The Honorable Richard A. Jones

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff v. ROMAN V. SELEZNEV, Defendant	NO. CR11-0070RAJ **SENTENCING MEMORANDUM**

I. INTRODUCTION

Defendant Roman Seleznev is to be sentenced for 38 convictions arising from his operation of a global cybercrime enterprise. From behind a keyboard in Vladivostok, Russia, and Bali, Indonesia, Seleznev and his associates hacked into thousands of computers around the world, including the systems of many small businesses in the Western District of Washington. Seleznev stole millions of credit card numbers from these computers, which he then sold to other criminals to use in fraudulent transactions.

But Roman Seleznev did not just steal and sell credit card data. He was a criminal entrepreneur whose innovations shaped the carding industry. Under the nickname "Track2," Seleznev created two automated vending sites, an innovation that made it possible for criminals to efficiently search for and purchase stolen credit card data

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

through a process as easy as buying a book on Amazon. Later, under the nickname "2Pac," Seleznev built a global resale operation, creating an online marketplace where scores of notorious hackers offered for sale the credit card data they had stolen through their own hacking activities. And, at the same time Seleznev was organizing the *supply* of credit card data in this manner, he worked to stimulate the *demand* for stolen card data by establishing a website known as "POS Dumps," which trained thousands of new criminals in the basics of how to use the data to commit fraud.

Seleznev enriched himself by these activities and lived an extravagant lifestyle at the expense of small, hard-working business owners who saw their businesses either damaged or destroyed as a result of Seleznev's attacks. Seleznev also caused massive losses to financial institutions. The *known* fraud loss associated with Seleznev's crimes is approximately $170 million. His victims include over 3,700 different financial institutions, over 500 businesses around the world, and millions of individual credit card holders. Simply put, Roman Seleznev has harmed more victims and caused more financial loss than, perhaps, any other defendant that has appeared before the Court.

This prosecution is unprecedented. Never before has a criminal engaged in computer fraud of this magnitude been identified, captured, and convicted by an American jury. The extraordinary nature and magnitude of this case is reflected in Seleznev's Sentencing Guidelines calculation. Seleznev's sentencing guideline calculation is literally off the charts: his offense level of 59 is 16 points higher than the top of the Sentencing Table, which reaches a maximum (and recommends a life sentence) at 43. Indeed, defendant's guideline calculation results in the highest total offense level for any prosecution in memory in this District.

There is tremendous public interest in deterring cybercrime. As Seleznev's victims made clear at trial, credit card fraud imposes devastating costs on businesses and financial institutions. Criminals like Seleznev who launch these attacks hide behind keyboards in foreign countries, and are careful to avoid putting themselves at risk of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

extradition. They use increasingly sophisticated tools and techniques to obfuscate their true identities and their infrastructure is frequently scattered across multiple international jurisdictions. Identifying these criminals and bringing them to justice—when it is possible at all—requires a massive commitment of law enforcement resources. Now that law enforcement has succeeded in bringing a top-tier cybercriminal to justice, it is imperative to deter other would-be cybercriminals around the world by sending a clear message that attacking and victimizing the United States' economy will result in severe penalties.

The community also has a compelling interest in preventing Seleznev himself from committing further crimes. This is a man with extraordinary computer abilities and cunning business acumen who has chosen to return to cybercrime again and again, each time increasing the scope of his criminal enterprise and the magnitude of its damage. Once released, Seleznev will return to Russia, where he will once again be beyond the reach of American law enforcement. The sentence should be calculated to ensure that Seleznev does not have the opportunity to launch his cyber-attacks for many, many years.

For all of these reasons, the government recommends that the Court sentence Roman Seleznev to a period of 30 years of imprisonment to be imposed as follows: as to each of counts 1-10 (Wire Fraud), defendant shall serve 336 months to be run concurrently with one another, and also concurrently with all other counts except counts 39 and 40; as to each of counts 12-19 (Intentional Damage to a Protected Computer) and counts 30-38 (Access Device Fraud), defendant shall serve a sentence of 120 months to be run concurrently with one another, and also concurrently with all other counts except counts 39 and 40; as to each of counts 21-29 (Obtaining Information from a Protected Computer), defendant shall serve a sentence of 60 months to be run concurrently with one another, and also concurrently with all other counts except counts 39 and 40; as to each of counts 39 and 40 defendant shall serve 24 months, these terms shall run concurrently with one another, but the 24 month sentence on counts 39 and 40 will run

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

consecutively, as required by statue, to the 336 month term of imprisonment on all other counts. The total term of imprisonment is 360 months (30 years). Seleznev should also be ordered to pay restitution to the victim financial institutions in the total amount of $169,418,843 and to the identified victim businesses in the amount of $465,742.95.

II. BACKGROUND

The Court is familiar with the facts of this matter, having presided over a jury trial and conducted numerous evidentiary hearings. Accordingly, the following discussion is intended not to be exhaustive, but instead, to identify the facts and issues most relevant to the sentencing considerations of Title 18, United States Code, Section 3553.

A. Defendant's Criminal Enterprises

1. NCUX

Roman Seleznev has been engaged in cybercrime his entire adult life. At the age of 18, Seleznev began using the online nickname "nCuX," which is the transliteration of the Russian word for "psycho." PSR ¶ 10. Using the nCuX identity, Seleznev began participating in the Russian underground "carding" community in approximately 2002.

Seleznev's career as a cybercriminal has evolved over the years. During his earliest years in the carding world, Seleznev traded in stolen personally-identifiable information such as names, dates of birth and Social Security numbers or "fullz" as that information is known in the criminal underground. The United States Secret Service ("Secret Service") began monitoring nCuX's online activities in approximately 2005. Through the review of underground forums, the Service learned that nCuX had been active on several carding forums including Carder.org, Vendors Name, and CarderPlanet since 2002. In approximately 2007, nCuX began selling stolen credit card data on a retail level, and between 2007-2009, he regularly advertised large volumes of stolen credit cards by placing advertisements on the carding forums for "dumps," a slang term for stolen credit card data, to customers who would later use the stolen data to commit fraud.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Between 2007 and 2009, nCuX developed a reputation in the carding community as a reliable source of stolen credit card data for the criminal underground and he became a top tier target of the Secret Service.

Seleznev stole his dumps by intruding into the credit card processing systems of small businesses. As witnesses explained at trial, Seleznev and his associates exploited a vulnerability that arose when businesses allowed off-site information technology services to remotely access their point of sale systems through entry points known as open "ports." Seleznev and his associates scanned the internet for open ports and intruded into the computers through these access points. They then infected the systems with malware that captured all the credit card data transiting the systems during payment transactions and sent the data to servers controlled by Seleznev.

By 2009, nCuX had become one of the world's leading providers of stolen credit card data. PSR ¶ 12. He was revered in the carding underworld and admired by thousands of other criminals.

Federal agents eventually developed evidence that Roman Seleznev, the son of a Russian politician, was the true identity behind nCuX. On May 19, 2009, agents with the Secret Service and the FBI met with representatives of the Russian Federal Security Service (FSB) in Moscow, and presented substantial evidence of defendant's computer hacking activities including his credit card hacking and other computer crimes. U.S. law enforcement provided the FSB with defendant's online alias names and information that they believed nCuX's true name was Roman Seleznev of Vladivostok, Russia. The agents' attempt at international coordination backfired. Just one month later, on June 21, 2009, nCuX notified his co-conspirators on multiple criminal forums that he was going out of business. Shortly after that, nCuX completely disappeared from the Internet. PSR ¶ 12.

As U.S. Probation noted, the information that U.S. law enforcement was investigating Seleznev "clearly got back to Mr. Seleznev." Indeed, Seleznev had his own

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

contacts inside the FSB. In chat messages between Seleznev and an associate from 2008, Seleznev stated that he had obtained protection through the law enforcement contacts in the computer crime squad of the FSB. Later, in 2010, Seleznev told another associate that the FSB knew his identity and was working with the FBI.

2. Track2 and Bulba

While Seleznev abandoned the "nCuX" nickname, he did not get out of the carding business. To the contrary, he expanded his operations under the nickname "Track2." In September 2009, Seleznev took his carding enterprise to the next level with a major innovation: the automated vending website. As shown at trial, Seleznev's automated vending websites, known as the "Track2" and "Bulba" sites, functioned like an Amazon.com for carders, allowing buyers to automatically search, select, and purchase credit card data by choosing criteria such as financial institution or card brand. Automated vending sites increased the efficiency credit card data trafficking, and remain the gold standard for credit card trafficking to this day.

The Track2 and Bulba websites achieved instant success, and were perhaps the leading source of stolen credit data during the period they operated. For example, on a single day in April 2011, Track2 posted 1 million "fresh dumps" (stolen credit card numbers) for sale. *See* Trial Exhibit (hereafter Tr. Ex.) 2.3, at 13. A Secret Service agent testified that in 2010, Track2 was the exclusive dumps vendor for Carder.su— one of the world's largest carding forums, with approximately 25,000 members. Trial Transcript (hereafter "Tr.") at 939-946.

Seleznev operated the Track 2 and Bulba websites until late April 2011, when he was injured in a terrorist bombing in Marrakesh, Morocco. Following the bombing, Seleznev was evacuated by an emergency flight to Moscow, where he was hospitalized for several months. Seleznev's co-conspirators continued to operate the Track2 and Bulba websites after the accident until January 2012, when they closed the site, citing an absence of new dumps.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

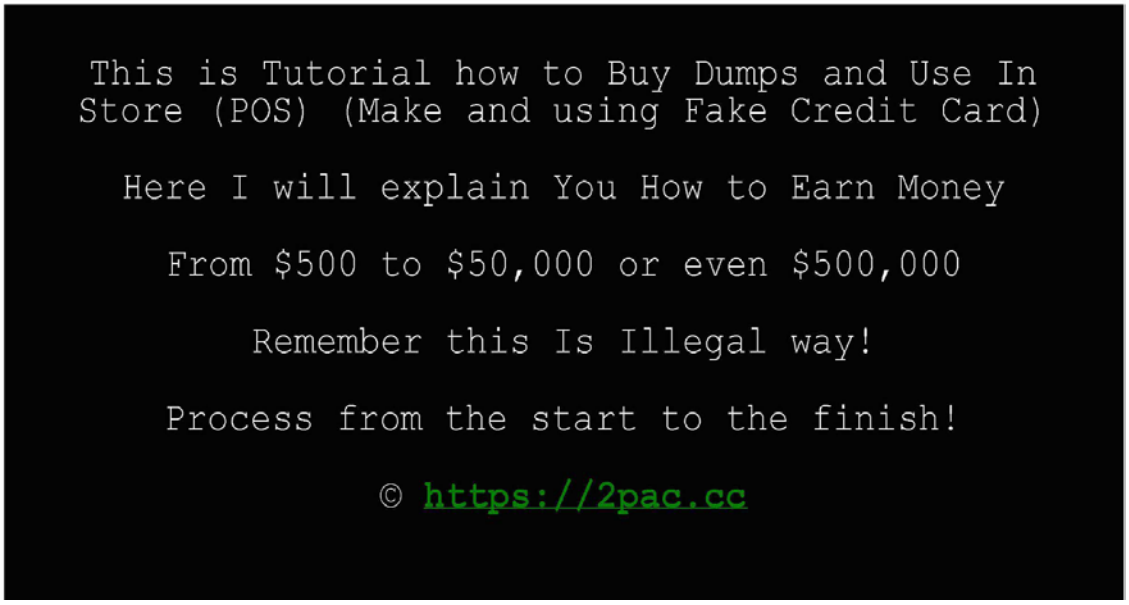
3. 2Pac and POS Dumps

After recovering from his injuries, Seleznev chose to return to the carding business again. This time he adopted the nickname "2Pac," after the hip-hop artist Tupac Shakur, whose likeness Seleznev used in advertisements on carding forums. Seleznev's 2Pac website was an automated vending site similar in many respects to his Track2 and Bulba sites. As 2Pac, however, Seleznev introduced two new innovations to his business.

First, the 2Pac site operated not only as an outlet for credit card data stolen by Seleznev himself (as the Track2/Bulba website had done), but also as a clearinghouse for data stolen by *other* major hackers all over the world. Seleznev advertised the 2Pac website as offering dumps from "the best sellers in one place." Under this reselling service, Seleznev agreed to offer other hackers' stolen credit card data on the 2Pac site. In return, Seleznev and the hacker would split the proceeds of each sale of stolen data. In this manner, Seleznev resold credit data stolen by some of the world's most notorious hackers, including data stolen in the breaches of Target, Michaels, and Nieman Marcus.

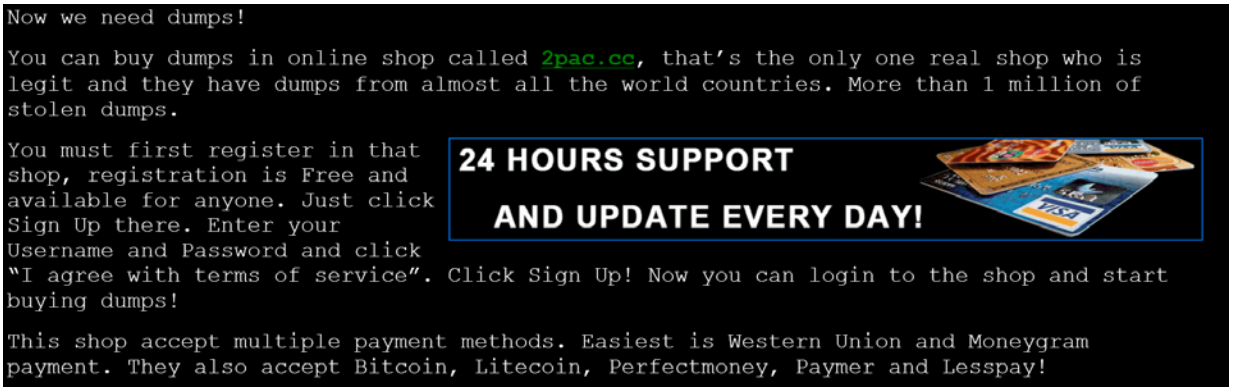
Second, Seleznev also opened a second website intended to increase the demand for stolen credit card data by training new street-level criminals on how to commit credit card fraud. Seleznev called this website "POS Dumps." The header of POS Dumps speaks for itself:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



Just as advertised, the POS Dumps website offered newcomers to carding a step-by-step guide on how to commit credit card fraud. It showed criminals-in-training what tools they needed to encode blank cards with stolen data, and provided links to websites where they could purchase these tools. POS Dumps distributed software Seleznev created (known as the "Jerm") to write the data onto blank cards. POS Dumps also provided other tips, such as how to determine a cardholder's ZIP code or the available credit balance on a credit card.

After training the viewers in the basics of credit card fraud, POS Dumps directed users to the 2Pac website to purchase stolen credit card data – promoting the vending site with glowing recommendations and linked advertisements:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

POS Dumps was an immediate hit: in its first month in operation (June 2014), POS Dumps was visited 4,498 times by 3,369 unique visitors. Tr. Ex. 13.14.

B. Seleznev Lived an Extravagant Lifestyle at the Expense of His Victims.

Seleznev made tens of millions of dollars through his fraud. He collected payments via online payment systems including Bitcoin, Liberty Reserve and WebMoney. Because these payment systems were designed to protect user anonymity, law enforcement will never know how much money Seleznev collected in total. However, one of these payment systems—Liberty Reserve—was seized by the government in connection with another criminal investigation. Liberty Reserve records show that Seleznev collected approximately $17 million in sales in approximately three years, 2010 – 2013, through this one payment system alone. Seleznev undoubtedly collected many millions more using Bitcoin and other currencies throughout his lengthy criminal career.

Seleznev used this money to live an extravagant lifestyle. He purchased two properties in Bali, Indonesia and jetted between Bali and Vladivostok at will. Photographs on Seleznev's phone show his associates with large bundles of cash, at luxurious resorts, and posing for photographs next to high-end muscle cars. Immediately before his capture, Seleznev spent over $20,000 to stay in a resort in the Maldives, boasting to an associate in a chat that "I took the most expansive villa" and that "I have my own manservant."

Seleznev's lifestyle came at a great cost to his victims, which included the owners of the small businesses Seleznev attacked, and the financial institutions that issued the cards he stole. At trial, the Court heard testimony from seven owners of businesses that Seleznev attacked. The witnesses described the tremendous losses that result from an intrusion, which include lost business while the point-of-sale system is down, the reputational damage that occurs when customers learn that a business has fallen victim to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

an attack, and the audit fees, fines and other costs associated with remediating the damage.

For example, CJ Saretto was the owner of Seattle's Broadway Grill, a Capitol Hill restaurant that had operated for over 20 years before the attack. Saretto testified that the breach had an "instantaneous" effect on his business, reducing revenue by 40%. Tr. 1157-58. Saretto testified that Broadway Grill was profitable before the breach, but that the attack sent the business into a "spiral" that ended in bankruptcy. *Id.* Ultimately, Saretto, testified, he was required to "walk away from the business, shutter the doors, filed personal bankruptcy. It was pretty devastating." *Id.* Sid Fanaroff, the owner of the Z Pizza chain, testified that the effect on his business was "horrendous," and that he experienced a "nervous breakdown" following the intrusion. *Id.* at 1236. Diane Cole, owner of the Casa Mia Italian restaurant in Yelm, testified that, following the attacks, the business had to use its "payroll money" to cover the costs it incurred responding to the intrusion. Tr. 1184. And City News Stand owner Joe Angelasteri told the jury that, six years after Seleznev's attacks, he was still trying to pay down the debt he incurred remediating the intrusion. Tr. 1191.

These were just a few of the hundreds of businesses victimized by Seleznev. The Presentence Report describes how defendant damaged several more. PSR ¶ ¶ 34-36. For example, the Houston Zoo was required to forego specific planned upgrades to its facilities that would have "benefitted its millions of guests, improved the work environment of its staff, and enhanced the lives of its animals." PSR ¶ 35. The owner of a market in Old Bridge, New Jersey, spent thousands of dollars in response to the attack and reports that "business has never been the same." *Id.* ¶ 34.

On top of this damage, Seleznev imposed staggering costs on the banks and credit unions that issued the credit cards he misused. The government was able to identify 2,950,468 unique credit card numbers that Seleznev stole, possessed or sold. Tr. 1197. These include the card numbers recovered from Seleznev's laptop, the Virginia-based

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

"HopOne" server, a server Seleznev operated in the Ukraine, and the server he used to host the 2Pac website. Tr. 1195. The 3,700 banks and credit unions that issued these cards report a total *known* fraud loss of approximately $170 million for those cards. PSR ¶ 28. In addition to the known losses, there are undoubtedly many more stolen card numbers the government did not identify, and additional fraud on the known cards that was not detected by cardholders or the financial institutions.

C. The Indictment and Capture of Roman Seleznev

The grand jury charged Seleznev in a sealed indictment on March 3, 2011. Seleznev remained at large for over three years. During this period, Seleznev carefully evaded apprehension, employing practices like buying last-minute plane tickets to avoid giving authorities advance notice of his travel plans. Seleznev obtained an account with the U.S. Court's PACER system, which he monitored for criminal indictments naming him or his nicknames. He avoided travel to countries that had entered into extradition treaties with the United States. Indeed, when Seleznev was finally confronted by U.S. agents in the Maldives, his first words were to question whether the United States had an extradition treaty with the Maldives. Tr. 231.

The circumstances of Seleznev's capture demonstrate the extreme difficulty of apprehending foreign cybercriminals. On July 1, 2014, the United States received information that Seleznev was vacationing in the Maldives, and would be departing from that country on July 5, 2014. This provided agents four days to (1) seek internal U.S. 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 18-hour flight from Hawaii); (4) coordinate the logistics of the apprehension with the local authorities; (5) arrange for private transportation (a private jet sufficient range to fly many thousands of miles over water) to take Seleznev to the nearest U.S. territory; and (6) take custody of Seleznev.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

As a result of extraordinary efforts by the Secret Service, the Departments of Justice and State, and Maldivian authorities, the government was able to clear these hurdles, and took Seleznev into custody on July 5, 2015. However, in imposing sentence, the Court should consider the near-impossibility of apprehending Seleznev again if he returns to crime after his release.

D. Seleznev's Litigation Conduct

1. Seleznev's False Testimony

The Court should also consider Seleznev's obstructive and intransigent conduct during this prosecution. First, Seleznev provided perjured testimony to this Court and the district court in Guam, where he made his initial appearance. In an effort to persuade the Court to release him, Seleznev stated in a sworn declaration (in Guam) and in sworn testimony (to this Court) that the arresting agents physically abused and mistreated him. Three federal agents testified at the hearing, however, that no one so much as raised their voice with Seleznev. To the contrary, Seleznev was allowed to smoke cigarettes and use silverware, and was even given his choice of entrée on the flight to Guam. Based on this testimony and photographic evidence consistent with it, the Court made a finding that Seleznev's claims of abuse were not credible.

Defendant also perjured himself at the evidentiary hearing on his motion to limit the government's use at trial of statements Seleznev made during a December 2015 interview. The hearing focused on whether the terms of Seleznev's written agreement with the government had been properly explained to him by his former attorneys. Seleznev testified that he was never provided a copy of the agreement translated into Russian. However, Seleznev's former attorneys produced a copy of the agreement that they had had translated into Russian (which contained a fax header showing it was sent to them the night before they met with Seleznev), and both attorneys testified they remembered providing the translated agreement to Seleznev. The attorneys also testified that they clearly explained the agreement's derivative use provisions to Seleznev, while

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Seleznev denied that they did so. In a written order, the Court stated that, having observed the testimony, it credited "counsel's version of the facts." Dkt. 327 at 5. Thus, Seleznev provided demonstrably false testimony at two different hearings.

2. Other Obstructive Conduct

Seleznev repeatedly attempted to manipulate and protract these proceedings, resulting in a cumulative delay of 26 months, and six sets of counsel, between his capture and trial. For example, the Court will recall that the evidentiary hearing on Seleznev's motion to dismiss was originally set for May 13, 2015. Transcripts of jail calls previously submitted to the Court reveal that, in the days leading up to the hearing, Seleznev and his father resolved to delay the hearing so that they could work on a secret strategy they elliptically referred to as "Uncle Andrey's option." To manufacture the delay, Seleznev's father suggested that Seleznev either "get sick" or "completely stop the communication with the lawyers." Dkt. 185 at 5. Sure enough, two days before the hearing, Seleznev's attorneys filed a motion to withdraw, purportedly because of a breakdown in communication. To accommodate the last-minute change in counsel, the Court was forced to move the hearing from May to November 2015. This delay imposed significant public expense, as witnesses had already travelled to Seattle from Sri Lanka, Honolulu, Chicago, and Washington, DC.

Seleznev abused the judicial system in other ways as well. After first retaining a large New York law firm, followed by a high-end Seattle litigation boutique, Seleznev then requested CJA counsel in February 2015, suddenly claiming that that he did not have funds to pay for his own defense. The government objected to this expenditure of public funds, noting that Seleznev had earned millions of dollars through his criminal activities, and clearly had access to vast resources just before his arrest. After Seleznev insisted that he had no remaining financial resources, the Court appointed the Federal Public Defender, and later, the Calfo Harrigan law firm, to represent Seleznev at public expense. However, when Seleznev became dissatisfied with these attorneys, he

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

miraculously obtained access to funds sufficient to retain the law firm of John Henry Browne, followed by his current New York-based attorney.

Seleznev now claims he has accepted responsibility for his crimes. However, before the jury convicted him of 38 counts, he made every effort to shirk responsibility for not just his misconduct, but also his previous admissions of guilt. For example, prior to trial he asked the Court to allow his attorneys to affirmatively misstate the facts of this case to the jury. In seeking to limit the government's use of the statements he made in his December 15, 2014 interview, Seleznev sought permission for his attorneys to contradict his confession without risk of being impeached by his prior admissions of guilt. As the Court found, it was "duty bound to protect the integrity of the proceeding" and specifically prohibited Seleznev's attorneys from contradicting Seleznev's confession, but Seleznev's efforts to escape these fundamental principles further demonstrate his conscious and ongoing efforts to obstruct the trial proceedings in this case.

E. The Trial and Verdict

This matter was presented to a jury over eight trial days beginning on August 15, 2016. On August 25, after less than a day of deliberations, the jury convicted Seleznev of 38 felony counts, acquitting Seleznev of two counts (counts 11 and 20) relating to victim Red Pepper Pizzeria. The jury convicted Seleznev of three other counts (counts 28, 39 and 40) relating to Red Pepper Pizzeria. In all, defendant was convicted of 10 counts of Wire Fraud, eight counts of Intentional Damage to a Protected Computer; nine counts of Obtaining Information From a Protected Computer Without Authorization, nine counts of Access Device Fraud, and two counts of Aggravated Identity Theft.

III. SENTENCING GUIDELINES

A. Guideline Calculation

The government calculates Seleznev's guideline range as follows:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Item	**Adjustment**	**Provision**
Base offense level	+7	2B1.1(a)(1)
Loss in excess of $550 million	+30	2B1.1(b)(1)(P)
10 or more victims	+2	2B1.1(b)(2)(A)
Receipt of stolen property	+2	2B1.1(b)(4)
Scheme committed from outside of the U.S.	+2	2B1.1(b)(10)
Trafficking in unauthorized access devices	+2	2B1.1(b)(11)[1]
Defendant derived more than $1 million from financial institutions	+2	2B1.1(b)(16)(A)
Conviction under 18 U.S.C. § 1030 with intent to obtain personal information	+2	2B1.1(b)(17)
Conviction under 18 U.S.C. § 1030(a)(5)(A)	+4	2B1.1(b)(18)
Organizer/leader	+4	3B1.1(c)
Obstruction of justice	+2	3C1.1
Total	**59**	

Even with a Criminal History Category of I (which substantially understates Seleznev's history given that he has been involved in crime his entire adult life), this results in a guideline range of **life**.

[1] U.S. Probation did not include this enhancement in its initial calculations and the government did not notice the absence of this enhancement prior to the release of Probation's final presentence report. Nonetheless, this enhancement fits squarely to Seleznev's misconduct as trafficking in unauthorized access devices goes to the very essence of his scheme.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

B. Defendant's Objections to the Offense Level Calculations

Defendant complains that the loss amount overstates the seriousness of the offense. He also complains that the Guideline enhancements unfairly overlap, resulting in a cumulative effect that overstates the seriousness of the offense. Defendant's objections are without merit for the reasons set forth below.

1. Loss Amount

The United States Sentencing Guidelines provide that "in a case involving any counterfeit access device or unauthorized access device, loss includes any unauthorized charges made with the counterfeit access device or unauthorized access device and **shall not be** less than $500 per access device." USSG § 2B1.1, Application Note 4(F) (emphasis added). According to Secret Service Investigative Analyst Megan Wood, the government found approximately 2.9 million stolen credit cards in defendant's possession over the course of this investigation. Tr. at 1197. That results in a loss amount of over $1.4 billion.

In *United States v. Onyesoh*, the Ninth Circuit held that in order to apply the $500 per access device loss amount calculation, the government must present some evidence that the devices in question were usable. *United States v. Onyesoh*, 674 F.3d 1157, 1159-1160 (9th Cir. 2012). In *Onyesoh*, Postal Inspectors had searched defendant's home and found a spreadsheet containing a list of 500 expired credit card numbers. *Id*. at 1157. Noting that the credit card trafficking statute "is intended to target major fraud operations instead of individual use of "an expired or revoked card" the Ninth Circuit found insufficient evidence to apply the $500 per card enhancement. *Id*. at 1158-1160. Unlike *Onyesoh*, Seleznev's operation is the epitome of a "major fraud operation" and the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

evidence shows beyond a reasonable doubt that at the time he hacked the credit card numbers in this case and sold them on his vending sites, the cards were in fact useable.[2]

The credit cards Seleznev stole were in active use at the time he hacked them, and the extraordinary losses tied to his scheme show the cards were in fact useable. Seleznev was not merely in possession of a small list of expired credit card numbers. As shown by the testimony at trial, the credit card numbers defendant stole were hacked while in the process of being used at restaurants and retailers around the world. The very nature of the transactions that defendant intercepted demonstrates that these cards were useable because they were in fact being used when he stole them. *See, e.g.*, *Onyesoh*, 674 F.3d at 1160 ("a working credit card can clearly be used to obtain value. . . ."). Additionally, as demonstrated by Ms. Wood's testimony and the related exhibits calculating the losses tied to the cards found in Seleznev's possession, the cards he sold were subsequently used to commit over $169 million in actual fraudulent transactions. Together, this evidence shows that at the time defendant stole the credit card numbers that were ultimately found in his possession, they were valid, useable credit cards, capable of causing enormous financial losses. Therefore, the Court should apply the required $500 per card minimum loss figured called for by the Guidelines.[3]

2. **Guideline Enhancements**

The enhancements do not overlap and are not unduly cumulative. Each of the enhancements applicable in this case captures a distinct aspect of Seleznev's criminal enterprise. Seleznev was not a mere mope committing street fraud with fake credit cards.

---

[2] Although the testimony at trial established that most of the cards were expired by the time of trial because nearly four years had passed since many had been found in defendant's possession, the test is whether defendant possessed them before they were expired. *See, Onyesoh*, 674 F.3d at 1160.

[3] It is worth noting, that even if the Court chose to use the actual loss amount of approximately $169 million dollars, defendant's guideline level would be 55, and the recommended range would continue to be life.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

He was the leader of a global cybercrime enterprise that used sophisticated hacking tools and a complex international computer infrastructure to steal the private financial data of millions of victims. His hacking scheme targeted hundreds of businesses and caused massive financial losses to thousands of businesses. He was also a sophisticated criminal visionary who devised an efficient and successful marketplace for stolen data. Each of these are aggravating factors that independent sections of Section 2B1.1 of the Guidelines seek to quantify as part of the guideline calculations.

Seleznev was a market leader in the business of obtaining stolen credit card data by hacking that data and selling it to other criminals. The magnitude of the loss is an independent variable and the guideline enhancement for loss is designed to capture that variable. As a result, the enhancements for the number of victims, the sophisticated and international nature of the crime, defendant's conviction for computer crimes involving damage to computers, his involvement in trafficking in stolen credit cards, his targeting of personally identifiable information and other enhancements do not improperly duplicate the enhancement for the loss amount. Contrary to defendant's conclusory arguments, each of these enhancements captures a unique variable that the United States Sentencing Commission carefully considered and determined constituted a separate aggravating factor. To accept defendant's argument that the enhancements unfairly overlap, the Court would effectively invalidate Section 2B1.1 of the guidelines. Because the enhancements each capture a unique aspect of Seleznev's criminal behavior, his arguments are without merit.

C. Leadership Adjustment

Probation has not recommended a leadership adjustment, stating that Seleznev's "leadership of others is unclear." Under 3B1.1(c), the Court is to apply a four-point enhancement if the defendant was "an organizer or leader of a criminal activity of five or more participants or was otherwise extensive." The evidence introduced at trial clearly established these conditions.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

First, the evidence established that Seleznev was the organizer or leader of a criminal activity. For example, a chat recovered from Seleznev's computer showed Seleznev describing himself as the "owner of 2Pac." Trial Ex. 13.2. Forensic evidence showed that Seleznev held the "administrator" credentials for the 2Pac website, and repeatedly logged on to various carding forums under the name "2Pac." *See, e.g.*, Trial Exs. 13.12c (credentials list); 13.18 (web history showing Seleznev logged into Omerta website as "2Pac"). Also instructive are the statements made by Seleznev's subordinates on the 2Pac website *after* Seleznev was arrested. One month after the arrest, a notice was posted on the website stating that "we apologize by the fact that there are no updates and the checker doesn't work. This is due [to] the fact that our *boss* had a car accident and he is in hospital . . . . Support [is] always available." Tr. Ex. 10.3 (emphasis added). This is similar to the operations of Track2 in the aftermath of Seleznev's bombing accident: others attempted to carry on the business of Seleznev's automated vending site but they were not able to effectively operate it without Seleznev, and ultimately closed it down. All of this evidence makes clear that Seleznev was the ringleader of the Track2 and 2Pac operations and that he had others in his employ to help run his operations.

The evidence also easily established that the criminal activity was "extensive" within the meaning of USSG § 3B1.1(a). In determining whether a criminal activity is "extensive," the Court's consideration is not limited to the size of the criminal organization itself. Rather, "all persons involved during the course of the offense are to be considered. Thus, a fraud that involved only three participants but used the unknowing services of many outsiders could be considered extensive." USSG § 3B1.1(a) cmt 3. The Track2 and 2Pac websites served as hubs for the criminal activity of a large number of people, even if only a handful of them were actual employees of Seleznev. While the exact number of people directly working for Seleznev is unknown, hundreds or perhaps thousands of criminals purchased credit cards from the sites, tens of other sellers offered their stolen numbers on the 2Pac vending site, thousands learned from his POS

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Dumps tutorial site, and millions of card numbers were stolen and offered for sale as part of the scheme.

Seleznev also used numerous other services (both criminal and legitimate) to facilitate his criminal enterprise including: bullet-proof hosting services for his websites; DDOS protection services for his websites; checking services he provided for his customers to validate the stolen cards he sold; online currency services such as Liberty Reserve and WebMoney for payment processing; and advertising on numerous carding forums designed to promote his business. For example, the evidence at trial showed defendant used multiple DDOS protection services to mitigate attacks from competing carders. *See* Tr. Exs. 6.4, 6.5, 6.13 (e-mail communications with DDOS protection services for the Track2 website). Other evidence showed defendant negotiating over the price for advertisements promoting his vending site 2Pac.cc on carding forums. *See* Tr. Ex. 13.25 (chat with "marysnow" regarding advertising for 2Pac.cc). And cached web pages found on his computer showed Seleznev used "checking services" to confirm the validity of credit card data he was selling. *See* Tr. Ex. 13.19 (recovered image of website Try2Check.me showing user 2Pac logged in). By any measure, the criminal activity was extensive and, coupled with Seleznev's role as organizer or leader, this supports a 4 level aggravated role adjustment.

IV. RATIONALE FOR SENTENCING RECOMMENDATION

The government recommends a total sentence of 30 years imprisonment in light of all the factors set forth in Title 18, United States Code, Section 3553(a). Notably, this is a significant variance from the Guideline recommendation of life. Defendant has already served nearly three years pending trial and, with credit for good time, will be released when he is still in his 50's. Upon release, he will be deported to Russia and, therefore, not subject to the supervision of U.S. Probation. The government shares the hopes of U.S. Probation that upon his return, defendant will reassess his earlier choices and resume

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

his life in a law abiding manner. But the high probability that he will return to his life as a criminal mastermind requires a substantial sentence of 30 years.

A. The Nature and Circumstances of the Offense

The nature and circumstances of this offense are unprecedented in this District and perhaps throughout the country. Seleznev is the highest profile long-term cybercriminal ever convicted by an American jury. His criminal conduct spanned over a decade and he became one of the most revered point-of-sale hackers in the criminal underworld. Carders all over the world turned to defendant to fuel their fraudulent conduct, leading to over $169 million in losses to over 3,700 banks worldwide. His hacking spree wreaked havoc at hundreds of small businesses throughout the United States and overseas as he scooped up millions of credit cards.

Unlike smaller players in the carding community, Seleznev was a pioneer in the industry. He was not simply a market participant – he was a market maker whose automated vending sites and tutorials helped grow the market for stolen card data. His final vending site, 2pac.cc became one of the leading marketplaces for stolen credit card data and sold stolen data from some of the most significant credit card breaches of the last decade.

Seleznev developed a criminal enterprise that was illegal on its face and made no pretentions of legitimacy. As shown by his POSdumps.com tutorial, Seleznev boldly proclaimed the illegality of his business with statements like "remember this is illegal way." His websites were wholly dedicated to the sales of stolen credit card data. He blatantly flaunted his illegal behavior knowing that his true identity was hidden behind the layers of anonymity provided by the internet. And even if his true identity was discovered by law enforcement, he was further comforted by the cover provided him by his connections in Russian law enforcement.

Seleznev's hacking was particularly predatory in that it targeted vulnerable small businesses that were ill-suited to defend against his attacks and struggled to recover from

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the damages he caused. Throughout much of his career, Seleznev primarily targeted businesses in the restaurant and hospitality industry. He quickly learned that many of these businesses' point of sale systems were remotely maintained by vendors with poor password security. Because most of his victims were small businesses, they were unlikely to have in-house IT or security personnel. As a result, these companies made extremely attractive targets for someone with Seleznev's skills as a hacker. Testimony from victim businesses and victim impact statements from others who could not attend trial describe how these businesses were forced to incur substantial expenses for incident response, private forensic investigations, fines from Visa and MasterCard and lost revenue resulting from the damage to their reputations. Several of the businesses described these impacts as devastating and some were even forced out of business.

The guideline calculations in this case reflect the unique and aggravating nature and circumstances of this case. Rarely will a case under the fraud guidelines result in such a high offense level. In this case, the complex international nature of defendant's scheme coupled with the extraordinary losses caused by his criminal enterprise result in an offense level of 59. This accurately and appropriately captures the essence of Seleznev's crimes.

Unlike more mundane schemes to defraud, Seleznev's crimes used the power of the internet to magnify the effectiveness of his attacks. His use of specialized computing skills to attack hundreds of businesses, steal massive volumes of personal data and traffic in that data shows the guideline calculations have accurately captured the nature and circumstances of the offense. Likewise, Seleznev's ability to orchestrate this scheme from Russia and Indonesia while attacking victims throughout the world highlights the sophisticated nature of his criminal enterprise.

These facts demonstrate the nature and circumstances of this case are extraordinary and weigh heavily in favor of a substantial prison term. A sentence of 30

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

years is necessary to reflect the severe nature and circumstances of Seleznev's criminal enterprise.

B. Defendant's History and Characteristics

Seleznev has been a cybercriminal his entire adult life. He began his career in carding when he was 18 years old and assumed the online name of nCuX. He is still a relatively-young man who is extremely intelligent and highly prolific. Although he has no prior criminal history, he is a career cybercriminal who is respected and looked up to by other cybercriminals around the world.

With the profits of his criminal enterprise, Seleznev has led a life of luxury. He purchased multiple homes in Bali, Indonesia and also owns apartments in Moscow and Vladivostok, Russia. He has purchased high-end muscle cars and prior to his capture, he frequently vacationed at expensive resorts including his last vacation in the Maldives where he stayed in a $1,400 a night hotel room on the beach. Tr. Ex. 13.5. Despite his apparent wealth, defendant sought and obtained court-appointed counsel for much of these proceedings before suddenly coming up with funds to pay private counsel at trial.

As U.S. Probation has noted, Seleznev had multiple opportunities to reassess his life and end his career as a hacker. The first was when U.S. law enforcement agents went to Russia and met with Russian law enforcement regarding Seleznev's activities as nCuX. Despite acknowledging to his co-conspirators that he had been tipped off by the FSB, Seleznev merely abandoned his original alias and began building new criminal infrastructure under new alias names of Track2 and Bulba. The second opportunity was after defendant was injured in 2011 as the result of a terrorist bombing in Morocco. Yet again, defendant simply returned to his life as a hacker as soon as he recovered. In each instance, defendant not only returned to his criminal ways, but also grew his criminal enterprise as he took it to new heights.

Throughout this case, defendant has abused the process and engaged in conduct that obstructed the proceedings. From the very beginning of this case, Seleznev pursued

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

frivolous litigation for the purposes of delay, including a fruitless effort to dismiss his charges in Guam that delayed his transfer to this District for over a month after his arrest. Once in the Western District of Washington, he spent nearly three years burning through attorney after attorney. While he now claims he only went to trial based on the bad advice of his attorneys, recorded calls from the FDC between defendant and his father demonstrate his attorneys repeatedly encouraged him to negotiate a plea agreement, and each time he was given this advice, he became frustrated with counsel, insisted on going to trial, and ultimately fired each successive set of attorneys. Although he now freely admits he is guilty, he pursued motions to suppress evidence based on misleading arguments that the government or some unknown super hacker had planted evidence on his computer. Given this extensive history of obstruction and obfuscation, it is clear that defendant's newfound perspective on his misconduct is entirely opportunistic.

Not only do defendant's history and characteristics reflect an individual who has an arrogant and disdainful attitude towards the U.S. justice system, they also reflect an individual with an unflinching willingness to steal from others. It gave Seleznev no pause that he was victimizing millions of individual credit card holders, thousands of financial institutions, and hundreds of businesses around the world. It takes a particularly callous individual to center their whole life on stealing from others.

Defendant poses an extremely high risk of recidivism. Given his stubborn refusal to accept responsibility for his crimes until hopelessly cornered, there is a high likelihood that upon his return to Russia, he will return to his criminal enterprise. In light of his history and characteristics, it is important that the sentence imposed shows the defendant that the costs of engaging in these crimes significantly outweigh the benefits he enjoyed for so many years. Therefore, a sentence of 30 years is necessary and appropriate in light of defendant's history and characteristics.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

C. The Need for the Sentence Imposed to Reflect the Seriousness of the Offense, to Promote Respect for the Law, and to Provide Just Punishment for the Offense

A sentence of 30 years should be imposed to reflect the seriousness of the offense, promote respect for the law, and provide just punishment for the offense. Computers, the internet and electronic information storage are an integral part of the U.S. economy. Consumers and businesses alike transmit and store ever increasing quantities of private information and financial data over the internet every day. The expansion of the internet and computer networks has brought great benefits to the economy and opened up new opportunities for millions of people. Unfortunately, this digital revolution has also created new and unprecedented opportunities for criminals to steal information and money on a scale and at speeds that were impossible in the physical world. The internet has opened a new frontier for criminals unbounded by traditional borders or physical barriers. Hackers like Seleznev can commit their crimes from around the world without ever facing their victims face to face, and can use any number of techniques to conceal their identities.

Point-of-sale hackers particularly, maximize their profits by quickly and efficiently bringing their stolen goods to market before banks have an opportunity to shut down the stolen credit cards. Seleznev was an expert at building and maintaining automated vending sites that facilitated these rapid and profitable sales. As he moved from selling his own stolen credit cards to operating his 2pac.cc clearing house for other hackers, he helped create a sustainable market for millions of stolen credit cards causing untold damage to hundreds of businesses and thousands of banks. Yet, the damage Seleznev was capable of causing in just hours, takes victims and law enforcement months, and sometimes years, to understand, analyze and successfully investigate and prosecute.

Seleznev's global hacking enterprise presented a serious threat to the viability of businesses and financial institutions all over the world, as well as the security of their

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

customers' private financial data. His crimes disrupted the economy by undermining trust in the systems and networks necessary for the healthy operation of businesses everywhere. Those who would commit such crimes should be put on notice that they will face substantial prison sentences that are commensurate with the loss and damages they cause. A sentence of 30 years in a case such as this, involving over $169 million in actual known losses, a recalcitrant defendant like Seleznev and thousands of victims, will appropriately reflect the seriousness of the crimes, promote respect for the law, and provide just punishment for the offenses.

D. The Need for the Sentence Imposed to Afford Adequate Deterrence and Protect the Public From Further Crimes of the Defendant.

In light of the massive profits generated from Seleznev's scheme and the difficulty of identifying and capturing international cybercriminals like Seleznev, a sentence of 30 years is necessary to afford adequate deterrence and protect the public from further crimes of defendant. Cybercriminals like Seleznev can make millions of dollars in a very short time period hacking computers and stealing personal financial records. The lure of such easy money in countries with spotty records of cooperating with U.S. law enforcement is substantial. Many may make the calculation that the rewards are worth the risk when their government is unlikely to extradite them to face justice in the United States. Seleznev's prosecution in particular has been watched carefully throughout the cybercrime world. His capture in 2014 was a rare victory in the fight against Eastern European cybercriminals. The worldwide media has covered Seleznev's arrest and prosecution closely and frequently highlighted the difficulties of identifying and capturing a criminal like Seleznev. As a result, his sentence will be widely known in the hacking community. A sentence of 30 years will send a strong message that cybercriminals face stiff penalties regardless of whether they are operating in the United States or abroad.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

As demonstrated through the exhibits and trial testimony in this case, computer hacking crimes are extremely difficult to solve. Identifying the hacker behind the keyboard takes unique investigative expertise and attention to detail. The investigations almost universally require the collection of evidence from sources all over the world. Electronic evidence often disappears before the legal and diplomatic procedures necessary to retrieve the evidence can be completed. Even when law enforcement can successfully identify a cybercriminal, many hackers reside in countries like Russia that will not extradite their citizens to face justice in the United States where their crimes have had the most impact. Therefore, it can be even more difficult to capture a cybercriminal than it is to identify him. In the rare instances in which the United States can bring a hacker of Seleznev's stature and significance to justice, the sentence must be significant to afford adequate deterrence. A sentence of 30 years is necessary in light of these compelling factors.

A sentence of 30 years is likewise necessary to protect the public from further crimes of the defendant. Upon his release, defendant will be immediately deported to Russia and will not be under any active supervised release. As noted above, despite multiple opportunities to stop his criminal behavior, Seleznev repeatedly returned to his hacking enterprise. Therefore, the likelihood of recidivism is substantial. Additionally, in light of his history of contacts with Russian law enforcement, he is likely to act with impunity upon return to Russia. Because he cannot be extradited from Russia and will likely be even more careful in his travels than before, if he returns to his criminal enterprise, he will forever remain beyond the reach of U.S. law enforcement. Therefore, a sentence of 30 years will serve to protect the public from further crimes of defendant.

E. The Need to Avoid Unwarranted Sentence Disparities Among Defendants with Similar Records Who Have Been Found Guilty of Similar Conduct

It is impossible to identify a fitting local comparison for this sentencing because Seleznev has no peer in this district. Nobody has ever been convicted of such serious

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

computer and financial crimes in the history of the Western District of Washington. The closest possible example was the prosecution of David Benjamin Schrooten in 2012. *United States v. Schrooten*, CR12-085RSM (W.D. Wa.). Schooten was also a carder who was active in the international carding community and operated a carding website between 2011 and 2012. While Schrooten was engaged in crimes similar to Seleznev, he was a much less significant participant in the carding world. Schrooten possessed approximately 100,000 stolen credit cards (3% of the number possessed by Seleznev), resulting in a guideline loss amount of $63 million for purposes of sentencing. As part of an 11(c)(1)(C) plea agreement, Schrooten agreed to a sentence of 144 months (12 years) and was sentenced on February 1, 2013, by the Honorable Ricardo S. Martinez.[4]

Perhaps the most similar defendant prosecuted in another district was defendant Roman Vega, who in December 2013, was sentenced to 18 years following a guilty plea with cooperation. *United States v. Roman Vega*, (E.D.N.Y.). Although he was not sentenced until 2013, Vega was originally arrested in Cyprus in 2003 and remained in custody from there forward. Much of his criminal activity took place in the 1990s. Mr. Vega was one of the early pioneers of the carding community having co-founded one of the original carding websites – CarderPlanet. Like Seleznev, he also operated a vending site of his own where he trafficked in stolen credit card data. At the time of his arrest, Vega had a laptop computer with approximately 500,000 credit cards in his possession.

Following his extradition from Cyprus, Vega was initially transported to the Northern District of California where he pleaded guilty to 20 counts of wire fraud related to his carding activity in November 2006. He was subsequently transferred to the Eastern

---

[4] The government refers to the *Schrooten* case and the cases discussed below to inform the Court of other prosecutions that are pertinent to the issues of sentencing disparity. However, the government is mindful that each defendant was sentenced on the unique facts of their cases and that aggravating or mitigating circumstances in one case may not be present in others.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

District of New York where he faced additional charges related to his role in the CarderPlanet carding forum. In January 2009, Vega pleaded guilty to the charges in EDNY pursuant to a cooperation agreement. According to the government's sentencing memo, Vega provided historical information about his own activity and that of his co-conspirators, but because the information was dated, it was only useful as background intelligence and did not lead to any charges or arrests. Additionally, Vega breached his cooperation agreement by later moving to withdraw his plea agreement and contradicting much of what he had told the government.

After the court denied Vega's motion to withdraw his guilty plea, the government recommended a sentence of 20 years based on defendant's failed cooperation and early leadership role in the carding community. The court in EDNY sentenced Vega to 18 years and he was later sentenced in the Northern District of California to 46 months concurrent to the New York sentence. In many ways, Seleznev represents the second generation of major carders since the time during which Vega and his cohorts were involved in the CarderPlanet forum. Seleznev's innovations, including the automated vending site, built on Vega's success and took carding to a new level for the 2000s and beyond.

Before Mr. Vega, the most prolific carder to be sentenced in the United States was Albert Gonzalez. On September 11, 2009, Gonzalez was sentenced to 20 years for two hacking schemes. *United States v. Albert Gonzalez* (D. Ma. and E.D.N.Y.). Like Vega, Gonzalez was a failed cooperator who pleaded guilty but breached his cooperation agreement. In the EDNY case, Gonzalez and co-defendants hacked into point-of-sale terminals at Dave & Busters restaurants and stole approximately 7,000 credit cards. In the Boston case, Gonzalez and his crew stole approximately 45 million credit card numbers. Seleznev, while not as prolific, had a greater and longer lasting impact on the carding community than Gonzalez. Seleznev's decade-long rise to prominence in the carding community and development of automated vending sites and reseller

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

marketplaces facilitated the sales of millions of stolen cards and helped monetize some of the most significant credit card breaches of the last decade.

Finally, defendant David Camez was a member of the Carder.su carding forum and is a co-defendant of Seleznev in his pending RICO case in the District of Nevada. Camez was not himself a hacker, but was rather a purchaser and user of counterfeit identification documents and stolen credit cards. Camez was a member of the Carder.su carding forum and frequently bought stolen cards from Seleznev while Seleznev was operating as Track2. Camez used the stolen cards and false identification documents to commit fraudulent transactions throughout the Phoenix and Tuscon, Arizona areas where he lived between 2008, and his arrest in 2012. The losses tied to Camez' own fraudulent transactions was approximately $53,000.00. Because he was convicted at trial of RICO and RICO conspiracy charges, he was held responsible for the entire Carder.su loss amount of $50 million. Camez also sold stolen electronics and skimming equipment on the Carder.su website. Camez, who had a substantial criminal history placing him in Category IV, was sentenced to 20 years following a trial conviction. Seleznev, in comparison, was not simply a street level credit card fraudster. He was a key player in the market place for stolen credit cards – hacking into victim businesses, selling stolen credit card data, and maintaining a monopoly on sales of credit card data on the Carder.su forum which was one of the largest carding forums of the time. Therefore, Seleznev's sentence should be substantially longer than Camez' 20-year term of imprisonment.

With the exception of Camez, each of the other defendants listed above accepted responsibility and pleaded guilty long before trial. Vega and Gonzalez' pretrial efforts to cooperate with law enforcement also contrast sharply with Seleznev's obstructive history of delay tactics and false testimony in multiple pre-trial hearings. Additionally, Seleznev's protection from law enforcement efforts to bring him to justice bring an element of public corruption that was completely non-existent in any of the other prosecutions noted above. With these distinguishing characteristics in mind, a sentence

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

of 30 years avoids unwarranted sentencing disparities while properly and necessarily highlighting the many egregious factors present in this prosecution that were not present in other cases.[5]

V. RESTITUTION

Pursuant to Title 18, United States Code, Section 3663A, restitution is mandatory for the victims of Seleznev's criminal conduct. The evidence at trial established a total actual loss to the victim financial institutions of $169,418,843. Those losses were traced to approximately 3,700 different banks and credit unions. The United States is attaching a complete list of the financial institution victims with amounts owed and addresses for the delivery of any restitution received on a CD in Microsoft Excel format for the Clerk of the Court. *See* Attachment A. The government also received victim impact statements from fourteen of the victim businesses that Seleznev hacked along with requests for restitution and supporting documentation. These restitution requests include expenses such as incident response, private forensic investigations, fines from Visa and MasterCard, and new computer equipment. For purposes of Title 18, United States Code, Section 1030, losses include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue

[5] Although the following cases did not involve computer crimes or internationally sophisticated criminal enterprises, the court may also consider these financial crimes prosecutions from this District as illustrative of significant fraud prosecutions: *United States v. Nolan Bush*, CR06-5504RBL (defendant sentenced to 30 years following conviction at trial for $30 million investment fraud); *United States v. John Zidar*, CR01-108RSM (defendant sentenced to 24 years following conviction at trial for $73 million investment fraud); *United States v. Kevin Lawrence*, CR02-260MJP (defendant sentenced to 20 years following guilty plea in $100 million investment fraud); *United States v. Darren Berg*, CR10-310RAJ (defendant sentenced to 18 years pursuant to 11(c)(1)(C) guilty plea in $140 million investment fraud).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). In this case, the total losses to the victim businesses that requested restitution is $465,742.95.

VI. FORFEITURE MONEY JUDGMENT

As part of the Second Superseding Indictment in this case, the grand jury returned forfeiture allegations that seek the forfeiture of any property constituting or derived from proceeds obtained directly or indirectly as a result of the offenses and any property used in any manner to commit or facilitate the offenses. The property to be forfeited included a money judgement representing the proceeds Seleznev obtained as a result of the offenses charged in the Second Superseding Indictment. The evidence at trial established that Seleznev received $17,886,971.09 in proceeds from the sales of stolen credit card data through Liberty Reserve. *See* Trial Exhibit 9.11; Tr. 725-726. This amount surely understates Seleznev's total earnings from this scheme as it only captures one of several payment mechanisms he used over the course of the scheme. Nonetheless, it provides the most direct evidence of the proceeds defendant obtained as a result of his hacking scheme. Therefore, the government is seeking a money judgment in the amount of $17,886,971.09.

Forfeiture in this matter is governed by Title 18, United States Code, Section 2323. That section provides that "[t]he court, in imposing sentence on a person convicted of an offense under section . . . 2320 . . . of this title, shall order, in addition to any other sentence imposed, that the person forfeit to the United States Government any property subject to forfeiture under subsection (a) for that offense." 18 U.S.C. § 2323(b)(1). Subsection (a) provides that the property subject to forfeiture includes:

> (A) Any article, the making or trafficking of which is, prohibited under section 506 of title 17, or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90 of this title.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(B) Any property used, or intended to be used, in any manner or part to commit or facilitate the commission of an offense referred to in subparagraph (A).

(C) Any property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of an offense referred to in subparagraph (A).

Section 2323 further provides that criminal forfeitures under this section shall be governed by Title 21, United States Code, Section 853. *See* 18 U.S.C. § 2323(b)(2).

As to the money judgment, the government recommends the Court make a finding as to the amount of proceeds that Seleznev obtained as a result of these crimes based on the evidence presented at trial pursuant to Federal Rule of Criminal Procedure 32.2(b)(1)(A). As noted above, the government believes the strongest evidence to establish the amount of proceeds Seleznev obtained through this scheme are the Liberty Reserve records from the accounts Seleznev used for his automated vending sites Track2 and Bulba. These records as outlined above, establish that defendant obtained $17,886,971.09 through Liberty Reserve alone. Therefore, this figure represents a very conservative money judgment in light of the fact that defendant also used Web Money, Western Union and other payment channels to receive payments from his customers.

VII. CONCLUSION

For the reasons set forth above, the government believes a sentence of 30 years is sufficient, but not greater than necessary, to address the important goals of sentencing set forth in Title 18, United States Code, Section 3553(a). Notably, this sentence represents a substantial downward variance from the Guideline recommendation of life in prison. As U.S. probation has noted, even if sentenced to 30 years as recommended, Seleznev will be in his 50s when he is released from prison and there is every indication that he will be capable of picking up where he left off upon release. Although the government agrees with Probation that the Guideline recommendation of life is greater than necessary

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

to achieve the goals of sentencing, a 30 year sentence is necessary to address the extraordinary facts of this case.

Dated: April 14, 2017.

ANNETTE L. HAYES
United States Attorney

s/ Norman Barbosa
NORMAN BARBOSA
Assistant United States Attorney
Western District of Washington

s/ Seth Wilkinson
SETH WILKINSON
Assistant United States Attorney
Western District of Washington

s/ Harold Chun
HAROLD CHUN
Trial Attorney
United States Department of Justice
Computer Crimes and Intellectual Property Section

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF SERVICE

I hereby certify that on April 14, 2017, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the attorney(s) of record for the defendant(s).

s/ Kylie Noble
KYLIE NOBLE
Legal Assistant
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101-3903
Telephone: (206) 553-2520
Fax: (206) 553-4440
E-mail: kylie.noble@usdoj.gov