, finding that Seleznev posed a flight risk (Carter, 2014).

In the following two years before the trial began in August 2016, Roman Seleznev hired and fired numerous attorneys and, prosecutors alleged, discussed how to bribe the prosecutors to make the trial go away (Black Hat USA, 2017). Seleznev also asked to represent himself at the pretrial motions stage of the proceedings and filed several motions to dismiss that alleged prosecutorial misconduct. His motions were denied. He also filed a motion to suppress the evidence found on his laptop, claiming that the government had tampered with it. The court found no evidence that the computer had been altered.

EVIDENCE AT TRIAL

When Roman Seleznev was arrested in the Maldives, authorities seized his laptop and phone, both of which provided a wealth of new evidence against him (Black Hat USA, 2017). The laptop contained 250 “dump files” that held 1.7 million stolen credit card numbers; pictures and text used to create one of the dump sites; and chat logs between 2Pac and other carders in which they discussed buying and selling credit card data (Government’s Trial Brief, 2016). Another key piece of evidence that linked Seleznev to the servers was an electronic password “cheat sheet” that listed his usernames and passwords, including frequent use of “smaus” as a username and “ochko” as a password. This was the same combination as the Yahoo email account used to create the Track2 and Bulba sites.

Two other items on the laptop caught investigators’ attention. First, chat logs from 2008 in which Seleznev bragged to an associate that he had protection through law enforcement contacts in the computer crime squad of the FSB, the Russian federal security service. In 2010, he told someone else that the FSB knew who he was and was working with the FBI (Government’s Sentencing Memorandum, 2017). This explained how Seleznev learned about the Secret Service’s 2009 attempt to get Russian law enforcement’s assistance to arrest him. The second item of interest was evidence that prior to traveling,

Seleznev had searched federal court records for an indictment in his name and his online aliases, using the online court filing system PACER (Government's Sentencing Memorandum, 2017).

On the stand during more than two days of testimony, Detective David Dunn walked through all of the electronic links between the computer breaches, the online sales of stolen credit card information, and Roman Seleznev. Building the case at trial is a challenge, observed Norman Barbosa, one of the two assistant US attorneys involved in the Seleznev case, "because attribution is everything. There's no debate that a crime occurred. It's not a fraud case where you're arguing about whether a security was fraudulent. This definitely happened. It was definitely illegal. The question is purely, who did it. And you're dealing with the anonymity of the internet, where it's all done with false names" (personal communication, September 23, 2019).

During the nine-day jury trial held in Seattle, business owners testified about the money they had to spend to install new computers after their point-of-sale systems were compromised by hackers—a huge expense for a small business operating on slim margins (Bellisle, 2016). The owner of Seattle's Broadway Grill testified that the breach instantly cut his revenue by 40 percent, eventually sending the business into bankruptcy (Government's Sentencing Memorandum, 2017). Another restaurant owner said he had a "nervous breakdown" due to the effect on his business. Another said that six years later, he was still trying to pay down the debt he took on to address the intrusion.

Prosecutors alleged that Seleznev's scheme enabled \$170 million in fraudulent credit card purchases and was linked to thirty-seven hundred banks around the world. Not all of the hundreds of businesses harmed by the hacking testified at trial, but many later submitted victim-impact statements and claims for damages that provided examples of how they were affected. The Houston Zoo reported that it had put off planned upgrades to facilities that would have "benefitted its millions of guests, improved the work environment of its staff, and enhanced the lives of its animals" (Government's Sentencing Memorandum, 2017, p. 10). The owner of a market in New Jersey spent thousands of dollars in response to the hack and said that the business still hadn't recovered.

Seleznev's defense aimed at the sufficiency of the government's case, arguing that there was reasonable doubt about whether the anonymous online acts were committed by this one individual.

On August 25, 2016, the jury returned guilty verdicts on thirty-eight of the forty criminal counts. Seleznev was acquitted on one count of intentional

MODEL JURY INSTRUCTIONS

9th Circuit Court of Appeals

*18 U.S.C. § 1029(a)(2). Unauthorized Access
Devices—Using or Trafficking.*

The defendant is charged in [Count ___ of] the indictment with trafficking in unauthorized access devices during a period of one year in violation of Section 1029(a)(2) of Title 18 of the United States Code.

In order for the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, the defendant knowingly [used] [trafficked in] the unauthorized access devices at any time during a one-year period [beginning [date], and ending [date]];

Second, by [using] [trafficking in] the unauthorized access devices during that period, the defendant obtained [anything of value worth \$1,000 or more] during that period;

Third, the defendant acted with the intent to defraud; and

Fourth, the defendant's conduct in some way affected commerce between one state and another state, or between a state of the United States and a foreign country.

An "unauthorized access device" is any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud.

To "traffic" in an access device means to transfer or otherwise dispose of it to another, or to obtain control of it with intent to transfer or dispose of it.

*18 U.S.C. § 1029(a)(3). Access Devices—Unlawfully
Possessing Fifteen or More*

The defendant is charged in [Count ___ of] the indictment with unlawful possession of access devices in violation of Section 1029(a)(1) of Title 18 of the United States Code.

In order for the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, the defendant knowingly possessed at least fifteen unauthorized access devices at the same time;

Second, the defendant knew that the devices were unauthorized;

Third, the defendant acted with the intent to defraud; and

Fourth, the defendant's conduct in some way affected commerce between one state and another state, or between a state of the United States and a foreign country.

An "unauthorized access device" is any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud.

18 U.S.C. § 1029. Access Device—Defined.

An "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access, that can be used alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

18 U.S.C. § 1030(a)(5)(A). Intentional Damage to a Protected Computer.

The defendant is charged in [Count ___ of] the indictment with transmitting [a program] [a code] [a command] [information] to a computer [system], intending to cause damage, in violation of Section 1030(a)(5) of Title 18 of the United States Code.

In order for the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, the defendant knowingly caused the transmission of [a program] [a code] [a command] [information] to a computer without authorization;

Second, as a result of the transmission, the defendant intentionally impaired the [integrity] [availability] of [data] [a program] [a system] [information]; and

Third, the computer was [exclusively for the use of a financial institution or the United States government] [used in or affected interstate or foreign commerce or communication] [located outside the United States but was used in a manner that affects interstate or foreign commerce or communication of the United States] [not exclusively for the use of a financial institution or the United States government, but the defendant's transmission affected the computer's use by or for a financial institution or the United States government].

damage to a protected computer and another count of wire fraud, both relating to an alleged computer intrusion at the same pizzeria.

SENTENCING

Seleznev returned to court for sentencing on April 21, 2017. As often happens, the two parties had very different views of how a proper sentence should be determined. Depending on who was talking about him, Roman Seleznev was either the privileged son of a member of the Russian parliament or a young man who was abandoned by his father, lost his mother at a young age, and grew up poor and alone (Carter, 2016; Personal Statement by Roman Seleznev, 2017).

Seleznev's attorney painted him as a man who had made terrible choices in the past, but who wanted now to cooperate with law enforcement and was on a better path (Transcript, Sentencing Hearing, 2017). Seleznev submitted a handwritten letter to the judge that explained his history and attempted to correct the impression that he'd benefited from his father's political connections. In fact, he said, nothing could be further from the truth. Seleznev said his father abandoned his family, leaving him and his mother with little to live on (Defendant's Sentencing Memorandum, 2017). He acknowledged his criminal activity, but said it was the only option he thought he had to support himself as a young man without resources or education. He also asked the judge to consider his ongoing health issues from the bombing, including severe seizures that required medication.

The government's sentencing memorandum took a different view of Seleznev. He had lived large and owned two properties in Bali, Indonesia, and spent his time jetting between Bali and Vladivostok, Russia. He stayed in luxury hotels, and spent \$20,000 at the resort in the Maldives prior to his arrest. The government estimated that through a single payment service, Liberty Reserve, he took in \$17 million between 2010 and 2013. Liberty Reserve was seized by the government in 2014 in connection with a separate criminal investigation, and Seleznev's account was found in the company's records (see chapter 7, "Money Laundering"). But prosecutors did not know how much Seleznev had profited from the scheme, because he used Bitcoin, WebMoney, and other payment systems that ensure anonymity.

The first step in determining a sentence in federal court is to calculate an advisory sentencing range under the United States Sentencing Guidelines (USSG). The guidelines seek to quantify all aspects of the crime and the

defendant's role in it and to promote consistent resolutions throughout the federal court system. Cases relating to financial crimes fall under Section 2B1.1 of the Guidelines, and determining the sentence is largely driven by the amount of money lost due to the fraudulent behavior. In Seleznev's case, the victims of the computer intrusions lost \$170 million, prosecutors estimated. But for purposes of sentencing, the Guidelines calculate loss based on how many credit cards Seleznev stole, possessed, or used (USSG § 2B1.1, App. Note 4(F)). Each card is valued at a minimum of \$500. Though Seleznev had 1.7 million credit card numbers on his laptop when he was arrested, the evidence at trial proved that he stole 2.4 million credit cards over several years. That brought the loss amount for sentencing purposes to \$1.2 billion.

There are additional specific offense characteristics that the court also must take into account. Aggravating factors include how many victims were involved, whether the defendant was in the business of receiving stolen property, whether the fraudulent scheme was committed from outside the United States, and whether the criminal conduct involved sophisticated means. The court found that all of these aggravating factors applied in Seleznev's case.

In addition to specific offense characteristics that the court uses to tally a score based on the criminal conduct, the court must also look at the defendant's specific conduct relating to any crime, such as the defendant's role in the offense. Here, the prosecutors argued that Seleznev was a leader of the operation. The court declined to adopt that finding, as it was unclear who else was involved in Seleznev's enterprise.

Under the Sentencing Guidelines, Seleznev's advisory sentence was life imprisonment. But calculating the advisory sentencing range is only the starting point. The sentence must be calculated based on all of the factors set forth in 18 U.S.C. § 3553(a).

The government was not seeking a life sentence for Seleznev, though it noted that this was an unprecedented prosecution and the sentence needed to have a strong deterrent value (Government's Sentencing Memorandum, 2017). Rather, government prosecutors sought a sentence of 30 years, plus restitution of nearly \$170 million. This sentence was similar to that recommended by the United States Probation Department's in its pre-sentence report: a total term of imprisonment of 27 years and nearly \$170 million in restitution to the identified victims (Defendant's Sentencing Memorandum, 2017).

Seleznev's attorneys urged the court to depart downward from probation's recommendation, for several reasons. Seleznev argued that the calculated loss

of about \$1.2 billion substantially overstated the actual loss of \$170 million attributed to the defendant. And the attorneys argued that sentencing Seleznev to decades in prison went against the parsimony clause in the sentencing law, which directs the court to impose a punishment that is “sufficient, but not greater than necessary,” to achieve the goals of the sentencing law (18 U.S.C. § 3553(a)). Due to his health issues, a lengthy sentence would be even harsher for Seleznev than others, his lawyer said. As he was not a citizen, once Seleznev was released from prison, he would be deported back to Russia.

Finally, Seleznev was sorry for his actions, his attorney said. He was embarrassed and humiliated by his conduct, and he deeply regretted the loss to the many victims (Defendant’s Sentencing Memorandum, 2017, p. 15). At the sentencing hearing, in his allocution (the opportunity to speak to the court), Seleznev again apologize for his conduct. He told the court that “not one day has passed which I have not felt extreme sympathy and sadness for the crimes I commit and negative impact to my victims” (Transcript, Sentencing Hearing, 2017, p. 37). Seleznev said he was ashamed of his conduct, did not want to minimize the seriousness of his crime, and understood that a long sentence would likely be imposed. He stressed that he missed his family in Russia and wished to get back to them as soon as possible.

US district court judge Richard A. Jones recognized the lack of parental guidance that Seleznev had had as a child. But on the whole, the judge believed, Seleznev’s life demonstrated far more aggravating circumstances than mitigating ones. Most of his adult life had been dedicated to credit card fraud. And while Seleznev had apologized to the court for his conduct and expressed remorse, the court found no true acceptance of responsibility for his conduct. Judge Jones noted that Seleznev had had multiple opportunities in his life to reset his “moral navigation system and avoid a life of crime” (Transcript, Sentencing Hearing, 2017, p. 44). The sentence that Seleznev and his attorney sought, essentially asking for time served or probation, would have no deterrent value, one of the factors the court must consider under 18 U.S.C. § 3553(a). In the end, the court imposed a 27-year sentence, following the recommendation of the probation office. The breakdown of the sentence was 300 months on most of the charges, concurrent with one another and concurrent with other counts. Under the statute, counts 39 and 40, the identity theft convictions, carry mandatory consecutive sentences of 24 months each.

THE RESOLUTION

Roman Seleznev was ordered to serve 27 years in prison and pay nearly \$170 million to his many victims. He was also charged and convicted in two other federal cases. In the US district court in Nevada, Seleznev was charged for his role in a \$50 million scheme to traffic in stolen credit cards and counterfeit and stolen identities (DOJ OPA, 2017). Seleznev pleaded guilty in the Nevada case to one count of participation in a racketeering enterprise, admitting to selling stolen credit card accounts for approximately \$20 each.

He also pleaded guilty to one count of conspiracy to commit bank fraud in a case filed in Georgia, where he admitted that he acted as a “cashier” in a 2008 scheme in which hackers infiltrated a company’s computer systems and accessed 45.5 million debit card numbers that they used to withdraw more than \$9.4 million in cash from 2,100 ATMs in 280 cities around the world over a twelve-hour period. In each case, Seleznev was sentenced to 168 months, to run concurrently with the sentence imposed in the Washington case.

In all of these cases, the victims were unlikely to recover any money. Norman Barbosa, the former assistant US attorney who prosecuted the Washington case, says that Seleznev’s money was in Russian banks and remained out of reach of US authorities. Seleznev also kept some profits in Bitcoin, but the government did not recover Seleznev’s wallet. Even with a court order, it is difficult to recover money from overseas jurisdictions.

THE FUTURE OF CYBERCRIME

At the time of Seleznev’s trial in 2016, his was the largest hacking case prosecuted by the federal government. Since then, several other defendants in large-scale cybercrime cases have been extradited to the United States to stand trial, but many are beyond the reach of US law enforcement—particularly those in Russia, Barbosa noted. “There’s a huge problem of impunity for Russian hackers, the difficulty in bringing anyone to justice,” he said. The Secret Service agents attempted to work with Russian law enforcement, only to have them tip off Seleznev (Government’s Sentencing Memorandum, 2017).

“One big trend over the last five years is that there is more nation-state involvement in computer crimes, hacking more for political purposes and espionage,” Barbosa said.

STATUTE

18 U.S.C. § 3553(a). Imposition of a Sentence.

(a) Factors to Be Considered in Imposing a Sentence. The court shall impose a sentence sufficient, but not greater than necessary, to comply with the purposes set forth in paragraph (2) of this subsection. The court, in determining the particular sentence to be imposed, shall consider—

- (1) the nature and circumstances of the offense and the history and characteristics of the defendant;
- (2) the need for the sentence imposed—
 - (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
 - (B) to afford adequate deterrence to criminal conduct;
 - (C) to protect the public from further crimes of the defendant; and
 - (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner;
- (3) the kinds of sentences available;
- (4) the kinds of sentence and the sentencing range established for—
 - (A) the applicable category of offense committed by the applicable category of defendant as set forth in the [United States Sentencing Guidelines] . . .
- (5) any pertinent policy statement—
 - (A) issued by the Sentencing Commission . . .
- (6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and
- (7) the need to provide restitution to any victims of the offense.

Cybercriminals are becoming more sophisticated and organized. As technology evolves, it has become easier for hackers and carders to cover their tracks through encryption or by conducting business on the Dark Web, websites that use anonymity tools to hide their IP addresses. The typical carder is also becoming better organized, operating as a criminal enterprise with multiple layers of actors running the operation as if it were a business, Barbosa reported. These suspects, he said, “are far more organized than Seleznev.”

Despite the challenges, according to Barbosa, these cases are solved using the same investigative techniques and dogged detective work as with any other crime.

“Any online investigation involves tracing every lead and looking for a mistake. You’ll follow a hundred leads to find one mistake,” he said; in Seleznev’s case, he used one of his carder email accounts to order flowers for his wife. The key is perseverance in following every lead. “What was striking about the investigation [is] that it was just good detective work and attention to detail that picked it apart,” Barbosa observed. “Even though it’s online, you’re doing the same things that detectives do in traditional cases—going to the crime scene and looking for anything that can be evidence of a crime.”

Seleznev appealed his conviction and sentence to the Ninth Circuit US Court of Appeals, which affirmed his conviction in April 2019. Upon his release, scheduled for early 2038, Seleznev will be deported to Russia.

REFERENCES

- Bellisle, M. (2016). “Trial of Alleged Russian Master Hacker Begins This Week; Targets Were Credit Cards Used at Pizza Places.” *Seattle Times*, August 14.
- Black Hat USA. (2017). “Ochko123—How the Feds Caught Russian Mega Carder Roman Seleznev.” YouTube, updated August 25. <https://www.youtube.com/watch?v=6Chp12sEnWk&feature=youtu.be>.
- Carter, M. (2014). “Accused Russian Hacker Must Stay in Custody, Judge Says.” *Seattle Times*, August 15.
- Carter, M. (2016). “Feds Outline Case against Alleged Russian Hacker.” *Seattle Times*, August 15.
- DOJ OPA (Department of Justice, Office of Public Affairs). (2017). “Russian Cybercriminal Sentenced to 14 Years in Prison for Role in Organized Cybercrime Ring Responsible for \$50 Million in Online Identity Theft and \$9 Million Bank Fraud Conspiracy.” United States Department of Justice. November 30. <https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-14-years-prison-role-organized-cybercrime-ring-responsible>.

COURT DOCUMENTS

- Defendant’s Sentencing Memorandum. (2017). United States v. Seleznev, 11-cr-0070. W. Dist. Washington. April 14.
- Government’s Sentencing Memorandum. (2017). United States v. Seleznev, 11-cr-0070. W. Dist. Washington. April 14.

Government's Trial Brief. (2016). United States v. Seleznev, 11-cr-0070. W. Dist. Washington. July 25.

Indictment. (2012). United States v. Seleznev, 11-cr-0070. W. Dist. Washington. March 3.

Personal Statement by Roman Seleznev. (2017). United States v. Seleznev, 11-cr-0070. W. Dist. Washington. April 10.

Second Superseding Indictment. (2014). United States v. Seleznev, 11-cr-0070. W. Dist. Washington. October 8.

Transcript, Sentencing Hearing. (2017). United States v. Seleznev, 11-cr-0070. W. Dist. Washington. April 21.

United States v. Seleznev, 766 Fed.Appx. 531 (9th Cir. 2019).