

The Honorable Robert S. Lasnik

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

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

UNITED STATES OF AMERICA,

Plaintiff,

v.

PAIGE A. THOMPSON

Defendant.

NO. CR19-159 RSL

**GOVERNMENT’S SENTENCING
MEMORANDUM**

I. INTRODUCTION

Thompson hacked dozens of companies over nearly six months. After she was caught, she began revising history to argue that she was simply a good-faith security researcher trying to identify vulnerabilities on the Internet. The truth, exposed by the evidence and determined by a jury, was that Thompson illegally hacked companies to benefit herself, not anyone else.

Thompson had both financial and non-financial motives for hacking. The fact that her motives were not purely financial does not excuse her crimes, nor does it make it any less important to deter her and others. People illegally hack computer systems for all kinds of reasons that are not financial: nationalism, politics, ideology, revenge, contempt, curiosity, excitement, and for notoriety, just to name a few examples. No

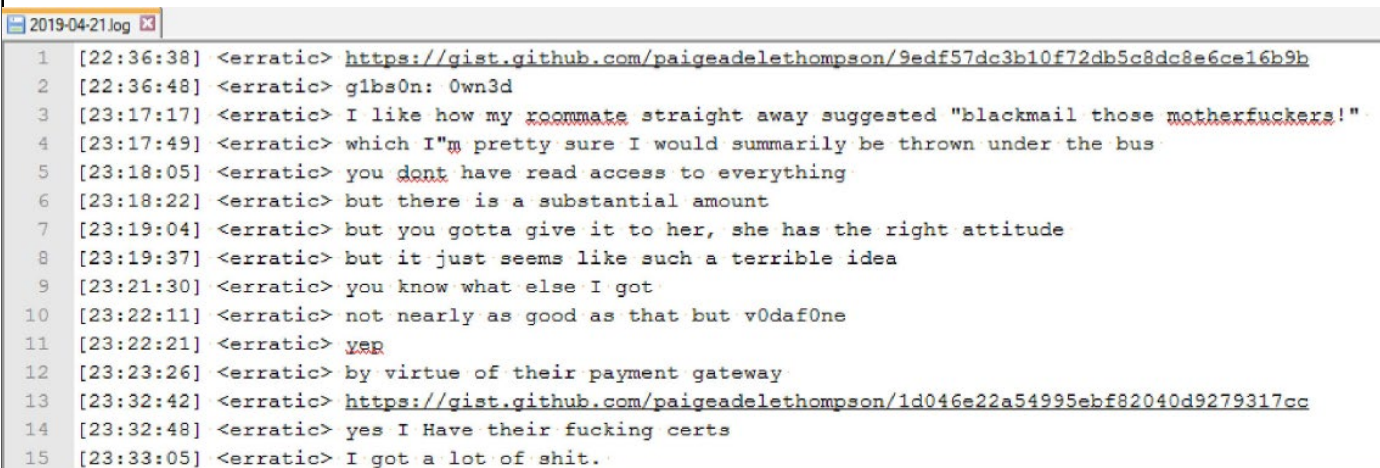
1 matter what the motivation, illegal hacking is harmful. It is true that Thompson exercised
2 restraint in not selling the data she stole, and the FBI, with Capital One's assistance, acted
3 quickly to arrest her before she lost that sense of restraint. But that does not mean that
4 Thompson did not commit a crime and cause massive harm. She did both. Throughout
5 this case, the defense has tried to reorient the perspective on this case, by focusing on
6 worse harms that Thompson could have caused. But a bank robber who decides not to
7 shoot the clerk has still committed a bank robbery. The fact that Thompson could have
8 benefited more from her crime, and that she could have harmed people more than she did,
9 does not mean that she did no harm. The actual harm she caused is the harm she must be
10 held accountable for.

11 Some of the harms that Thompson caused are measurable, like the hundreds of
12 millions of dollars Capital One spent on security remediation and customer response and
13 class-action lawsuits. Many of her harms are less measurable but no less significant.
14 One hundred million Capital One customers read about their personal identifying
15 information being stolen and wondered whether and how it had been used. Some became
16 very anxious and upset, even after they were assured that their data had never been used.
17 Employees of the hacked companies spent long hours trying to understand the
18 vulnerability, fix it, and assess the damage. Some companies lost customer data or
19 confidential business information. Others received large bills in the mail that they could
20 not afford to pay, for services they did not use. Several suffered reputational damage.

21 The Sentencing Commission recommends a sentencing range of 17.5 years to 22
22 years in prison for Thompson's crimes. That range is not based on her motives, rather, it
23 is based on the Commission's recognition that she committed a serious crime that caused
24 substantial harm. Much like a drunk driver has no idea whether he will hit a pedestrian
25 crossing the street, Thompson did not know what kind of data she would catch in her
26 broadly cast hacking nets. But the risk that illegally acquired information will include

1 people's personal identifying information and sensitive business data was not only
 2 entirely foreseeable—it was inevitable given the large number of companies she hacked.
 3 This is the precise set of risks and harms that the Computer Fraud and Abuse Act
 4 (CFAA) criminalizes and seeks to deter. The critical decision point is the point of
 5 unauthorized access, followed closely by the decisions to install malware and download
 6 the data. The CFAA is much more concerned with illegally accessing and acquiring
 7 information than it is about what a person does with the information afterward.

8 Although Thompson's methods of identifying vulnerabilities were largely
 9 automated, she downloaded the data by executing a separate command that she had to
 10 enter manually. These are the precise decision points that the law criminalizes and seeks
 11 to deter with meaningful consequences. The evidence on her computer showed that she
 12 downloaded data from the charged victims on multiple different dates. She downloaded
 13 Capital One's data on March 21-22, and by March 28 had created the
 14 "Capitol_One_Inclusion_List" [sic] with a list of Seattle residents' personal identifying
 15 information. The following week, she hacked another large company and then bragged
 16 about it:

17 

```

18 1 [22:36:38] <erratic> https://gist.github.com/paigeadelethompson/9edf57dc3b10f72db5c8dc8e6ce16b9b
19 2 [22:36:48] <erratic> glbs0n: Own3d
20 3 [23:17:17] <erratic> I like how my roommate straight away suggested "blackmail those motherfuckers!"
21 4 [23:17:49] <erratic> which I'm pretty sure I would summarily be thrown under the bus
22 5 [23:18:05] <erratic> you dont have read access to everything
23 6 [23:18:22] <erratic> but there is a substantial amount
24 7 [23:19:04] <erratic> but you gotta give it to her, she has the right attitude
25 8 [23:19:37] <erratic> but it just seems like such a terrible idea
26 9 [23:21:30] <erratic> you know what else I got
27 10 [23:22:11] <erratic> not nearly as good as that but v0daf0ne
28 11 [23:22:21] <erratic> yep
29 12 [23:23:26] <erratic> by virtue of their payment gateway
30 13 [23:32:42] <erratic> https://gist.github.com/paigeadelethompson/1d046e22a54995ebf82040d9279317cc
31 14 [23:32:48] <erratic> yes I Have their fucking certs
32 15 [23:33:05] <erratic> I got a lot of shit.
```

33 Trial Exhibit 453; *see also* Trial Exhibit 760.

1 Thompson has never been circumspect or remorseful about her hacking scheme,
2 despite recognizing, at the time, that she was committing serious crimes that would land
3 her in prison if she were caught. Even as she began to realize the full scope of the harm
4 she was causing, she still did not stop hacking computer systems, downloading data or
5 cryptojacking. She did not even delete the data she stole. Instead, she archived all the
6 data she had stolen by compressing it and moving it to a different volume of her
7 computer for long-term storage.

8 Considering the broad impact of her crimes and the critical role that the CFAA
9 plays in deterring cybercrime, is particularly troubling that Thompson still does not
10 accept that her conduct was criminal and still does not express remorse for the harm she
11 caused. She continues to blame the victims for her poor choices, continues to question
12 whether the jury's verdict was just, continues to mischaracterize her actions as "good-
13 faith security research" (despite volumes of evidence to the contrary), and continues to
14 trivialize her crimes. The Court's sentence can either endorse her false narrative or reject
15 it.

16 The government recommends that the Court impose a sentence of 7 years (84
17 months), less than half of the low end of the standard range. The Guidelines range would
18 be appropriate for a person with purely malicious motives who committed maximum
19 harm. A significant downward variance is appropriate to recognize that Thompson could
20 have caused even more harm than she did, that her decision-making was influenced by
21 her mental health circumstances, trauma, and lack of a robust support system, and that
22 there are widely recognized medical, mental, and physical risks she will face in prison as
23 a transgender woman. At the same time, a significant sentence is necessary to recognize
24 the seriousness of this offense and deter Thompson and others engaging in similar
25 conduct. Thompson has made it clear that she believes her crimes were no big deal and
26 that her victims are to blame. Only a sentence that includes a substantial term of

1 imprisonment will dispel that narrative, provide just punishment for these offenses, and
2 deter others.

3 II. BACKGROUND

4 A. Thompson spent months developing and refining a hacking scheme 5 that targeted millions of potential victims.

6 At trial, FBI forensic computer scientist Waymon Ho testified for five hours about
7 the steps Thompson took to hack Amazon Web Services (AWS) accounts and the digital
8 evidence on her computer, most of which was located in a file directory she named
9 “AWS_hacking_shit.” Thompson’s multi-step hacking scheme—which she
10 implemented, repeated, and refined for months—required a high degree of sophistication,
11 persistence, and intentionality.

12 First, Thompson anonymized her Internet identity using both a virtual private
13 network (VPN) and The Onion Router (TOR). Then, using programming scripts she
14 wrote, she scanned tens of millions of publicly available IP addresses hosted by AWS,
15 looking for vulnerabilities. When she found a vulnerability, she requested private
16 information from an internal server that she knew she was not supposed to access. If she
17 received the private information, she went further by requesting security credentials for
18 the vulnerable accounts.

19 Once Thompson acquired the victims’ security credentials, she used those
20 credentials to log in to the victims’ cloud computing accounts. After gaining access to a
21 victim’s account, Thompson used the security credentials to perform various actions in
22 the victim company’s cloud environment, such as viewing and copying data, and creating
23 instances (virtual servers), security groups, keypairs, and secured pathways to plant and
24 run cryptocurrency mining programs.

25 The bash history on Thompson’s computer revealed that she often required
26 multiple attempts to accomplish each of the steps described above. Over months,

1 Thompson corrected, improved, and streamlined her code to improve upon its
2 functionality and to automate additional actions against victim servers.

3 Thompson attacked some victims multiple times. She never notified them of their
4 cyber-security vulnerabilities; instead, she wrote notes and chats and texts about how
5 ignorant the companies were in failing to fix the issue. These were notes like “hit this
6 before,” “[a]nother unfixed previously used account,” and “guess whos back.” Trial
7 Exhibits 808, 810. When possible, Thompson used stolen credentials to create new
8 security groups and keypairs, so that she could have another pathway to access
9 companies’ resources even if they discovered and fixed the vulnerability that allowed her
10 to access their resources in the first place. She deleted log files that customers use to
11 review how their resources are being used.

12 And Thompson enjoyed committing these crimes. On June 5, 2019, after
13 successfully hacking another company, she wrote “heh heh heh heh heh gottem.” Trial
14 Exhibit 455. In an online chat on July 8, 2019, she bragged about how her cryptomining
15 malware “effectively leaves the customer unable to do any kind of forensic recovery.”
16 Trial Exhibits 416, 417. On July 15, approximately two weeks before her arrest, she
17 wrote that she was “1,000x more qualified than” the people she hacked and asked, “why
18 do I have to fuckin be the one who’s trying to go to jail for wire fraud, to prove their [sic]
19 qualified enough to have a job?” Trial Exhibit 460. In that same conversation, she said
20 “the sooner I get busted for it and make a name for myself the better” *Id.* The next
21 day, in a different conversation, she wrote:

22
23 [11:43:13] <erratic> yeah aws is great, except when someone steals your IAM
24 instance profile that has full access to the account :)

1 **B. Thompson committed one of the largest data breaches in U.S. history,**
2 **causing millions of dollars of damage.**

3 Thompson's computer showed that she scanned approximately 37 million IP
4 addresses looking for vulnerabilities. At trial, the government admitted a file from her
5 computer that contained security credentials for roughly 200 AWS accounts. Trial
6 Exhibit 609. She cryptojacked dozens of victims, making thousands of dollars in
7 cryptocurrency over a short period of time. Her computer contained a directory of
8 approximately 40 different keypairs created using stolen security credentials. Trial
9 Exhibit 607. She stole data not only from Capital One, but also from at least 30 other
10 entities. *See* Trial Exhibit 605. The stolen data included millions of people's names,
11 addresses, email addresses, and phone numbers, application source code, and security
12 certificates. Most notably, after breaching Capital One's system, Thompson exfiltrated
13 the personal identifying information of over 100 million people—roughly one-third of the
14 United States' adult population—constituting one of the largest data breaches in United
15 States' history.

16 Although Capital One was severely affected by the breach, it is a large corporation
17 that will survive its multi-million-dollar losses. Many of the other victims in this case
18 were not large companies. They did not have large cybersecurity payrolls to investigate
19 and repair the vulnerability or assess the damage, they did not have the operating budget
20 to afford large AWS bills, and they did not have the market strength to withstand bad
21 publicity.

22 In some cases, the companies at issue were involved in the cybersecurity industry
23 themselves, making the fact that they have been victims of a highly publicized hack
24 particularly harmful to their reputation. Some companies were unwilling even to
25 cooperate with the government's investigation. In other cases, companies cooperated
26 with the investigation (with more or less encouragement), but then chose not to submit

1 victim impact materials at sentencing, because they perceived the ongoing reputational
 2 harm of being associated with the breach to be so significant. A memorandum describing
 3 one such company's decision is attached as Exhibit 1.

4 In sum, although many of the victims of Thompson's conduct were businesses, the
 5 impact of Thompson's conduct on those businesses should not be underestimated or
 6 dismissed as mere financial loss. Thompson's conduct has had long-term ripple effects
 7 for all kinds of different companies.

8 **C. Thompson was one bad day away from sharing the data she stole.**

9 Shortly after downloading the Capital One data in March 2019, Thompson
 10 searched the data for personal identifying information of people who had addresses in
 11 Seattle. She created a list of Seattle residents' personal identifying information that she
 12 named the "Capitol_One_Inclusion_List" [sic]. Then, she took the personal identifying
 13 information of one of the people on that list, J.B., and put it into a file she named "id."
 14 J.B.'s personal identifying information also appears in an autofill field on Thompson's
 15 phone, indicating she had used it to fill out an online form.

16 For several months, Thompson thought about what she would do with the
 17 terabytes of data she had downloaded. She researched illegal credit card forums, where
 18 personal information is sold on the dark web to people who use it to commit access
 19 device fraud, and she explored renting servers in Russia, where the data would be
 20 inaccessible to United States law enforcement. She considered publishing the data. On
 21 May 6, 2019, she told a friend:

22 [05:40:05] <erratic> pisses me off
 23 [05:40:29] <erratic> Javantea: it pisses me off so bad, it makes me want to ... leak these TSA s3 buckets
 I got
 24 [05:40:53] <erratic> shit nigga, nah I aint trying to go out like that
 [05:41:06] <erratic> we gettin there tho

25 Trial Exhibit 454.
 26

1 On June 5, 2019, she told a friend that she was “thinking about carding alot [sic]
2 lately” and that she needed carding fraud items “to go shopping.” Trial Exhibit 455.

3 That same day, she remarked:

```
4 [10:04:25] <erratic> I'm pretty careless but I'm careless because nobody gives a fuck
5 [10:04:33] <erratic> but I could stand to be less careless
6 [10:05:09] <erratic> seriously like
7 [10:05:13] <erratic> the shit I've done
8 [10:05:27] <erratic> way worse than what adrian lamo got arrested for initially
9 [10:05:41] <erratic> and that guy made his whole fucking career off being a scene whore
10 [10:05:53] <erratic> RIP adrian
```

8 Trial Exhibit 455.¹

9 Then on July 14, 2019, only a few days before K.V.’s responsible disclosure to
10 Capital One and two weeks before her arrest, Thompson wrote to an associate:

```
11 2019-07-14.log x
12 663 [07:54:12] <erratic> lol
13 664 [07:56:30] <erratic> kongfuzi: you got a place I can upload 2.2TB of stuff
14 665 [07:56:52] <erratic> I cant really talk about what it is or how I got it
15 666 [07:56:58] <erratic> its just stuff
16 667 [07:57:05] <erratic> you know how it goes
```

16 Trial Exhibit 459.

17 The FBI acted quickly after learning of the breach. Within a week, it obtained a
18 search warrant and recovered the data from Thompson’s bedroom before she uploaded it
19 anywhere. If the FBI had not acted so quickly, there is no way of knowing what
20 Thompson ultimately would have done with the data she stole, or where it would be now.

21 //

22 //

25 ¹ Adrian Lamo was prosecuted and convicted of violating the CFAA for hacking the New York Times via a
26 misconfigured proxy server and causing approximately \$65,000 worth of damage. He was 22 years old at the time.
In 2010, he reported Chelsea Manning’s leak of classified records to the FBI. Lamo died of unknown causes in
2018, when he was 37 years old.

1 **D. After her arrest, Thompson continued to profit from her scheme and**
2 **flouted her conditions of release.**

3 Thompson will undoubtedly argue that her crimes were the product of untreated
4 mental health conditions and an unstable employment and living situation. There may be
5 some truth to these arguments, but it is not the full story of her criminal activity. As
6 Thompson's statements from the time of the crime illustrate, there were aspects of
7 Thompson's crimes that were fully intentional and grounded in spite, revenge, and willful
8 disregard for the law. She exhibited a smug sense of superiority and outright glee while
9 committing these crimes. The government's recommendation of a below-Guidelines
10 sentence recognizes the aspects of her crime that are attributable to mitigating
11 circumstances, while also holding Thompson accountable for the aspects of her crimes
12 that were fully volitional.

13 Thompson's unrepentant contempt of the law is evident in her post-arrest conduct.
14 Not only does she continue to assert a good-faith security motive that is completely at
15 odds with the evidence, but she continues to engage in misconduct. Most notably, the
16 government uncovered evidence that she withdrew financial proceeds of cryptojacking
17 while on pretrial release, and that she violated conditions of pretrial release that restrict
18 her access to computers and the Internet.

19 **1. Thompson continued to profit from her crimes while on pretrial**
20 **release.**

21 The FBI identified two private keys for Ethereum cryptocurrency wallets on
22 Thompson's computer. The Court may recall from trial testimony that the private key
23 corresponds to a public key associated with a cryptocurrency wallet. Possession of the
24 private key is necessary to identify a person's ownership rights over the wallet. If a
25 person loses a private key, or a private key is stolen, that person loses their ownership
26 over the wallet.

1 At trial, FBI Forensic Computer Scientist Vincent Kenney testified about a
2 particular wallet that was identified in Thompson’s mining scripts (ending in “ea74f”). In
3 other words, trial testimony, and ultimately the jury’s verdict on Count 8, connected this
4 wallet to Thompson’s cryptojacking activity on victim servers. FBI CS Waymon Ho
5 identified another wallet on Thompson’s device (ending in “491b3”), but did not connect
6 that wallet to any mining scripts.

7 While preparing for sentencing, the FBI reviewed publicly available transaction
8 data for Thompson’s cryptocurrency wallets. *See* Exhibit 2. The wallet ending in
9 “ea74f” had three outgoing (“cash out”) transactions in 2021, long after Thompson’s
10 arrest, with a total value of approximately \$4,900.00. The second wallet had outgoing
11 transactions between November 19, 2020, and May 23, 2021, again, long after
12 Thompson’s arrest and release on bond, with a total value of approximately \$39,860.00.

13 The timing of these wallet transactions is consistent with the evidence in the case.
14 Thompson was arrested on July 29, 2019. Her mining script was designed to run in
15 active memory until the rogue instances were identified and shut down. For the wallet
16 ending in “ea74f,” cryptomining rewards continued to flow into the wallet until August 5,
17 2019, roughly a week after Thompson’s arrest. In the wake of the FBI’s investigation,
18 Thompson’s arrest, and the publicity surrounding it, AWS and its customers likely
19 identified rogue instances associated with “ea74f” and shut them all down.

20 As for the wallet ending in “491b3,” income began flowing into this wallet on July
21 16, 2019. That is about a week after July 9, 2019, the day that Thompson commented in
22 an online chat that several of her rogue cryptojacking instances were shut off at once, and
23 she believed that the customer(s) had identified her activity through the IP addresses
24 associated with her wallet. *See* Trial Exhibits 416, 417. She had a plan to obscure her
25 conduct further, remarking that “[e]ach deployment will use a separate wallet and I
26 suspect it will take them significantly longer to locate and stop all of the instances if the

1 instances don't hit their billing limit before they are found first." *Id.* Consistent with
2 Thompson's statements, "491b3" was one of the wallets that was harder to find, leading
3 to mining activity and receiving deposits that began in mid-July, shortly before her arrest,
4 that continued automatically while Thompson was in custody, and ended in December
5 2019 when the last miners and instances presumably were discovered and shut off.

6 The fact that Thompson continued to withdraw money from her cryptocurrency
7 wallets while on pretrial release, rather than allocate it toward restitution, is further
8 evidence that she is not remorseful.

9
10 **2. Thompson used computers and the internet in ways that were not**
11 **authorized by Pretrial Services, and then lied to Pretrial Services about**
12 **having done so.**

13 Thompson also violated her conditions of release by using computers and lying
14 about it. Last month, Pretrial Services allowed Thompson to attend DEF CON, a large
15 and well-known hacking convention in Las Vegas. On the flight back to Seattle, FBI CS
16 Waymon Ho (who had also attended DEF CON and was returning to Seattle on the same
17 flight) overheard Thompson discussing her Internet and computer use with another
18 passenger. *See* Exhibit 3. According to the other passenger, the conversation started
19 because Thompson was frustrated that she had to pay for Internet access on the plane, and
20 they brainstormed ways to bypass the paywall. Thompson invited him to an Internet
21 Relay Chat (IRC) that she ran and offered to connect with him on Discord (an instant
22 messaging social media platform). *Id.*

23 During their conversation, Thompson also discussed packing malware to evade
24 detection, using "teamspeak" (a VoIP communication system for online gaming), and
25 playing a lot of Counter-Strike and Minecraft (two video games usually played online
26 with other users).

1 This computer usage exceeded what was authorized by Pretrial Services, as
2 Thompson was only permitted to be online for employment-related activity and job
3 searching. When Pretrial Services confronted Thompson about her unsanctioned use of
4 computers, she denied it. It is only through happenstance that the government and
5 Pretrial Services learned about Thompson's computer activities. Private computer usage
6 is notoriously difficult for Pretrial Services and Probation to monitor effectively,
7 underscoring the fact that Thompson's perspective on the law and its consequences are
8 more important to protecting community safety than post-conviction supervision.

9 I. SENTENCING GUIDELINES

10 Probation has correctly calculated the base offense level as 7, with a 22-level
11 upward adjustment for a loss of more than \$25 million, a 2-level upward adjustment for
12 an offense affecting 10 or more victims, a 2-level upward adjustment for an offense
13 involving sophisticated means, and a 4-level upward adjustment for being convicted of an
14 offense under 18 U.S.C. § 1030(a)(5)(A). PSR ¶¶ 53-57. Therefore, the total offense
15 level is 37. PSR ¶ 64. Because Thompson has never demonstrated acceptance of
16 responsibility for her crimes, Probation has not allocated a 3-level reduction for
17 acceptance of responsibility. PSR ¶ 63.

18 Based on a Criminal History Category of I and a total offense level of 37,
19 Thompson's sentencing range under the Guidelines is 210 to 262 months of
20 imprisonment. PSR ¶ 124.

21 *Defense Objections*

22 Thompson indicated in her objections that she "maintains her innocence of the
23 counts of conviction under the operative case law." The following objections remain
24 outstanding.
25
26

1 **A. Thompson is not entitled to a reduction for acceptance of responsibility**
 2 **because she does not accept responsibility.**

3 As her counsel made clear, Thompson still “maintains her innocence.” She is free
 4 to do that, but she cannot both deny she committed these crimes and accept responsibility
 5 for committing them. Those are fundamentally inconsistent positions.

6 For a defendant to meet her burden to obtain a reduction for acceptance of
 7 responsibility, she must manifest a “genuine acceptance of responsibility for her actions,”
 8 based on her on “statements and conduct” that make it “clear” her contrition is sincere.
 9 *United States v. Cortes*, 299 F.3d 1030, 1038 (9th Cir. 2002). The reduction’s “primary
 10 goal” is to “reward defendants who are genuinely contrite.” *United States v. Green*, 940
 11 F.3d 1038, 1042 (9th Cir. 2019). As this memorandum makes clear, Thompson is not,
 12 and has never been, genuinely contrite about committing these crimes.

13 **B. Probation’s loss calculation and associated Guidelines adjustment is**
 14 **supported by clear and convincing evidence.**

15 Consistent with U.S.S.G. § 2B1.1(b)(1)(L), Probation has appropriately assigned a
 16 22-level enhancement for a loss exceeding \$25 million.² Specifically, Probation has
 17 calculated a loss of approximately \$40 million to Capital One, based on the following
 18 expenditures that are directly attributable to Thompson’s conduct: (1) costs associated
 19 with identifying and remediating the breach; (2) costs associated with storing large
 20 volumes of log data and remediating storage buckets; (3) costs associated with analyzing
 21 the stolen data to determine the number and identity of customers affected, (4) costs
 22 associated with notifying affected customers, and (5) costs associated with responding to
 23

24 _____
 25 ² The government also believes that Capital One’s class-action lawsuit settlement is properly included in the loss
 26 calculation as direct and reasonably foreseeable consequences of Thompson’s hack. However, given that the
 government’s recommendation remains well below the Guideline range calculated by Probation based on a \$40
 million dollar loss, it is unnecessary for the Court to decide that issue or include that amount in the Guidelines
 calculation.

1 customer concerns, including providing credit monitoring services. *See* Exhibit 4, Watts
2 Decl. (filed under seal).

3 Notably, most of these costs were incurred because Thompson downloaded
4 customer data. These massive financial losses would not have been incurred if
5 Thompson had acted as a good-faith security researcher and reported the vulnerability
6 rather than exploiting it.

7 U.S.S.G. § 2B1.1(b)(1) provides that a defendant’s offense level should be
8 adjusted upward if the actual loss caused by the offense exceeds certain thresholds. The
9 Guidelines’ commentary clarifies that “[a]ctual loss’ means the reasonably foreseeable
10 pecuniary harm that resulted from the offense.” U.S.S.G. § 2B1.1, cmt. n.3(A)(i). The
11 commentary further explains that “[r]easonably foreseeable pecuniary harm’ means
12 pecuniary harm that the defendant knew or, under the circumstances, reasonably should
13 have known, was a potential result of the offense.” *Id.* cmt n.3(A)(iv). It is reasonably
14 foreseeable that the victim of a hack will have to pay the technological costs of
15 remediation, costs associated with analyzing the scope of the breach (including the scope
16 of any data exfiltration), and customer relations costs (such as notifying customers about
17 the breach, responding to customer inquiries about the breach, and taking steps to
18 mitigate the impact of the breach through proactive steps like identity protection services
19 or credit monitoring). *See* Exhibit 4, Watts Decl. (filed under seal); *see also* Seth Edgar
20 Testimony, Trial Tr., Vol. 7, 6/15/22, p. 23 (Dkt. 345) (noting that, under different
21 circumstances, Michigan State University “very well could have been declaring a data
22 breach instead, and notifying the attorneys general all over the U.S., and notifying
23 victims and buying identifying protection services, and all the rest of it”).

24 In addition, it is worth noting that a substantial portion of Capital One’s losses fall
25 within a Guidelines provision specific to offenses under 18 U.S.C. § 1030. *See* U.S.S.G.
26 § 2B1.1, cmt. n.3(A)(v)(III). This provision includes certain categories of pecuniary

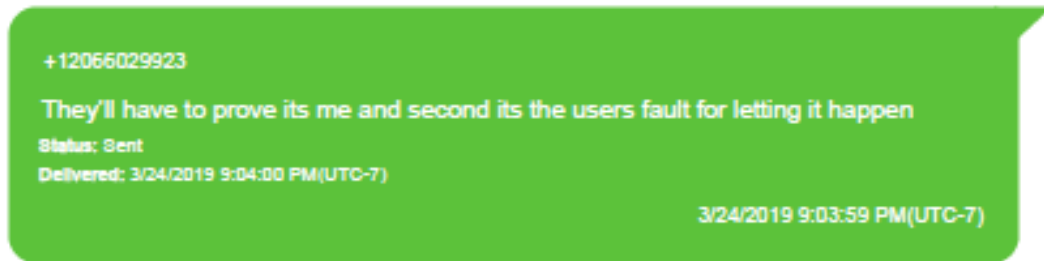
1 harm as actual loss, regardless of whether that harm is foreseeable. Such costs include
2 “any reasonable cost to any victim, including the cost of responding to an offense,
3 conducting a damage assessment, and restoring the data, program, system, or information
4 . . . and any revenue lost, cost incurred, or other damages incurred because of interruption
5 of service.” *Id.* This provision clearly covers the costs that Capital One incurred to
6 confirm that it had identified and remediated the vulnerability, as well as the costs it
7 incurred to confirm the number of impacted customers. *See* Exhibit 4, Watts Decl. ¶¶ 3-5
8 (filed under seal). Therefore, at a bare minimum, Thompson is responsible for at least
9 \$3.245 million in loss without any determination of foreseeability. The CFAA-specific
10 loss category likely also includes the costs of notifying affected customers, responding to
11 customer concerns, and remediating the harm to customers through identity protection
12 and credit monitoring services. *See id.* ¶¶ 7-9. Regardless, even if customer notification,
13 response, and harm/risk mitigation did not fall within this special provision for CFAA
14 offenses, those costs would still be counted as reasonably foreseeable pecuniary harm
15 under the Guidelines. *See id.* cmt n.3(A)(iv).

16 Finally, the Court should reject Thompson’s argument that Capital One should be
17 blamed for its losses rather than her. Thompson has not provided any authority that
18 supports her position. Further, this argument not only ignores the decisions Thompson
19 made that caused these losses, it also sets a terrible precedent that could be extended to
20 any victim of a phishing attack or spam call who unwittingly gave their financial and
21 personal identifying information to a cybercriminal. Setting aside the parties’ dispute
22 over whether this was an anomalous vulnerability or not, there is no legal authority or
23 policy reason to blame Capital One for the losses it suffered or ignore those losses when
24 assessing an appropriate sentence. These losses “resulted from the offense,” and all
25 should be counted as loss and factored into the Court’s sentencing calculations under
26 U.S.S.G. § 2B1.1(b)(1).

1 **II. THE GOVERNMENT’S SENTENCING RECOMMENDATION**

2 **A. Thompson is not sorry.**

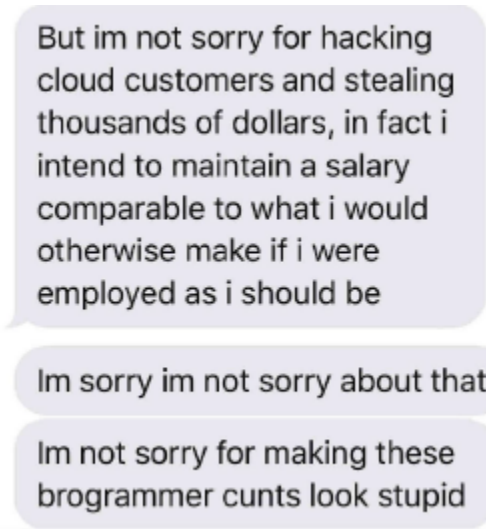
3 Three days after hacking Capital One and downloading its data, Thompson wrote
4 to a friend:



5
6
7
8
9
10 Trial Exhibit 502. Four months later, and only about two weeks before her arrest,
11 Thompson explained her hacking scripts to a friend, invited the friend to hack AWS
12 companies, and wrote:

13 [11:51:32] <erratic> but yeah if you just wanna use it to learn how to do some
14 shit with aws go for it its not my shit lol

15
16 Trial Exhibit 460. Around that same time, Thompson texted a friend:



17
18
19
20
21
22
23
24
25
26 Trial Exhibit 551, 554 (not offered).

1 *“It’s the victims’ fault for letting it happen.”*

2 *“Look how much smarter I am than the victims I hacked.”*

3 *“Sorry, I’m not sorry.”*

4 *“What’s the big deal anyway?”*

5 These were not just the excuses Thompson made at the time of the crime—they
6 were the themes of her defense at trial nearly three years later. *See* Def.’s Mtn. to
7 Dismiss CFAA Counts, p. 10-11 (Dkt. 123) (arguing that Thompson used “the *very*
8 *same*” techniques as a “white hat hacker” and that the government was selectively and
9 arbitrarily prosecuting Thompson) (emphasis in original); Defense’s Oral Argument,
10 3/15/22, p. 9 (Dkt. 221) (arguing that Thompson’s intent to commit crimes did not matter
11 because “you could think you took \$5 from somebody, later realize you didn’t”); Defense
12 Opening, Trial Tr., Vol. 2, 6/13/22, p. 57 (Dkt. 340) (asserting that Thompson
13 “request[ed] credentials that anyone could ask for” and that “the government is trying to
14 criminalize accessing publicly accessible information”); Defense Closing, Trial Tr., Vol.
15 8, 6/17/22, p. 72 (Dkt. 346) (“Ms. Thompson is here because she read the instruction
16 manual, and Capital One did not.”); Def.’s Mtn. for a New Trial, p. 9 (Dkt. 360) (denying
17 that Thompson intentionally violated access permissions); Def.’s Reply to Mtn. for a
18 New Trial, p. 8 (Dkt. 368) (proffering evidence that some Capital One employees
19 assumed Thompson was a good-faith security researcher—before they realized that she
20 downloaded the data and threatened to disseminate it).³

21 Thompson was convicted by a jury that rejected her defenses and found her guilty
22 of five felonies and two misdemeanors. She was convicted of perpetrating a scheme to
23 defraud and illegally hacking computers in ways that caused significant amounts of
24

25 ³ This evidence was available for the defense to admit at trial. The defense likely chose not to offer that evidence
26 because the witnesses who wrote those messages would have testified that their initial impressions changed after
they learned Thompson stole data. Data theft is fundamentally inconsistent with a good-faith security interest.

1 damage. Yet Thompson still believes and argues, to this day, that she did nothing wrong.
2 And not only is she not contrite, after her arrest, she continued a problematic pattern by
3 continuing to live on the financial proceeds of her crime, violating conditions of pretrial
4 release, and lying to Pretrial Services about her violations.

5 These crimes were not the victims' fault; they were Thompson's fault. No one can
6 create an impenetrable security system, no matter how hard they try, how many security
7 professionals they hire, and how much money they spend. Perfect security is not, cannot
8 be, and will never be the standard. The standard is: Don't circumvent other people's
9 security measures to hack into their computer systems.

10 At trial, the defense called Seth Edgar, Michigan State University's Chief
11 Information Security Officer at the time of the breach, as a witness. Edgar explained why
12 Thompson's hack *was* big deal, even for a victim like Michigan State University that
13 ultimately determined it had not lost any sensitive data. He testified, "So regardless of
14 the content of the data for a moment, this is unauthorized access . . . I understand this is
15 public data – but imagine the attacker doesn't know what they're attacking. Imagine the
16 system was a healthcare system instead, and now they're accessing patient data, or
17 system storing credit card numbers, or a power plant, or a water-treatment plant, or – the
18 list goes on and on right?" He continued, "I – I consider this a near miss. Right? This
19 happened to be public data. Thank goodness for me, or for the university in this case."
20 Trial Tr., Vol. 7, 6/24/22, p. 23 (Dkt. 345).

21 Thompson's hack cost people sleepless nights and weeks of work to figure out the
22 problem, fix it, and mitigate the damage from the stolen data and compromised resources.
23 This was true even for victims like Michigan State University, which survived the hack
24 without significant data loss. *See* Exhibit 5. In Capital One's case, the hack not only
25 caused *months* of work and tens of millions of dollars in financial losses, it caused
26 anxiety to the millions of customers whose data was stolen, who did not know what had

1 been done with their information and who, at a minimum, did not want their personal
2 information stored on a computer in Thompson’s bedroom or uploaded to a server farm
3 in Russia.⁴ Several other victims were afraid that simply having their names associated
4 with this high-profile case would cause serious reputational harm.

5
6 **B. Thompson advanced a false narrative that she was a “white hat
7 hacker.”**

8 Thompson’s crimes are all the more aggravated because she knew, at the time, that
9 she was breaking the law and did it anyway. But instead of accepting responsibility and
10 showing remorse afterward, she crafted a false narrative in which she is the hero and her
11 victims are the villains.

12 Thompson misled the jury and the public by suggesting that she was a “white hat
13 hacker.”⁵ Her lawyers told the New York Times that her activities were “the same
14 practices used by legitimate security researchers and should not be considered criminal
15 activity.”⁶ But the evidence never supported Thompson’s claims. At trial, the jury and
16 the Court heard from an actual security researcher and “white hat hacker” who testified
17 that downloading data, cryptojacking, deleting logs, creating security groups, and setting
18 up backdoors with keypairs for persistent access all clearly violate the established norms
19 of good-faith security research and have dire consequences for victim companies. If he
20 had been permitted to offer an opinion regarding Thompson’s conduct, the government’s
21 cybersecurity expert would have testified that what Thompson did—using stolen security

22
23 ⁴ Again, it was fortunate that the FBI and Capital One acted quickly to arrest Thompson and retrieve the data *before*
24 it could be uploaded anywhere.

25 ⁵ Conger, Kate, “Fraud and Identity Theft Trial to Test American Anti-Hacking Law,” New York Times (June 8,
26 2022), *available at*: <https://www.nytimes.com/2022/06/08/technology/capital-one-hacker-trial.html> (last visited
Sept. 21, 2022).

⁶ *Id.*

1 credentials to access cloud computing accounts, exfiltrate data, cryptojack—crossed the
2 line into “black hat hacking.”

3 At a fundamental level, good-faith security researchers are motivated to improve
4 cybersecurity and make the Internet safer. That was not Thompson’s motivation.
5 Thompson was motivated to make money at other people’s expense, to prove she was
6 smarter than the people she hacked, and to earn bragging rights in the hacking
7 community. Perhaps Thompson’s cybercrimes are less egregious than cybercrimes
8 committed by people whose sole purpose is to steal and use data to make money. But
9 that is not the same as saying, as Thompson does, that her cybercrimes carry no moral
10 culpability. Culpability is a continuum, not a dichotomy. As this case illustrates, once a
11 person illegally accesses a computer system, the extent of the harm is often a function of
12 sheer luck. This is why Congress criminalizes the act of illegal hacking, separate and
13 apart from the act of disseminating data, and why the United States Sentencing
14 Commission focuses its Guidelines calculation on the harm to the victim, not the money
15 that a person makes from the crime.

16 Thompson never should have hacked these companies. She never should have
17 used their accounts for cryptomining. She should never have stolen their data. And once
18 she stole their data, she should never have kept it on her computer, archived it, and
19 looked for places to upload it. As the government explained at trial, there were numerous
20 off-ramps Thompson could have taken to act ethically, if ethical hacking had truly been
21 her goal. She likely would have earned a “bug bounty” by making responsible
22 disclosures. But she had no plan for, and no interest in, responsible disclosures because
23 she was not conducting good-faith security research. She was hacking computers to
24 cryptojack and steal data.

25 Even now, there is still a large chasm between the innocuous way that Thompson
26 characterizes her conduct and what the evidence proved she did. That disconnect is

1 particularly troubling because, if Thompson had actually acted like a good-faith security
2 researcher, the victims would not have incurred the significant harm they suffered as a
3 result of Thompson's hacking. The victims were harmed *because* Thompson did not act
4 in good faith. The victims had to spend countless hours working to find, understand, and
5 resolve the vulnerability because Thompson did not contact them directly or make herself
6 available (even anonymously) to explain the vulnerability she exploited, as a good-faith
7 security researcher would have done. The victims had to work with AWS to resolve
8 inexplicably large bills that Thompson racked up through cryptojacking. A good-faith
9 security researcher would not have stolen other people's resources and left them to pick
10 up the check. And the victims had to spend countless hours figuring out what data
11 Thompson had stolen and what the impact was to their customers and their operations,
12 when a good-faith security researcher would never have taken any data. Thompson needs
13 to be held accountable for the stress, time, and massive financial loss that was caused by
14 her decision *not to be* a good-faith security researcher. That need for accountability is all
15 the more acute because Thompson continues to mischaracterize her conduct to this day
16 and demonstrates no remorse for it.

17
18 **C. The criminal justice system plays a critical role in cybersecurity by**
19 **detering illegal hacking.**

20 As the Court is aware, Thompson's case has garnered a tremendous amount of
21 national and international media attention. Tellingly, Thompson's release on pretrial was
22 expressly referenced in the correspondence of international criminal actors under FBI
23 investigation for a different hacking scheme. Throughout the world, the public, security
24 professionals, and cybercriminals are watching the outcome of this case. Security
25 professionals are considering whether they can expect accountability from the criminal
26 justice system in future cases. Cybercriminals are weighing the rewards of hacking

1 against the anticipated costs. This is true both of financially motivated hackers, and of
2 individuals who hack for ideological or political reasons, for notoriety, or just for the
3 thrill of it.

4 Because no system is completely secure and breaches are inevitable, individuals
5 and companies rely on incentives and disincentives for people to do the right thing when
6 they identify a vulnerability: do no harm and report it so it can be fixed. The incentives
7 for responsible disclosure are bug bounties and the less quantifiable positive feeling of
8 helping someone else and making the world a better place. The disincentives are the
9 consequences of breaking the law. If the incentives for breaking the law, whether
10 financial or non-financial, outweigh the perceived consequences, more people will
11 choose to break the law. A sentence that does not include a significant period of
12 imprisonment in a case of this magnitude will not be perceived as a sufficient sanction to
13 deter future hackers.

14 **D. The mitigating factors of Thompson’s background do not eliminate the**
15 **need for the Court’s sentence to provide accountability and have a**
16 **deterrent effect.**

17 The Court will consider Thompson’s history and characteristics when imposing
18 sentence, and rightly so. Thompson has undeniably encountered numerous challenges in
19 her life that have threatened her mental and physical well-being. And the trauma of her
20 lived experiences no doubt affected her mindset while she was committing these crimes.
21 These are mitigating factors, and the government does not suggest otherwise. Even so,
22 Thompson inflicted massive harm and engaged in serious conduct that cannot be ignored.

23 The government recognizes that Thompson faces significant challenges and risks
24 as a transgender woman in prison. It is also appropriate for the Court to consider those
25 circumstances when imposing a sentence, just as it would consider any other person’s
26 medical or psychological prognosis in a prison setting. Unfortunately, there is no way to

1 predict the exact circumstances of Thompson’s confinement, such as her housing
2 designation, before she is sentenced.

3 The Bureau of Prisons has gone to significant effort to meet the needs of its
4 transgender population and reconsidered past policies and practices that emphasized an
5 individual’s sex assigned at birth over an individual’s gender identity, gender expression,
6 and safety. There are approximately 1,480 transgender inmates currently in BOP
7 custody. On January 13, 2022, the Bureau of Prisons issued a manual to standardize
8 procedures and policies for working with transgender inmates, and to provide more
9 awareness and education for staff around increased risks that transgender inmates face.⁷
10 The policy established a Transgender Executive Council (TEC) as the authority on issues
11 affecting the transgender population, and directed the Warden of each penal institution to
12 “establish a multi-disciplinary approach to the management of transgender inmates.”⁸
13 Facility designations are ultimately determined by the TEC based on a broad
14 consideration of factors that include current gender expression, medical and mental health
15 needs, and vulnerability.⁹ The Bureau of Prisons indicated that TEC will not make
16 designation decisions before sentencing. It remains entirely possible, but uncertain, that
17 Thompson could be designated to a female institution.

18 Even though some amount of downward variance is justified based on
19 Thompson’s history and characteristics, the Court must consider that it is varying
20 downward from a starting point of 17.5 to 22 years in prison. Some consideration of
21 Thompson’s mitigating circumstances is entirely appropriate; too much consideration
22 loses sight of the seriousness of her crimes, reduces any deterrent effect, and creates
23 unwarranted sentencing disparity.

25 ⁷ <https://www.bop.gov/policy/progstat/5200-08-cn-1.pdf>

26 ⁸ *Id.*, pp. 4-5.

⁹ *Id.*, pp. 5-6.

1 This Court routinely sentences people who have experienced terrible trauma, such
2 as fleeing a war-torn country and living in refugee camps, enduring horrific abuse in
3 foster homes, or being introduced to a life of violence and drug addiction by careless and
4 neglectful parents. The appropriate sentence in those cases is always a balance between
5 the need for rehabilitation, compassion, and understanding, and the need for
6 accountability, deterrence, and just punishment. Even when confronted with the most
7 devastating traumas, the interests of rehabilitation, compassion, and understanding are
8 never the only interests before the Court, to the exclusion of all others.

9 Considering the Guidelines range for Thompson’s offense and all of the
10 aggravating factors in this case—most significantly, the fact that Thompson committed
11 one of the largest data breaches in history, the huge harm she caused, the fact that she
12 kept committing the same crime over and over again, her refusal to accurately
13 characterize the conduct she engaged in, acknowledge her culpability, or apologize for
14 the harm she caused, and the need to deter similar conduct—a sentence that does not
15 include a significant term of imprisonment would be substantively unreasonable in light
16 of the Guidelines and in consideration of the 3553(a) factors.

17 //

18 //

1 **VI. CONCLUSION**

2 For the foregoing reasons, the government respectfully asks the Court to impose a
3 sentence of 7 years (84 months) in prison, to be followed by five years of supervised
4 release.

5
6 DATED: September 27, 2022.

7 Respectfully submitted,

8 NICHOLAS W. BROWN
9 United States Attorney

10 *s/ Andrew C. Friedman*

11 *s/ Jessica M. Manca*

12 *s/ Tania M. Culbertson*

13 ANDREW C. FRIEDMAN

14 JESSICA M. MANCA

15 TANIA M. CULBERTSON

16 Assistant United States Attorneys

17 700 Stewart Street, Suite 5220

18 Seattle, Washington 98101

19 Phone: (206) 553-7970

20 E-mail: Andrew.Friedman@usdoj.gov

21 Jessica.Manca@usdoj.gov

22 Tania.Culbertson@usdoj.gov