

1 DAVID L. ANDERSON (CABN 149604)
United States Attorney

2 HALLIE HOFFMAN (CABN 210020)
3 Chief, Criminal Division

4 MICHELLE J. KANE (CABN 210579)
KATHERINE L. WAWRZYNIAK (CABN 252751)
5 Assistant United States Attorney

6 1301 Clay Street, Suite 340S
Oakland, California 94612
7 Telephone: (510) 637-3680
FAX: (510) 637-3724
8 michelle.kane3@usdoj.gov
katherine.wawrzyniak@usdoj.gov

9 Attorneys for United States of America

10
11 UNITED STATES DISTRICT COURT
12 NORTHERN DISTRICT OF CALIFORNIA
13 SAN FRANCISCO DIVISION

14 UNITED STATES OF AMERICA,) No. CR 16-00440 WHA
15)
Plaintiff,) **UNITED STATES' SENTENCING**
16) **MEMORANDUM**
v.)
17) Hearing Date: September 29, 2020
YEVGENIY ALEXANDROVICH NIKULIN,) Time: 2:00 p.m.
18) Courtroom 12, 19th Floor
Defendant.)
19)
20)

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

INTRODUCTION.....1

BACKGROUND2

 A. Offense Conduct2

 B. Procedural History3

SENTENCING GUIDELINES.....4

 A. Guidelines Calculation.....4

 B. Defendant’s Objection to the Guidelines Calculation5

UNITED STATES SENTENCING RECOMMENDATION10

 A. Nature and Circumstances of the Offense10

 B. Defendant’s History and Characteristics11

 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.....12

 D. The Need for the Sentence Imposed to Afford Adequate Deterrence and
 Protect the Public From Further Crimes of the Defendant.12

CONCLUSION13

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF AUTHORITIES

CASES

United States v. Borrasi, 639 F.3d 774 (7th Cir. 2011) 6

United States v. Rigas, 583 F.3d 108 (2d Cir. 2009) 6

United States v. Tadios, 822 F.3d 501 (9th Cir. 2016) 6

United States v. Uddin, 551 F.3d 176 (2d Cir. 2009) 6

STATUTES

18 U.S.C. § 371 4

18 U.S.C. § 1028A 4

18 U.S.C. § 1029(a)(2) 4

18 U.S.C. § 1030 4, 5

18 U.S.C. § 3553(a) 2, 10, 13

OTHER AUTHORITIES

U.S.S.G. § 2X1.1 4

U.S.S.G. § 2B1.1 4, 5

U.S.S.G. § 2B1.1, cmt. n. 3 5

U.S.S.G. § 2B1.6(a) 5

U.S.S.G. § 3D1.2(d) 4

INTRODUCTION

Defendant Yevgeniy Nikulin is to be sentenced for his convictions on nine counts arising from his sustained hacking campaign affecting computer users around the world. From behind a keyboard in Moscow, Russia, Nikulin gained access to the computers of at least four U.S. companies, including victims based in the Northern District of California. To do so, he used the identities of individual employees while installing malicious software on the victims' computers. Nikulin stole millions of user credentials, which he sold for profit and shared with fellow hackers. His conduct left those users vulnerable to other crimes, including fraud and identity theft. Nikulin himself used some of the information he stole to perpetrate further crimes.

As the victims testified at trial, computer intrusions like Nikulin's impose devastating costs on businesses and individuals. Someone like Nikulin can work in anonymity, half a world away, profiting off his attacks on U.S. companies while insulating himself from consequences. Identifying a cybercriminal like defendant and bringing him to justice – which is the rare success story – requires a massive effort by U.S. law enforcement. It is therefore 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.

Moreover, defendant himself poses a significant risk of committing further crimes. Defendant has expressed no remorse or regret for his actions. He will return to Russia when he is released from custody and will once again be outside the reach of U.S. law enforcement. The Court should impose a sentence that will prevent Nikulin from resuming his crimes for a long time.

For all these reasons, the United States respectfully recommends that the Court sentence defendant Nikulin to a term of 145 months of imprisonment, which, as specified in the PSR, includes terms of 61 months on each of Counts Two, Six, and Eight and 60 months on each of Counts One, Four, Five, and Seven, to run consecutively to each other, and 24 months on each of Counts Three and Nine, to run concurrently to each other and consecutively to all other counts. This sentence represents the low end of the applicable Guidelines range. The Court should also sentence defendant to a three year term of supervised release on Counts One, Two, and Four through Eight, and a one year term of supervised release on Counts Three and Nine, to run concurrently. Finally the Court should award restitution to the

1 victim companies as recommended in the PSR.

2 **BACKGROUND**

3 The Court is familiar with the facts of this matter, having presided over the recent trial.
4 Accordingly, the following discussion highlights the facts and issues most relevant to the sentencing
5 considerations of 18 U.S.C. § 3553(a).

6 **A. Offense Conduct**

7 The evidence introduced at trial proved that, beginning in early 2012, defendant targeted
8 LinkedIn Site Reliability Engineer Nick Berry. He put a malicious shell called “madnez” on Mr. Berry’s
9 personal computer, which allowed him to send commands to the computer remotely. Because Mr. Berry
10 used that computer to access LinkedIn’s corporate network via Virtual Private Network (“VPN”),
11 defendant was able to obtain Mr. Berry’s login credentials. He eventually was able to log on to a
12 LinkedIn production server using Mr. Berry’s credentials and exfiltrate data for millions of LinkedIn
13 users, including email addresses, “hashed” passwords, and other data.

14 LinkedIn discovered the intrusion when someone posted a portion of the hashed passwords on an
15 online hacking forum, seeking help cracking them. Both Bruno Connelly and Ganesh Krishnan testified
16 about LinkedIn’s response, including the steps taken to determine how the then-unknown attacker had
17 gained access to their network, and how to remediate the damage. Evidence from the computer of
18 accused hacker Oleksandr Ieremenko showed defendant sharing stolen LinkedIn data with Ieremenko
19 later the same year.

20 The evidence also showed that defendant obtained login credentials to Dropbox’s corporate
21 system for employee Tom Wiegand, because Mr. Wiegand had used the same password on LinkedIn
22 and Dropbox. Once he was able to access Dropbox’s system as Mr. Wiegand, he gave himself access to
23 Dropbox document repositories, including a set of Dropbox user credentials with email addresses and
24 hashed passwords. The FBI alerted Dropbox to the possible threat based on evidence from its LinkedIn
25 investigation. Cory Louie of Dropbox testified about the significant response mounted by Dropbox to
26 investigate and remediate the attack.

27 Evidence introduced at trial further showed that defendant attacked Formspring’s corporate
28 network using credentials for employee John Sanders that he found through a compromise of Mr.

1 Sanders' Dropbox account. Using Mr. Sanders' Formspring credentials, defendant again installed the
2 malicious software on Formspring's system and exfiltrated a set of user credentials. Formspring
3 discovered the breach when credentials were posted to the same Internet forum. Founder Ade Olonoh
4 testified to the effect the attack had on his company and the work its employees undertook to repair the
5 damage. Evidence from email accounts and Western Union showed that defendant worked with co-
6 conspirators to sell the stolen Formspring user credentials later in 2012.

7 The government also introduced evidence that, in 2013, defendant attacked Automattic's
8 computer systems, compromising the identities of several employees. Evidence from defendant's
9 Google account showed him systematically searching for information about those employees online,
10 targeting them as he had targeted the victims at LinkedIn, Dropbox, and Formspring.

11 Defendant's method of operation throughout the four attacks was consistent – targeting
12 engineering employees with high-level access through Internet research, compromising employee
13 credentials, installing malicious software to maintain access, researching corporate infrastructure
14 through access to internal documentation, and exfiltration of valuable user credentials. All through this
15 campaign of intrusions, database thefts, and trafficking the results, defendant used various online
16 identities in an effort to hide his involvement. The FBI's painstaking investigation unmasked the
17 defendant by systematically connecting each fake account through victim logs, subscriber records,
18 account contents, and other documentary evidence.

19 **B. Procedural History**

20 Defendant was indicted on October 20, 2016, following his arrest in the Czech Republic at the
21 request of the United States, supported by a provisional arrest warrant. Defendant is a citizen and
22 resident of Russia, but according to news reports, was in the Czech Republic on a vacation. He was held
23 in custody while the United States' request for his extradition was litigated. He was eventually ordered
24 extradited and made his initial appearance in the Northern District of California on March 30, 2018.

25 Trial commenced March 9, 2020, with jury selection. Two days of opening statements and
26 testimony followed. After a break in proceedings due to the public health emergency, trial resumed on
27 July 6, 2020. The government rested its case on July 9, 2020, and defendant declined to present
28 evidence. Closing arguments were held on July 10, 2020.

1 After approximately six hours of deliberations, the jury returned guilty verdicts on all nine
 2 charged counts: three counts of computer intrusion, in violation of 18 U.S.C. § 1030(a)(2)(C) (as to
 3 LinkedIn, Dropbox, and Formspring), two counts of causing damage to a protected computer, in
 4 violation of 18 U.S.C. § 1030(a)(5)(A) (as to LinkedIn and Formspring), two counts of aggravated
 5 identity theft, in violation of 18 U.S.C. § 1028A (as to employees of LinkedIn and Formspring), one
 6 count of conspiracy, in violation of 18 U.S.C. § 371 (as to trafficking of Formspring's credentials), and
 7 one count of trafficking in stolen access devices, in violation of 18 U.S.C. § 1029(a)(2) (as to
 8 Formspring's credentials). The jury also agreed that the government had proven at least one aggravating
 9 factor increasing the maximum penalties for the violations of 18 U.S.C. § 1030(a)(2) from one year of
 10 imprisonment to five years for Counts One, Four, and Seven, and increasing the maximum penalties for
 11 causing damage to a protected computer from one year of imprisonment to ten years for Counts Two
 12 and Eight.

13 SENTENCING GUIDELINES

14 A. Guidelines Calculation

15 The United States agrees with the Sentencing Guidelines calculation in the PSR:

16 Counts One, Two, Four through Eight:

17	a. Base offense level: U.S.S.G. § 2B1.1(a)(2), 2X1.1	6
18	b. Specific offense characteristics:	
19	U.S.S.G. § 2B1.1(b)(1)(I) – Amount of Loss: more than \$1,500,000	+16
20	U.S.S.G. § 2B1.1(b)(10) – Sophisticated Means	+2
21	U.S.S.G. § 2B1.1(b)(11)(B)(i) – Trafficking of unauthorized access devices	+2
22	U.S.S.G. § 2B1.1(b)(18) – conviction under 18 U.S.C. § 1030(a)(2)(C) and intent to obtain personal information	+2
23	U.S.S.G. § 2B1.1(b)(19)(A)(ii) – Conviction under 18 U.S.C. § 1030(a)(5)(A)	+4
24	c. Adjusted offense level	32
25	d. U.S.S.G. § 3D1.2(d) – Adjusted offense level after grouping	32
26	e. Total offense level	32
27		
28		

1 **Counts Three and Nine:**

- 2 a. U.S.S.G. § 2B1.6(a) – Aggravated Identity Theft 24 months
3 consecutive to any
4 other sentence

5 With a criminal history category of I, the result is a Guidelines range of 121 to 151 months of
6 imprisonment on Counts One, Two, Four through Eight and 24 months consecutive on Counts Three
7 and Nine.

8 **B. Defendant’s Objection to the Guidelines Calculation**

9 Defendant objected to the loss figures in the draft PSR. Defendant has not provided an
10 alternative loss calculation. Based on the available evidence, the Court should accept the estimate of loss
11 in the PSR. First, the Court need only make a reasonable estimate of the loss, as noted in the
12 commentary to Guidelines. Moreover, as incorporated in the revised final PSR, the victims have
13 provided more thorough explanations of their losses through Victim Impact Statements. In addition, the
14 witnesses who testified at trial on behalf of the victims provided sufficient basis for the Court to find that
15 the reported loss amounts are reasonable estimates.

16 **1. Reasonable Estimate of Loss for Offenses Under 18 U.S.C. § 1030**

17 The parties and the PSR are in agreement that U.S.S.G. § 2B1.1 governs sentencing in this case.
18 Under section 2B1.1, the base offense level increases based on the amount of loss. U.S.S.G. § 2B1.1(b).
19 The Commentary to section 2B1.1 defines loss as the “greater of actual loss or intended loss.” U.S.S.G.
20 § 2B1.1, cmt. n. 3(A). In this case, the PSR uses “actual loss,” which typically means the “reasonably
21 foreseeable pecuniary harm that resulted from the offense.” *Id.* at cmt. n. 3(A)(I). For cases involving a
22 violation of 18 U.S.C. § 1030, however, the Commentary contains a special provision regarding loss,
23 which states:

24 Offenses Under 18 U.S.C. § 1030.—In the case of an offense under 18
25 U.S.C. § 1030, actual loss includes the following pecuniary harm,
26 regardless of whether such pecuniary harm was reasonably foreseeable:
27 any cost to any victim, including the cost of responding to an offense,
28 conducting a damage assessment, and restoring the data, program, system,
or information to its condition prior to the offense, and any revenue lost,
cost incurred, or other damages incurred because of interruption of
service.

U.S.S.G. § 2B1.1, cmt. n. 3(A)(v)(III). Thus, the Court may consider the types of pecuniary harm

1 described by the victims in their statements and testimony, foreseeable or not, in calculating the loss
2 amount under section 2B1.1 in this case.

3 That calculation need only be a “reasonable estimate of loss, given the available information.”
4 *United States v. Tadios*, 822 F.3d 501, 503 (9th Cir. 2016) (citation omitted) (upholding loss amount
5 based on estimate of employee’s wrongly-claimed salary); *see also* U.S.S.G. § 2B1.1, n. 3(C) (“The
6 Court need only make a reasonable estimate of the loss. The sentencing judge is in a unique position to
7 assess the evidence and estimate the loss.”); *United States v. Borrasi*, 639 F.3d 774, 784 (7th Cir. 2011)
8 (acknowledging that government has burden to prove loss but that defendant must come forward with
9 substantiated evidence, not “vague valuations” to refute the government’s proof; *United States v. Rigas*,
10 583 F.3d 108, 120 (2d Cir. 2009) (upholding district court’s estimate even though it could not determine
11 the “precise amount” of the loss attributable to defendants’ fraud,); *United States v. Uddin*, 551 F.3d
12 176, 180 (2d Cir. 2009) (finding loss calculation reasonable in food stamp fraud case where district court
13 used multiple estimates including average dollar amount of food stamp redemptions at similar stores,
14 witnesses’ observations of defendant’s store, and estimate of percentage of transactions that were
15 actually fraudulent).

16 **2. Evidence Regarding Losses Suffered by the Victims**

17 Sunnyvale-based LinkedIn Corporation has submitted a Victim Impact Statement establishing
18 that it spent at least \$2 million responding to defendant’s attack and exfiltration of data. The total cost
19 reflects its internal incident response and consultation with external vendors. According to the statement:

20 LinkedIn addressed the breach by (1) notifying the owner of any
21 potentially compromised account, (2) investigating the breach itself, and
22 (3) remediating the company’s systems and procedures to prevent further
23 unauthorized access by the hacker. This effort required a company-wide
24 response, including employees from Operations, Engineering, Product,
25 Marketing, Legal, Human Resources, Security, and Customer Support.
26 Due to the 24/7 nature of the response effort and the magnitude of Mr.
27 Nikulin’s breach, many employees had to work significantly increased
28 hours for the two-month period. Furthermore, LinkedIn hired external
security and IT vendors to investigate the breach, conduct security
assessments, and reveal any potential vulnerabilities in LinkedIn’s system.

26 This statement is supported by the sworn trial testimony of both Bruno Connelly and Ganesh
27 Krishnan. Importantly, LinkedIn notes that its estimate is extremely conservative, and based solely upon
28 the expenditures they could document. After eight years, this resulted in a claimed loss amount that was

1 less than the actual amount spent responding to the offense.

2 Mr. Connelly testified that when LinkedIn discovered the breach, it established a “war room” in
3 which 40 to 50 people worked to help with the response. Trial Transcript (“Trial Tr.”) at 31:12-16. He
4 testified that the people working on the response had roles “across all parts of engineering” as well as
5 the security team. Trial Tr. at 31:19-22. Mr. Connelly explained that the incident was the highest level of
6 critical – “code red” – which meant that it was an “existential risk” for the company. Trial Tr. at 32: 20-
7 23. He testified at length about the multi-step process that the company went through to track the
8 attacker through the LinkedIn system, including by review of VPN logs to identify anomalous activity.
9 E.g., Trial Tr. at 43:24-44:9. Mr. Connelly explained that the identification of particular IP addresses led
10 to multiple investigations by the Code Red team to look at the usage on the LinkedIn public platform.
11 Trial Tr. at 44:21-25. Mr. Connelly explained how the internal team used the IP addresses to identify
12 suspicious browser cookies and unusual user agent strings, which all together formed a “fingerprint” of
13 the attacker. E.g., Trial Tr. at 50:3-51:6. He testified that LinkedIn identified over 30 LinkedIn customer
14 accounts that had unauthorized access by the attacker using this “fingerprint.” Trial Tr. at 51: 23-52:10.
15 In addition to the customer accounts, the Code Red team followed the attacker’s path through the
16 LinkedIn corporate network, including access to the Oracle database machines where user credentials
17 were stored. Trial Tr. at 57: 12-24.

18 Mr. Connelly testified that LinkedIn spent approximately six weeks remediating the attack,
19 including dealing with compromised member accounts. Trial Tr. at 73:16-75:24. He testified that
20 LinkedIn spent “significantly” more than \$5,000 (the jurisdictional threshold) responding to defendant’s
21 attack, that approximately 100 employees were ultimately involved, that those employees were diverted
22 from doing other business activities, and that it was the most serious data breach that he has worked on.
23 Trial Tr. at 75:25-76:24.

24 Ganesh Krishnan of LinkedIn also testified to the company’s incident response. He described the
25 steps, which included verifying that the password hashes actually belonged to LinkedIn, figuring out the
26 extent of the breach, determining whether the breach was still occurring, and identifying remedial steps.
27 Trial Tr. at 289:1-9. Mr. Krishnan noted that it was “all hands on deck” with employees across the
28 company working on the “Code Red.” Trial Tr. at 288:2-11. He also confirmed that LinkedIn hired an

1 outside consultant to assist with the incident response. Trial Tr. at 296:19-22. He explained that
2 LinkedIn viewed the stolen data as valuable and said that it was the most important issue at LinkedIn at
3 the time. Trial Tr. at 288:2-25. Like Mr. Connelly, Mr. Krishnan testified that this was the most
4 significant data breach that he worked on. Trial Tr. at 297:6-8. He confirmed Mr. Connelly's account
5 that the investigation lasted a few months and the remedial steps lasted "longer after that." Trial Tr. at
6 296:15-18.

7 San Francisco-based Dropbox, Inc., has submitted a Victim Impact Statement describing how the
8 company:

9 ...expended significant internal resources to investigate the scope of Mr.
10 Nikulin's intrusion into its systems and the damage caused. The team of
11 employees who dedicated their time and energy to this investigation and
12 mitigation effort did so at the expense of otherwise working on improving
13 and developing Dropbox's products. Dropbox also incurred infrastructure
14 costs to remediate systems affected by Mr. Nikulin's criminal conduct.
15 Additionally, Dropbox hired external forensic vendors and attorneys to
16 assist in the investigation.

17 Dropbox has conservatively estimated that its costs in responding to defendant's attack was at least
18 \$514,000. The testimony of Cory Louie, former head of Trust and Security for Dropbox supports this
19 estimate. Mr. Louie testified that, when he began working at Dropbox, the company had begun
20 responding to its discovery of the breach. Trial Tr. at 79:19-22. He explained that Dropbox also had a
21 "war room." to investigate the attack. Trial Tr. at 85:10-17. Mr. Louie testified that it was "all hands on
22 deck," with employees working to determine what had happened while securing the company
23 infrastructure from further attacks. *Id.* He estimate that 20 to 25 employees actively worked on the
24 response, and that those people were leaving aside their other jobs to do so. Trial Tr. at 86:4-14. Mr.
25 Louie was brought in to lead and coordinate the response, investigation, and recovery. Trial Tr. at 86:15-
26 18. Dropbox determined that multiple corporate accounts had been compromised using IP addresses
27 originating in Russia. Trial Tr. at 86:18-87:12. Mr. Louie testified about how Dropbox identified the
28 corporate accounts using the suspicious IP addresses and a unique identifier called GVC that could trace
activity by one computer across multiple Dropbox logins. Trial Tr. at 89:5-90-17. He testified about the
process Dropbox employees used to follow the attack through its systems via activity logs for the
compromised accounts and how those activity logs showed access to the account belonging to Tom

1 Wiegand, which contained a file with a subset of usernames and hashed passwords. Trial Tr. at 94:10-
2 25.

3 San Francisco-based Formspring, which is now defunct, has submitted a Victim Impact
4 Statement outlining \$20,000 in losses as the result of defendant's conduct. The statement describes
5 approximately \$15,000 in engineering resources and approximately \$5,000 in messaging and new
6 infrastructure. The statement also notes that "[t]his incident had an impact on our brand, and the trust
7 our users had in us to protect their data. We had thousands of users delete their Formspring accounts
8 shortly after the incident." The losses are supported by the testimony of founder Ade Olonoh.

9 Mr. Olonoh testified that Formspring first learned of the breach upon being contacted in July
10 2012 by someone who had seen the posting of approximately 420,000 Formspring credentials to an
11 Internet forum. Trial Tr. at 106:5-18. At the time, Formspring had about 30 million registered users and
12 approximately 20 employees. Trial Tr. at 89:22-90:13. Mr. Olonoh testified about the process that
13 Formspring went through to investigate the potential breach. He explained how he verified that the
14 posted credentials actually belonged to Formspring users. Trial Tr. at 108:13-109:21. Mr. Olonoh then
15 described how Formspring combed through a "large volume of system logs" to understand what
16 "vector" had been used in the attack. Trial Tr. at 109:22-111:12. He testified about the "chaotic"
17 environment in the Formspring office as "everybody from the engineering team" was investigating the
18 attack and a support team was "busy responding to user questions and concern about the hack." Trial Tr.
19 at 127:20-128:3. He testified that after they had figured out what happened the next step was to secure
20 the compromised server, send messages out to all Formspring users, write new code, and rebuild the
21 development server. Trial Tr. at 128:4-21. Mr. Olonoh estimate several hundred to over a thousand
22 employee hours were spent on the response, and certainly over the \$5,000 jurisdictional threshold. Trial
23 Tr. at 128:22-129:10. Formspring was much smaller at the time than LinkedIn or Dropbox, so even an
24 "all hands on deck" (Trial Tr. at 128:3) situation resulted in significantly smaller losses than those of the
25 other victims, although the attack had a major impact on the company. Mr. Olonoh testified to the fact
26 that many users deleted accounts following the publicity of the breach. Trial Tr. at 131:1-10. Formspring
27 employee John Sanders whose credentials defendant used to infiltrate the corporate system, testified to
28 the "panic" and "anxiety" he felt as a young employee, new to the industry, whose account had been

1 compromised and put the company at risk. Trial Tr. at 72: 8-19.

2 Automattic has estimated its loss amount as \$250,000. Automattic is the parent company of
3 Wordpress.com and other online services. FBI Special Agent Jeffrey Miller testified at trial regarding
4 the scope of the intrusion into Automattic's system, which included multiple compromised employee
5 accounts. Trial Tr. at 525:7-532:5; 557:18-558:23. He described the extensive logs gathered by the
6 company, a summary of which was admitted at Exhibit 17A. Given the estimates by the other victims,
7 Automattic's estimate is within the expected range of reasonable expenditures. Automattic has
8 represented that the company is attempting to gather information regarding its losses. The United States
9 will provide that information if it is received before sentencing.

10 Altogether, the evidence provided by the victims for sentencing and the evidence introduced at
11 trial supports the loss figure in the PSR as a reasonable estimate, and likely understatement, of the costs
12 to the victims.

13 **UNITED STATES' SENTENCING RECOMMENDATION**

14 The United States' recommended sentence of 145 months of imprisonment is substantively
15 reasonable and sufficient, but not greater than necessary, to address the factors set forth in 18 U.S.C.
16 § 3553(a).

17 **A. Nature and Circumstances of the Offense**

18 Defendant's attacks created existential crises for the victim companies. As discussed above, each
19 company expended massive resources responding to his intrusions, pulling employees and resources
20 from their ordinary functions. Moreover, we know that defendant himself used the stolen LinkedIn data
21 to compromise at least 30 customer accounts identified by LinkedIn in its own investigation. He may
22 have targeted those individuals based on their professional positions with the goal of hacking their
23 companies and selling that data.

24 Far more than that, however, his conduct left millions of users vulnerable to further crimes by the
25 people with whom defendant shared their personal information. Special Agent Miller testified about the
26 uses for stolen data, including accessing bank accounts, hacking email accounts, and spam advertising.
27 Trial Tr. at 625: 19-24. He testified that even when companies protect passwords through hashing, there
28 are individuals who specialize in cracking those passwords for profit. Trial Tr. at 625:25-626:6. Special

1 Agent Miller explained that user credentials are most valuable when first stolen, that the value
2 diminishes as the breach becomes public, and that data is sold multiple times at declining prices through
3 dark markets. Trial Tr. at 626:13-627:4. The LinkedIn data would have been the most valuable of all the
4 stolen databases, not just because it was the largest set, but also because, as a social network, it enabled
5 cybercriminals to target individuals based on their associates and employment. Trial Tr. at 627:5-19.
6 The evidence at trial proved that defendant sold the complete Formspring data set to an individual
7 known as Mehmet Sozen or “Rais” in 2012 and gave LinkedIn email addresses and passwords to
8 accused hacker Oleksandr Ieremenko. The evidence also showed that portions of the LinkedIn,
9 Dropbox, and Formspring databases were all posted publicly at some later point. Defendant thus
10 released users’ personal data into the wild, where any cybercriminal could use it to perpetrate new
11 crimes.

12 The Guidelines offense level does not account for the potential harm to these millions of
13 individuals around the world, and thus, if anything, understates the seriousness of the offenses. The
14 nature and circumstances of his massive data breaches merit a substantial custodial sentence.

15 **B. Defendant’s History and Characteristics**

16 Defendant has declined to speak with the Probation Officer who prepared the PSR, but the Court
17 can glean information about him from the proceedings in this case. In particular, the Court will recall
18 that defendant’s refusal to work with his retained counsel, and the resulting need for competency
19 proceedings and substitution of panel counsel, caused a significant delay in bringing this case to trial.
20 Defense counsel raised doubts regarding defendant’s competency for trial based on his lack of
21 communication with his counsel. Defendant then refused to meet with the psychiatrist retained by his
22 attorneys to assess his competency. Defendant was therefore committed to the custody of the Bureau of
23 Prisons (“BOP”) for a competency evaluation. Only when the BOP forensic psychologist, Dr. Lesli
24 Johnson, opined that the defendant was competent to stand trial, did defendant participate in an
25 evaluation by his own expert. The Court held an evidentiary hearing at which both experts testified
26 regarding their opinions. Dr. Johnson found that the defendant’s unwillingness to communicate with his
27 attorney was “directly related to his narcissistic traits” and was “volitional and goal-directed.” Johnson
28 Report at 20. She reported that he told her at one point “I’m always capable of participating in

1 conversations, but depending on the situation, the ambience and the people.” ECF No. 89 (Transcript of
2 Evidentiary Hearing) at 26:9-14; Johnson Report at 19. When the Court found defendant competent, his
3 retained attorney withdrew, and the Court appointed CJA panel counsel. ECF Nos. 94, 106. Almost a
4 year elapsed from defendant’s August 10, 2018, Motion for Psychiatric Exam and Mental Competency
5 Hearing, to the Court’s August 6, 2019, appointment of counsel. This delay was the product of
6 defendant’s disregard for the Court, the U.S. criminal justice system, and the people working on all sides
7 to ensure his fair trial.

8 In preparation for sentencing defendant has not expressed remorse or accepted any responsibility
9 for his actions. While declining an interview with the Probation Officer, he has written multiple letters to
10 the Court since his conviction. ECF Nos. 270, 272, 275. In those letters his only concern has been that
11 he be allowed a portable video game system, radio, and MP3 player while in custody. He has also used
12 his letters to confirm some of the evidence introduced against him at trial by the United States, such as
13 his brother’s and girlfriend’s email addresses, and his own birthday. ECF Nos. 270, 272. The Court
14 should consider this lack of regret on its own, and also consider how it affects the need to deter future
15 crimes by defendant when he returns to Russia.

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

18 Offenses like defendant’s undermine trust in the innovative technology that is the hallmark of the
19 Northern District of California. The Internet has opened up opportunity for billions of people around the
20 world, but also created new and unprecedented opportunities for criminals to steal information on a
21 previously unimaginable scale. Despite that scale, it is important to remember that these crimes affected
22 real people and real companies – for example, Mr. Olonoh testified to the difficulties the breach at
23 Formspring caused to his young company. A computer intrusion and data breach, whether at a large
24 public company or a new venture, can present a serious threat to the viability of the victim business.
25 This type of crime is not merely the moving around of anonymous bytes. The Court’s sentence should
26 reflect the seriousness of the threat posed by this type of cybercrime to technology companies and their
27 customers.

28 //

