U.S. Department of Justice

United States Attorney
Eastern District of New York

271 Cadman Plaza East
Brooklyn, New York 11201

DMP
F.#2020R01165

September 3, 2024

By ECF and Email

The Honorable Margo K. Brodie
Chief United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: United States v. Stephen Mead
Criminal Docket No. 21-48 (MKB)

Dear Chief Judge Brodie:

The government respectfully submits this letter in advance of the sentencing of the defendant Stephen Mead, scheduled for September 12, 2024, at 10:30 a.m.

In brief, the defendant used his access to login information and passwords that did not belong to him to steal sensitive and proprietary data from his former employer to benefit his new company, enhance his own standing within that company, and harm his former employer. The defendant's conduct, and that of fellow executives and employees of his new company, contributed to his former company—which was estimated to be valued at more than $100 million—going out of business.

For his conduct, the defendant pled guilty to one count of conspiracy to commit computer intrusions, in violation of Title 18, United States Code, Sections 371 and 1030.[1] The defendant's advisory sentencing range under the United States Sentencing Guidelines ("U.S.S.G." or "Guidelines") is 70 to 87 months' imprisonment, as constrained by the 60-month statutory maximum sentence for the offense of conviction. However, the government acknowledged at the time of the defendant's guilty plea that a sentence below the effective Guidelines range might be appropriate in this case. For the reasons discussed below, the government now respectfully requests that the Court sentence the defendant to a term of 12 months' imprisonment, with credit for the time served in custody awaiting extradition.

[1] The plea proceeding took place before the Honorable Lois Bloom. As discussed below, the government requests that the Court accept the plea prior to sentencing the defendant.

Moreover, although the defendant agreed when he pleaded guilty on June 26, 2024, to pay $67,970 in forfeiture by 30 days in advance of the date of his sentencing (Plea Agreement ¶ 7), the defendant has to date made *no payments* toward the forfeiture amount. The government respectfully requests that the Court impose forfeiture in the amount of $67,970, and enter the proposed Order of Forfeiture filed on August 30, 2024 (ECF No. 27).

I. Factual Background

A. The Defendant and His Employment at the Victim Company

The government agrees with the description of the defendant's conduct set forth in the Presentence Investigation Report ("PSR"). The defendant is a citizen and national of the United Kingdom, and resided in Brooklyn, New York, during the relevant period. From May 2010 to July 26, 2012, the defendant was employed as Senior Vice President for Global Operations and General Manager for North America for CrowdSurge, the victim company. CrowdSurge was a U.K.-based business with U.S. operations headquartered in Brooklyn, New York, that, among other things, offered an online platform through which musicians and other artists could sell presale concert tickets to fans. As part of its offering, CrowdSurge created a proprietary online product – the "Artist Toolbox" dashboard – through which CrowdSurge provided artists and managers with detailed information about fans who purchased their tickets through CrowdSurge's platform. CrowdSurge also created and managed ticketing websites for clients. (PSR ¶¶ 6, 7, 9).

The defendant left CrowdSurge in August 2012. A separation agreement signed by the defendant and CrowdSurge required the defendant to return any material that constituted "Confidential Information," which was defined to include passwords, and also directed the defendant to keep such information confidential and not to share it with any third party. As part of the separation agreement, the defendant was paid $52,970 by CrowdSurge. (PSR ¶ 10).

Following his separation from CrowdSurge, and a one-year "garden leave" period, the defendant was hired by Live Nation, the parent company of Ticketmaster, in July 2013. (PSR ¶ 11). The defendant shared his separation agreement with Live Nation, and he was warned by Live Nation not to retain copies of any confidential or proprietary information of any prior employer and not to use such materials as part of his work for Live Nation. The defendant acknowledged these requirements, but repeatedly breached his obligations under the separation agreement, his agreement with Live Nation, and Live Nation's own internal policies, in his work for Ticketmaster.

B. The Defendant's Criminal Conduct

CrowdSurge was a competitor to Live Nation, and information about CrowdSurge's business activities and client base was of significant value to Live Nation. Despite the defendant's promises not to retain or divulge CrowdSurge's confidential information, the defendant quickly violated those terms, as well as Live Nation policies, by responding to requests from Ticketmaster executives for competitive intelligence about CrowdSurge. In response to these requests, the defendant shared with Ticketmaster employees spreadsheets of internal CrowdSurge financial information and passwords to CrowdSurge's Artist Toolboxes, and used those passwords

to access, without authorization, those Artist Toolboxes to obtain competitive information about CrowdSurge's technology and clients. (PSR ¶ 11).[2]

Specifically, between January 2014 and December 2015, Live Nation and Ticketmaster employees used login credentials provided by the defendant to access without authorization numerous password-protected CrowdSurge Artist Toolboxes. Indeed, after joining Ticketmaster and being asked to provide competitive intelligence about CrowdSurge, the defendant volunteered the login information, which had not specifically been requested by Ticketmaster executives. The defendant personally used the login information to obtain unauthorized access to CrowdSurge's Artist Toolboxes and also provided the login information to others at Ticketmaster so that they could access CrowdSurge's Artist Toolboxes as well. In doing so, the defendant directed others to keep the conduct secret from CrowdSurge. (PSR ¶ 12). The defendant committed, among others, the following acts:

In January 2014, the defendant provided co-conspirator Zeeshan Zaidi and another Ticketmaster employee with CrowdSurge Artist Toolbox login credentials, and advised them to "screen-grab the hell out of the system." The defendant warned the others that "***this is access to a live CS [CrowdSurge] tool I would be careful in what you click on as it would be best not to giveaway*** [sic] ***that we are snooping around.***" (Emphasis in original, bracketed text added.) Later, during a teleconference with Zaidi and a Ticketmaster executive, the defendant gave Zaidi and the Ticketmaster executive a live tour of CrowdSurge's Artist Toolbox, in which the defendant demonstrated the functionality of CrowdSurge's Artist Toolbox application. (PSR ¶ 12(a)).

In May 2014, at Zaidi's request, and in response to concerns from a Live Nation executive that "Crowd surge [*sic*] pushing hard" and a demand "to see exact plan" of a response, the defendant participated in a presentation being given by Zaidi to a room full of Ticketmaster employees and executives at an "Artist Services Summit" in San Francisco about CrowdSurge's Artist Toolbox, during which the defendant accessed CrowdSurge's Artist Toolboxes and gave the Ticketmaster employees and executives a live tour of a password-protected CrowdSurge Artist Toolbox page. Following the meeting, Zaidi and other Ticketmaster employees prepared a presentation for senior executives of Live Nation and Ticketmaster that compared Ticketmaster's offering to CrowdSurge's and included screenshots of CrowdSurge's Artist Toolboxes, obtained using login credentials provided by the defendant. (PSR ¶ 12(b)).

From January 2015 to December 2015, Live Nation and Ticketmaster employees continued to use credentials provided by the defendant to access without authorization CrowdSurge's Artist Toolboxes. IP log data and other evidence confirm that the defendant and

---

[2] Contrary to the defendant's sentencing letter, the information the defendant accessed and shared with Ticketmaster was far more significant than merely "the appearance and design" of the Artist Toolboxes (see ECF No. 26 at 1). It included the identities of artists who were contracting with CrowdSurge rather than Ticketmaster and real-time data about ticket sales through CrowdSurge, including information about where tickets were being purchased, the number of tickets sold at each venue, and information about tickets sold on particular dates.

others at Live Nation and Ticketmaster engaged in unauthorized access of the CrowdSurge computers on at least 20 separate occasions. (PSR ¶ 12(c), 12(d)).

The information the defendant and others obtained was used in presentations to Live Nation and Ticketmaster senior management, to benchmark CrowdSurge's products against Ticketmaster's own products, and to plan a competitive response by developing or improving Ticketmaster's products in an effort to win artist presale ticketing business from CrowdSurge. (PSR ¶ 13).

The defendant also informed Ticketmaster executives and employees that they could access draft and mock sales-pitch websites created by CrowdSurge, which the defendant knew how to access based on his prior employment at CrowdSurge. The websites, while not password-protected, were not indexed in search engines and therefore could not be located by the public using search engines such as Google. Instead, in order to access one of the ticketing web pages, a person would have to figure out its exact Uniform Resource Locator ("URL"), i.e., its webpage address. Because of the defendant's information, Ticketmaster was able to access these website pages. Ticketmaster used this information to learn competitive intelligence about CrowdSurge's clients and to attempt to obtain business from those clients. (PSR ¶ 14).

The defendant's motivation was not merely to help Ticketmaster and to improve his standing with Ticketmaster, but also to harm CrowdSurge. For example, on one occasion the defendant discussed "cut[ting] off CrowdSurge at the knees," and on another he wrote, "[N]ow we can really start to bring down the hammer on CrowdSurge." In January 2015, following much of the conduct described above, the defendant was promoted to Director of Client Service in Ticketmaster's Artist Services Division, reporting directly to Zaidi. (PSR ¶¶ 10, 11, 14).

C. Related Criminal and Civil Litigation

In December 2015, CrowdSurge filed a civil suit against Ticketmaster. In January 2018, Ticketmaster and CrowdSurge (which had by that time declared bankruptcy) settled the civil lawsuit. Ticketmaster paid $110 million to the owners of CrowdSurge, and Ticketmaster also acquired the remaining assets of CrowdSurge, including the intellectual property and code related to the Artist Toolbox that was the focus of the defendant's criminal intrusions. (PSR ¶ 15).

On October 18, 2019, Zaidi, the defendant's supervisor and co-conspirator, pled guilty to a single-count Information in the Eastern District of New York, charging him with a conspiracy to commit computer intrusion and wire fraud, in violation of 18 U.S.C. § 371. See United States v. Zaidi, No. 19-CR-450 (MKB). Zaidi has not yet been sentenced. (PSR ¶ 21).

On December 30, 2020, Ticketmaster, the defendant's employer during the time of the conspiracy, entered a deferred prosecution agreement (the "DPA"), which was filed along with an Information charging Ticketmaster with (i) conspiracy to violate the Computer Fraud and Abuse Act in violation of 18 U.S.C. § 371 (specifically to violate 18 U.S.C. §§ 1030(a)(2)(C) and 1030(a)(4)); (ii) computer intrusion for commercial advantage or private financial gain, in violation of 18 U.S.C. § 1030(a)(2)(C); (iii) computer intrusion in furtherance of fraud, in violation of 18 U.S.C. § 1030(a)(4); (iv) conspiracy to commit wire fraud and (v) wire fraud, in violation of

18 U.S.C. §§ 1343, 1349. See United States v. Ticketmaster, No. 20-CR-563 (MKB). As part of the DPA, Ticketmaster paid a $10 million fine. On or about July 11, 2024, Ticketmaster completed the terms of the DPA, and the Information was dismissed by the government. (PSR ¶ 16).

D. The Defendant's Return to the United Kingdom, Arrest in Italy, and Extradition to the United States

During the investigation of his criminal conduct, and after the defendant's counsel had been in contact with the government about the investigation, on or about October 14, 2019, the defendant departed the United States and returned to the United Kingdom. The defendant did not violate any legal obligations by leaving the country, but he was aware of the ongoing criminal investigation at the time of his departure. The defendant did not return to the United States until he was arrested in Italy and extradited, as described further below. (PSR ¶ 17).

On January 25, 2021, the defendant was charged by Indictment with in Conspiracy to Commit Computer Intrusions, in violation of Title 18, U.S. Code, Section 371 (Count One); Computer Intrusion of a Protected Computer, in violation of Title 18, U.S. Code, Sections 1030(a)(2)(C), 1030(c)(2)(A), 1030(c)(2)(B) and 2 (Count Two); Computer Intrusion in Furtherance of Fraud, in violation of Title 18, U.S. Code, Sections 1030(a)(4), 1030(c)(3)(A) and 2 (Count Three); Wire Fraud Conspiracy, in violation of Title 18, U.S. Code, Section 1349 (Count Four); and Wire Fraud, in violation of Title 18, U.S. Code, Sections 1343 and 2 (Count Five). A warrant for the defendant's arrest was issued, and the government secured an Interpol "red notice" for foreign assistance with his arrest. (PSR ¶ 18).

On or about February 29, 2024, the defendant was arrested by Italian authorities after traveling to Ciampino, Italy, and extradition proceedings were commenced by the United States. After agreeing to the terms of the operative guilty plea, the defendant consented to his extradition and was brought to the United States on or about June 15, 2024. On June 26, 2024, the defendant pled guilty before Chief Magistrate Judge Bloom to Count One of the Indictment, conspiracy to commit computer intrusions. (PSR ¶¶ 19-20). The government is providing to the Court a copy of the transcript of the plea proceeding, and requests that the Court accept the plea.[3]

The defendant has been released on bail since his arraignment.

---

[3] The government notes one inaccuracy in the plea colloquy. The Court advised the defendant that "The United States Attorney's Office will not recommend to the Court a specific sentence to be imposed. . . ." (See Plea Tr. at 23). In fact, the plea agreement contained no such limitation. The government respectfully requests that the Court correct that misstatement and confirm that the defendant still wishes to persist in his plea of guilty.

The government is not publicly filing the plea transcript because defense counsel has requested that certain portions of the transcript reflecting the defendant's private medical information be redacted. (See ECF No. 23).

II. Applicable Law

It is settled law that "a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range. As a matter of administration and to secure nationwide consistency, the Guidelines should be the starting point and the initial benchmark." Gall v. United States, 552 U.S. 38, 49 (2007) (citation omitted). Next, a sentencing court should "consider all of the § 3553(a) factors to determine whether they support the sentence requested by a party. In doing so, [it] may not presume that the Guidelines range is reasonable. [It] must make an individualized assessment based on the facts presented." Id. at 50 (citation and footnote omitted). "When a factor is already included in the calculation of the [G]uidelines sentencing range, a judge who wishes to rely on that same factor to impose a sentence above or below the range must articulate specifically the reasons that this particular defendant's situation is different from the ordinary situation covered by the [G]uidelines calculation." United States v. Sindima, 488 F.3d 81, 87 (2d Cir. 2007) (quotation omitted, alterations in original). "[W]here the sentence is outside an advisory Guidelines range, the court must also state 'the specific reason' for the sentence imposed, in open court as well as in writing – 'with specificity in a statement of reasons form' that is part of the judgment." United States v. Aldeen, 792 F.3d 247, 251-252 (2d Cir. 2015), as amended (July 22, 2015) (quoting 18 U.S.C. § 3533(c)(2)).

Title 18, United States Code, Section 3553(a) provides that, in imposing sentence, the Court shall consider:

> (1) the nature and circumstances of the offense and the history and characteristics of the defendant;
>
> (2) the need for the sentence imposed –
>
> > (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
> >
> > (B) to afford adequate deterrence to criminal conduct; [and]
> >
> > (C) to protect the public from further crimes of the defendant.

At sentencing, "the court is virtually unfettered with respect to the information it may consider." United States v. Alexander, 860 F.2d 508, 513 (2d Cir. 1988). Indeed, Title 18, United States Code, Section 3661 expressly provides that "[n]o limitation shall be placed on the information concerning the background, character, and conduct of a person convicted of an offense which a court of the United States may receive and consider for the purpose of imposing an appropriate sentence."

Thus, the Court must first calculate the correct Guidelines range, and then apply the 3553(a) factors to arrive at an appropriate sentence, considering all relevant facts. To the extent there remain any open issues as to the correct Guidelines range, the Court should first make any

necessary finding to arrive at the correct range. Nevertheless, however the Court arrives at the correct Guidelines range, it still must fashion a sentence that meets the criteria of Section 3553(a) under the specific facts of this case.

III. The Advisory Guidelines Sentence

Consistent with the plea agreement, the government respectfully submits that the following is the appropriate Guidelines calculation:

Base Offense Level (U.S.S.G. § 2B1.1(a)(2))		6
Plus:	Loss exceeded $65 million (U.S.S.G.§ 2B1.1(b)(1)(M))	+24
Plus:	Offense resulted in substantial financial hardship to a victim (U.S.S.G. § 2B1.1(b)(2)(A)(iii))	+2
Less:	Zero-Point Offender (U.S.S.G. § 4C1.1)	-2
Less:	Acceptance of Responsibility (U.S.S.G. § 3E1.1)	-3
Total Offense Level		**27**

Based on a total offense level of 27 and criminal history category of I, the defendant's estimated Guidelines range is 70 to 87 months. Because the count of conviction has a statutory maximum sentence of 5 years, the defendant's effective Guidelines range is 60 months' imprisonment. The defendant stipulated to this calculation in the plea agreement.

In the PSR, the Probation Department added a two-level enhancement under Section 3B1.3 for the defendant's abuse of a position of trust in a manner that significantly facilitated the commission of the offense. (PSR ¶ 30). This enhancement was not included in the plea agreement. The defendant objected to this enhancement in his objection to the PSR. Consistent with the plea agreement, the government does not seek to apply this enhancement. The government notes that the Court need not decide the application of this enhancement, because even without that enhancement, the resulting Guidelines range exceeds the statutory maximum sentence for the offense of conviction. See Fed. R. Crim. P. 32(i)(3)(B).

IV. The Court Should Sentence the Defendant to a Term of 12 Months' Imprisonment

The sentence imposed on the defendant must reflect the seriousness of the conduct, deter the defendant from committing further crimes, deter others from committing similar crimes, and promote respect for the law. These factors counsel in favor of a sentence of 12 months'

imprisonment, with credit for the time that the defendant served in custody in Italy awaiting extradition to the United States.[4]

As an initial matter, although the advisory Guidelines call for a sentence of 60 months' imprisonment, the government believes that the Guideline is not an appropriate measure of the defendant's culpability in this particular instance given the unique facts of this case. Indeed, in the plea agreement, the government stated that it "acknowledges that a sentence below the effective Guidelines range may be appropriate in this case." (Plea Agreement ¶ 2). That is because, in this case, the Guidelines offense level is driven by the significant loss amount, which the defendant stipulated exceeded $65 million, resulting in a 24-level increase to the offense level. As the defendant notes in his sentencing submission, the defendant did not engage in the criminal conduct in order to personally profit from the scheme, beyond the benefit that the defendant received by improving his standing and his position within Ticketmaster. (ECF No. 26 at 17-18). This stands in stark contrast to standard white-collar criminal cases, for which the Guidelines are intended. Accordingly, the government is not seeking a Guidelines sentence.

Nevertheless, notwithstanding some significant mitigating factors identified by the defendant, the government does not believe that a time-served sentence is appropriate either. Rather, for the reasons set forth below, the government respectfully submits that a period of 12 months' imprisonment is appropriate.

First, the defendant and others at Ticketmaster engaged in serious criminal conduct to benefit Ticketmaster and to harm CrowdSurge. That conduct involved the theft of information about a competing product used by CrowdSurge and about CrowdSurge clients who were using the Artist Toolboxes. The defendant and other Ticketmaster employees who used the login and password credentials that the defendant provided obtained this information through fraud: lying about who they were when they accessed CrowdSurge's Artist Toolboxes via passwords that only a CrowdSurge insider (or their client) could ordinarily access. The defendant took those actions in violation of his separation agreement with CrowdSurge, his acknowledgement to Live Nation that he would not use competitor information in the course of his employment, and Live Nation's own internal policies.

Second, the defendant engaged in this conduct for Ticketmaster's commercial advantage and for the defendant to improve his own standing within Ticketmaster. The defendant notably was promoted following his commission of the crime.

Third, the defendant intended for his criminal conduct to cause substantial harm to CrowdSurge. As noted above, the defendant discussed with others at Ticketmaster how he hoped

[4] To the extent the Court is concerned that a sentence of 12 months' imprisonment means that the defendant could be designated to serve his time at the Metropolitan Detention Center in Brooklyn ("MDC Brooklyn"), the government has been advised that the Bureau of Prison's Designation and Sentence Computation Center has been instructed not to designate to MDC Brooklyn, and if the defendant is not in custody when designated, he can self-surrender to the designated facility.

their conduct would harm CrowdSurge, and the defendant wrote emails about "cut[ting] off CrowdSurge at the knees" and "bring[ing] down the hammer on CrowdSurge."

Fourth, the defendant and Ticketmaster in fact caused significant harm to CrowdSurge through their actions. The evidence shows that Ticketmaster successfully lured clients from CrowdSurge based on Ticketmaster's strategy of obtaining information about artists using CrowdSurge's Artist Toolboxes and then pitching those artists using intelligence that Ticketmaster was able to glean from CrowdSurge. The defendant's efforts on behalf of Ticketmaster to ensure Ticketmaster's own product was competitive or better than CrowdSurge's product and to affirmatively take client business away from CrowdSurge caused pecuniary losses to CrowdSurge. These losses were particularly significant in a highly competitive business environment, and were a contributing factor to CrowdSurge going out of business. Indeed, Ticketmaster employees discussed how stealing even one major client from CrowdSurge could undermine its business.

Finally, there is substantial need for general deterrence. The fact that the criminal conduct required little technical know-how shows how even relatively unsophisticated individuals could use their access to login information and passwords to steal data for their benefit. The fact that this conduct occurred within a large and well-known corporate entity, by a person with no prior criminal history, indicates that this sort of crime is potentially appealing to individuals who would not otherwise think of engaging in criminal activity. An appropriate sentence is necessary to warn others that they will face consequences if they choose to engage in similar misconduct—in other words, to alter the cost-benefit analysis of would-be white-collar criminals. Cf. United States v. Brown, 880 F.3d 399, 405 (7th Cir. 2018) (collecting cases for the proposition that "white-collar criminals act rationally, calculating and comparing the risks and rewards before deciding whether to engage in criminal activity," making them "prime candidates for general deterrence").

In recommending a term of imprisonment of 12 months, the government is also mindful of a number of mitigating factors raised by the defendant, including the defendant's serious health issues since committing the criminal conduct, the defendant's lack of criminal history beyond the instant conduct, and prison conditions that the defendant has endured while awaiting extradition. In addition, the government believes that it would be appropriate for the time that the defendant spent in prison in Italy awaiting extradition to be credited against the sentence imposed by the Court.

However, the government disagrees with several of the factors that the defendant suggests warrant leniency in this case.

First, the defendant appears to suggest that he has been fully cooperative with the government's investigation, has at all relevant times kept the government apprised of his whereabouts, and has offered to voluntarily surrender to face any charges. (ECF No. 26 at 11, 19). In fact, that is not the case. The defendant did not respond "diligently and proactively" to the government's investigation. On the contrary, other than responding to a subpoena, which he was legally obligated to do, the defendant (through counsel) declined to assist the government's

investigation, including by sitting for a voluntary interview.[5] The defendant did not notify the government of his anticipated departure from the United States before he left; rather counsel informed the government of his departure months after the fact. Indeed, the defendant left the United States, intending to permanently relocate to the United Kingdom, less than two weeks after the government filed a public notice with the Court advising that the defendant's co-conspirator Zaidi would waive indictment and scheduled a guilty plea proceeding. While in the United Kingdom, the defendant did not agree to voluntarily surrender to face charges in the United States (ECF No. 26 at 11); rather he sought only to voluntarily surrender to UK authorities in the event an arrest warrant was issued in the United Kingdom, and specifically advised that he "would contest any extradition proceedings." (ECF No. 26, Ex. E, ¶ 9). And while the defendant ultimately consented to his extradition, he appears to have done so only because fighting extradition would have meant substantially more time in an Italian prison pending the resolution of extradition proceedings.

Second, the defendant suggests that the nature of plea discussions prior to the plea agreement warrants leniency (ECF No. 26 at 12-13, 19-20, 29). In fact, while counsel for the government discussed several potential resolutions with counsel for the defendant, including resolutions under Rule 11(c)(1)(B) and Rule 11(c)(1)(C), the government never formally offered either plea agreement, and the Office affirmatively declined to authorize the Rule 11(c)(1)(C) plea that the parties discussed. The only agreement the parties reached is the operative agreement in which the government acknowledged that a sentence below the advisory Guidelines range of 60 months' "may be appropriate" and made no promises about what position it would take at sentencing other than that it would not seek an upward departure.

Third, while the defendant argues that other similarly situated defendants have not been punished with incarceratory sentences (ECF No. 26 at 29-30), the government disagrees that the cases highlighted by the defendant are truly comparable. In the cases on which the defendant relies, the conduct was isolated or limited to a short period of time or was not committed for the purpose of financial gain, unlike the multi-year course of conduct by Mead. In United States v. Hunter, No. 16-CR-355 (E.D.N.Y.), the defendant employed an offshore "hacker for hire" to access another person's email account for information to give the defendant an advantage in negotiations relating to business opportunities. However, unlike here, there was no evidence of financial harm to the victim, and the course of conduct amounted to accessing the victim's email five times over the course of eight days. Indeed, the advisory Guidelines were zero to 6 months' imprisonment. This was not a sustained multi-year campaign, like Mead's. In United States v. Sazanov, No. 17-CR-657 (S.D.N.Y.), the defendant downloaded source code for his employer's proprietary trading platform, tried to prepare the source code in a way he could remove it without detection, and then, after being fired that afternoon, tried to return to his desk to obtain the files with the source code, all on a single day. Over the next two months, the defendant continued

[5] While the government would ordinarily not comment on a defendant's refusal to cooperate with the government's investigation, which a defendant has no obligation to do, the government raises this point merely to correct the misleading impression created by the defendant's sentencing submission that he has in fact been fully cooperative.

contacting his former employer to obtain those files prior to being arrested. His Guidelines range was also zero to 6 months' imprisonment. This was also not comparable to the sustained course of conduct in which Mead engaged, and did not cause any financial injury to the victim. In United States v. Rocchio, No. 16-CR-222 (S.D.N.Y.), the defendant accessed his former supervisor's email account over a period of two years after leaving a job with that employer. It appears that the defendant deleted some emails from the supervisor's account and forwarded others to his own account. Unlike Mead, the defendant did not appear to have been motivated by any financial gain or to have done anything with the information he obtained. The advisory Guidelines range was 6 to 12 months' imprisonment. The government submits that the conduct in each of these cases is not comparable to Mead's conduct, and the probationary sentences that were imposed in each of these three cases are not appropriate here.

In contrast, the government has identified other cases that are more comparable to Mead's conduct. In the Houston Astros-St. Louis Cardinals cyber intrusion case, an employee of the Cardinals professional baseball team—who was a former employee of the Astros—used other peoples' passwords to access the Astros' computer systems (and individual email accounts) to steal confidential analytics data about the team, for the benefit of his new employer. In that case, the defendant pled guilty to five felony computer intrusion counts and was sentenced to 46 months' imprisonment. See United States v. Correa, No. 4:15-CR-679 (S.D.TX). In another comparable case, Judge Bianco sentenced a defendant to 12 months and 1 day of imprisonment for using passwords belonging to other employees to access his former employer's computer systems for the purpose of causing damage to those systems, which caused approximately $19,000 in damage. United States v. Meneses, No. 13-CR-321 (E.D.N.Y. Jan. 9, 2017).

Finally, the government also requests that the Court impose forfeiture in the amount of $67,970, as agreed to in the plea agreement, and enter the proposed Order of Forfeiture filed on August 30, 2024 (ECF No. 27). That amount represents the payment that the defendant received from CrowdSurge upon his separation, given that he did not uphold his obligations under that agreement, and an estimate of the increase in his compensation from Ticketmaster as a result of his employment and promotion resulting from his conduct. Although the defendant agreed approximately two months ago to pay this amount 30 days prior to his sentencing, the defendant has to date made no payments toward his forfeiture obligation.

V. Conclusion

Accordingly, for these reasons, the government respectfully requests that the Court impose a sentence of 12 months' imprisonment, with credit for the time the defendant served in custody awaiting extradition, and order the defendant to forfeit $67,970.

Respectfully submitted,

BREON PEACE
United States Attorney

By: /s/ Douglas M. Pravda
Douglas M. Pravda
Assistant U.S. Attorney
(718) 254-7000

cc: Counsel for the Defendant (by email and ECF)