

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

**SUPPLEMENTAL SENTENCING  
MEMORANDUM**

**I. Defendant's Cooperation**

Defendant Roman Seleznev suggests in his sentencing memo that he has “fully accepted responsibility for his crimes” and that he “wants to actively rectify the consequences of his criminal actions” by cooperating with U.S. law enforcement. In light of defendant’s newfound willingness to discuss his efforts to cooperate in public, the government submits this supplemental briefing to provide the Court with an accurate record of defendant’s efforts in this regard.

As the Court is already aware, Seleznev first met with the government in December 2014, purportedly to provide assistance to the government. At that time, shortly after defendant’s arrest, the information he possessed may have been helpful in furthering other government investigations. In advance of the meeting, the government

1 repeatedly told defense counsel that the value of any information defendant might have  
2 was extremely time-sensitive given the dynamic nature of the carding industry. The  
3 government made clear that the value of cooperation would be diminished or non-existent  
4 if Seleznev waited until after the trial, which was then set for May 4, 2015.

5 Defendant, nonetheless, chose not to cooperate. While he met with the  
6 government in December 2014, defendant was combative and repeatedly refused to  
7 identify others he had conspired with or those he knew were involved in criminal  
8 behavior. When asked why he would not name others or provide information regarding  
9 others involved in cybercrime, defendant explained that he was withholding that  
10 information as bargaining chips. When told that the government would require a  
11 complete statement from defendant before negotiating the terms of a cooperation  
12 agreement, defendant terminated the proffer session stating that he thought the proffer  
13 was supposed to be a “negotiation.” Defendant provided no information of value to  
14 apprehending other targets.

15 During the 20 months between the first “proffer” session and the eventual trial, the  
16 government and defense counsel had many discussions about the possibility of  
17 cooperation. The government repeatedly advised the defense that time was of the  
18 essence, and that defendant had already seriously compromised the value of his  
19 information by refusing to cooperate in the months following his apprehension.  
20 Defendant provided no additional information to the government over this 20-month  
21 period.

22 Following his conviction at trial (over two years after his apprehension), defendant  
23 again requested an opportunity to meet with the government and provide information.  
24 Although defendant’s potential usefulness has declined substantially as a result of the  
25 passage of time, the government agreed to meet with defendant and participated in  
26 proffer sessions on March 28-29, 2017. Unfortunately, he did not have any particularly  
27 useful information. Defendant acknowledged his guilt and that of his co-conspirators on  
28

1 the carding forums. He also identified some of those he conspired with between  
2 approximately 2005 and his capture in 2014. Much of the information that he provided,  
3 however, was already well known to the Secret Service. Defendant simply did not have  
4 any immediately actionable information that could assist law enforcement. As such, the  
5 information he provided was mainly useful as background intelligence. Furthermore,  
6 Seleznev made statements that the government believes to be demonstrably false, thereby  
7 further undermining the value of any information he provided.

8 Defendant's belated effort to cooperate is insufficient to justify any reduction in  
9 his sentence. For law enforcement to make effective use of assistance in cybercrime  
10 investigations, they need timely and complete information from a cooperating defendant.  
11 The time to cooperate is in the immediate days and weeks after they are arrested. As time  
12 passes, the value of any information a cybercriminal may possess quickly dissipates as  
13 co-conspirators learn about the potential cooperator's arrest, change their online  
14 identities, and move to new infrastructure. Defendant was fully aware of the fact that  
15 time was of the essence if he were to be useful to government. If he had provided useful  
16 information when he first met with the government in 2014, this case may have turned  
17 out very differently. Defendant, however, made a choice to throw that opportunity away  
18 and proceed to trial. In light of his explicit refusal to provide useful information when it  
19 was most valuable, he should not be rewarded for his belated efforts to cooperate.

20 As the government has advised counsel, post-judgment remedies are available in  
21 the unlikely event that any information defendant provided turns out to be helpful.  
22 Should any of the information or evidence defendant provided prove to be of assistance  
23 to U.S. law enforcement in the future, the government will consider the credibility,  
24 effectiveness and usefulness of his information in good faith. To the extent a reduction in  
25 sentence is appropriate pursuant to Federal Rule of Criminal Procedure 35, the  
26 government will file a motion seeking that relief.

27 ///

## II. Loss Amount

As the government noted in its sentencing memorandum, the loss amount for purposes of the guidelines is based on a minimum of \$500 per access device that defendant possessed in relation to the crimes of conviction. *See* Government's Sentencing Memorandum at 16-17. The testimony at trial established that defendant possessed approximately 2.9 million credit cards that he stole while the cards were in the process of being used. Therefore, the testimony and evidence at trial established that the cards he possessed were in fact useable at the time defendant possessed the cards. *Id.* In addition, Detective David Dunn conducted additional analysis of a sampling of the credit card data found in defendant's possession and completed the attached report detailing his conclusion that "while there is a reasonable likelihood that Roman Seleznev did possess a miniscule number of stolen cards that were expired, that percentage of cards would have been a tiny fraction of the overall cards that he possessed." *See* Attachment A. Given that only 1.1 million of the 2.9 million cards Seleznev possessed would need to be usable to meet the \$550 million loss threshold, the Court may easily find by a preponderance of the evidence that this threshold is satisfied.

Dated: April 17, 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 Attorneys  
Western District of Washington

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

UNITED STATES v. SELEZNEV, CR11-070RAJ  
SENTENCING MEMORANDUM- 4

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

**CERTIFICATE OF SERVICE**

I hereby certify that on April 17, 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](mailto:kylie.noble@usdoj.gov)