UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
v.	)	Criminal No. 25-40015-MRG
MATTHEW D. LANE,	)	
Defendant	)	

GOVERNMENT'S SENTENCING MEMORANDUM

Defendant Matthew Lane targeted multiple victim companies for cyberattacks and participated in and profited from the extortion of these victims for millions of dollars in ransom. As a ransom demand to one of the victims recounted, the intent of the scheme was "to destroy your company and bankrupt it to the point of absolute no return if the ransom is not paid." Indeed, Lane caused losses of more than $14 million for that victim and put the victim's customers—including tens of millions of children, some as young as five years old—at risk of identity theft for years to come. The incidents for which Lane faces sentencing are two in a line of criminal cyber activity dating to at least 2021. To protect the public from the continuing danger he poses and to deter others from committing perilous and costly network attacks, the government recommends a sentence of 84 months in prison, three years of supervised release, restitution of $14,075,540.58, and forfeiture as outlined in the government's motion for forfeiture (Dkt. 12).

The Offense Conduct

Lane's Extortion of Victim 1

Between April and May 2024, Lane exploited an earlier data breach of the computer network of Victim 1, a wireless telecommunications company based in the United States, and re-victimized Victim 1 by demanding an additional ransom in exchange for not publicly leaking

Victim 1's data. PSR ¶¶ 8-10. Lane, using an anonymized email address and phone number, purported to be a member of a notorious hacking group in order to induce Victim 1 to pay the $200,000 ransom Lane demanded. *Id.* ¶¶ 9-10. Lane took extensive steps to conceal his identity and discussed getting caught by the "FED" with his co-conspirator, demonstrating an understanding that he knew what he was doing was wrong. *Id.* ¶¶ 9-12, 14, 20, 23, 25. For example, in addition to using an anonymous phone number and email address, Lane discussed with a co-conspirator using burner phones, hiding his IP address with virtual private networks ("VPNs") and eSIMs, directing the proceeds of his crimes to cryptocurrency wallets, transferring those funds to anonymous virtual credit and debit cards, and wearing masks and gloves when taking money from ATMs that support those virtual cards or, alternately, using money mules to withdraw cash for them, all so investigators "will literally find nothing." *Id.* When it appeared that Victim 1 might not pay the ransom, Lane discussed with his co-conspirator identifying and attacking additional victims who would be more likely to pay, including government contractors, or causing a supply chain attack to target 30,000 companies at once. *Id.* ¶¶ 14, 19. Lane's messages make clear he was motivated by greed: he wanted money to buy designer clothing, diamond jewelry, and luxury vehicles. *Id.* ¶¶ 13, 16, 19, 25, 27. As a result of Lane's conduct, Victim 1 incurred losses totaling $59,822.43, which includes the ransom payment as well as fees for a cyber security negotiator, cyber security consultant, and legal services necessary to respond to Lane's offense. *Id.* ¶ 48.

Lane's Intrusion on Victim 2's Computer Network and the Resulting Extortion of Victim 2

In May 2024, while he was extorting Victim 1, Lane commented to his co-conspirator that, "we need to hack another shitty company that[']ll pay. [W]e need SSNs." PSR ¶ 27. By August 2024, Lane had done just that: he gained access to the computer network of Victim 2, a cloud-based software company that helped K-12 schools manage student and teacher data, using stolen employee credentials. *Id.* ¶ 31. By September 2024, Lane had exfiltrated student and teacher data, including Social Security numbers, dates of birth, and confidential medical information, from one of Victim 2's customers, which was one of the largest school districts in California. *Id.* ¶ 32. In December 2024, Lane leased a computer server from a cloud storage provider located in Ukraine to which student and teacher data of Victim 2's customers were exfiltrated the next day. *Id.* ¶ 33. The night he leased the server, Lane told his girlfriend he was "gonna be on the laptop" that night because "I just need to actually make $ for a second," again demonstrating that money and greed motivated his actions. *Id.* Days later, a threat actor claiming to be the same notorious hacking group Lane had professed to be when he extorted Victim 1, claimed to have compromised more than 60 million records of student data and 10 million records of teacher data from Victim 2's customers in the United States, Canada, and elsewhere and demanded a ransom of 30 bitcoin (worth approximately $2.85 million at the time). *Id.* 34. The ransom demands included threats to publicly leak the Social Security numbers of students as young as five years old and warned of the harms that would come to Victim 2, including the message: "Final note, we fully intend to destroy your company and bankrupt it to the point of no absolute return if the ransom is not paid." *Id.* ¶ 36. As a result of Lane's conduct, Victim 2 incurred losses totaling $14,015,718.15, which includes the ransom payment and the cost to provide identity theft protection services for the students and teachers affected by Lane's offense. *Id.* ¶ 48.

Guidelines Calculation

The parties and the Probation Office agree that Lane's Total Offense Level is 27. This calculation is comprised of:

a. an Adjusted Offense Level of 22 on Counts One and Two, which is comprised of a base offense level of 18 under Section 2B3.2(a); a two-level enhancement under Sections 2B3.2(b)(2) and 2B3.1(b)(7)(C) because Lane demanded $200,000 from Victim 1; and a two-level enhancement under Section 3B1.3 because Lane used his intricate knowledge of computer science, programming, and coding in a manner that significantly facilitated his commission and concealment of the offenses;

b. an Adjusted Offense Level of 32 on Count Three, which is comprised of a base offense level of 6 under Section 2B1.1(a)(2); a 20-level increase under Section 2B1.1(b)(1)(K) because the loss was more than $9.5 million but not more than $25 million; a two-level enhancement under Section 2B1.1(b)(10)(C) because the offense involved sophisticated means; a two-level enhancement under Section 2B1.1(b)(18) because Lane was convicted under 18 U.S.C. § 1030 and the offense involved an intent to obtain personal information; and a two-level enhancement under Section 3B1.3 because Lane used his intricate knowledge of computer science, programming, and coding in a manner that significantly facilitated his commission and concealment of the offenses;

c. a grouping analysis under Section 3D1.4 results in a Combined Adjusted Offense Level of 32; and

d. a three-level decrease under Section 3E1.1 for acceptance of responsibility and a two-level decrease under Section 4C1.1(a)(1)-(11) because Lane meets the criteria of a Zero-Point Offender.

Because Lane is in Criminal History Category I, the resulting Guidelines sentencing range for a

Total Offense Level of 27 is 70 to 87 months. Factoring in the mandatory 24-month sentence on Count Four results in a total advisory Guidelines sentencing range of **94 to 111 months**.

Sentencing Recommendation

The government respectfully recommends that a total sentence of 84 months in prison (comprised of 60 months to run concurrently on Counts One, Two and Three, and 24 months to run consecutively on Count Four), 36 months of supervised release, restitution of $14,075,540.58, and forfeiture as laid out in the government's Motion for Forfeiture (Dkt. 12), is sufficient, but not greater than necessary to satisfy the requirements of 18 U.S.C. § 3553(a).

The Nature, Circumstances, and Seriousness of the Offense

Lane's conduct re-victimized Victim 1, threatened the viability of the business of Victim 2, caused tens of millions of dollars in losses, and put innocent children and their teachers at risk of identity theft for years to come. In a matter of months, he targeted at least two victims, participated in extorting more than $3 million in ransom, and put the data of approximately 70 million people at risk. Lane's conduct was sophisticated, involving virtual private networks, eSIMs, anonymized email addresses and phone numbers, stolen credentials, and foreign servers. His extensive conduct coupled with the significant harm he caused warrants a meaningful term of imprisonment.

That Lane has facilitated the return of approximately $160,000 the government was able to trace to his crimes does not reduce the seriousness of his offense, particularly where approximately $3 million remains unaccounted for. The money he returned is barely one percent of the financial loss he caused. Nor will this money make up for the hardship imposed on the nearly 70 million innocent students and teachers who have to navigate the remainder of their lives as identity theft victims.

History and Characteristics of the Defendant

Lane grew up in a safe, small town with, in his words, loving and nurturing parents. PSR ¶ 87. While he disclosed pushing them away when he was younger, he also reported sharing close relationships with all his family members. *Id.* ¶¶ 87, 93. Growing up, all of his basic necessities were met, *id.* ¶ 87, he received treatment for any medical conditions, *id.* ¶¶ 97-98, 101, and he was attending a moderately selective private university with a partial scholarship when he committed the offenses described in Counts Three and Four. *Id.* ¶ 109. Indeed, Lane's conduct was not motivated by desperation nor was he a victim of his circumstances. It was greed. As he discussed with a co-conspirator, he used the money he received from his schemes to buy designer clothes and diamond jewelry. Financial records reflect his spending on extravagant rental apartments and near daily fast-food delivery. Lane could have funded these luxuries through legitimate work—his messages to a co-conspirator describe his plans to work for Google and how he expected his college internships would cover any student debt, *id.* ¶ 19, and even now, he plans to pursue higher education in the future and remains extremely skilled in computer science, research, coding, and cyber security. *Id.* ¶¶ 109, 111. Instead, he chose to use his position to extort companies and victimize them and their customers.

The government acknowledges that Lane was a senior in high school at the time he extorted Victim 1 and a freshman in college at the time of his attack on Victim 2. But the sophistication and planning involved in his crimes and the steps he took to conceal his identity—including identifying which victims to target, gaining access to their networks, negotiating ransom payments with professional cybersecurity companies, hiding the flow of funds from the ransom payments to himself and others—belies any argument that Lane was too young to understand what he was doing was wrong. Further, Lane's upbringing did not involve the risk factors of environment, adverse childhood experiences, substance use, lack of educational opportunities, and familial relationships that might justify a downward departure based on his age. *See* USSC § 5H1.1.

Further, Lane's crimes were not a mistake resulting from an isolated lapse in judgment. Rather, they were part of a pattern of criminal cyber activity dating to 2021 and targeting victims ranging from a school athletic association to private companies to foreign governments. PSR ¶¶ 43-47. That Lane experienced isolation as a result of the COVID-19 pandemic does not excuse his conduct, as millions of students nationwide had the same experience and did not turn to hacking and extorting companies and putting their employees' and customers' personal identifying information at risk. Further, by 2024, when Lane committed the instant offenses, he had returned to in-person classes and had multiple girlfriends. *See, e.g.*, *id.* ¶¶ 20, 33.

That Lane will suffer collateral consequences as a result of his crimes, including remorse for the harm he caused his family and public shame, is not a mitigating factor, but something applicable to nearly all defendants facing criminal charges. Indeed, the First Circuit has said that "it is impermissible for a court to impose a lighter sentence on white-collar defendants than on blue-collar defendants because it reasons that white-collar offenders suffer greater reputational harm or have more to lose by conviction." *United States v. Prosperi*, 686 F.3d 32, 47 (1st Cir. 2012); *see also United States v. Stall*, 581 F.3d 276, 286 (6th Cir. 2009) ("We do not believe criminals with privileged backgrounds are more entitled to leniency than those who have nothing left to lose.").

<u>Deterrence and Promotion of Respect for the Law</u>

The need for both general and specific deterrence heavily weigh in favor of the government's sentencing recommendation. As described in the PSR, Lane has been an active and persistent cyber attacker since at least 2021. In addition to Victims 1 and 2, Lane targeted a minimum of six other victims, including foreign government entities. PSR ¶¶ 43-46. As he described in his own words, Lane planned to target additional victims, including U.S.-government contractors. *Id.* ¶¶ 14, 19. Nor did Lane need much motivation to engage in criminal cyber activity. As he told a co-conspirator, he was willing to "dox,"—that is, publish the private identifying information of individuals online—for just $25. *Id.* ¶ 26. Lane's proclivity for cyber crime will not go away simply because he has been caught this time; indeed, when he was interviewed in connection with the search of his dorm room, he lied to investigators and fabricated a story about receiving packages of cash. *Id.* ¶ 41. In a subsequent interview, Lane lied about ever engaging in extortion, and only admitted his conduct when faced with his indisputable text messages confirming he did just that. Accordingly, a meaningful term of imprisonment is necessary to convey the message to Lane that there are serious consequences for breaking the law, attacking and extorting victims, causing more than $14 million in losses, and putting tens of millions of innocent children and their teachers at risk of identity theft.

Additionally, the government has serious concerns that Lane poses an ongoing threat to the community and remains in denial about the scope of his criminal activity. In a similar case, the court sentenced a young college student to 48 months in prison for cybercrimes, and that sentence was not sufficient to deter him from engaging in additional cybercrimes upon his release from prison. *See United States v. Cameron Lacroix*, No. 14-cr-10162-MLW (D. Mass.); No. 14-cr-10227-PBS (D. Mass.). Like Lane, Lacroix had already engaged in several cyberattacks by his early 20s. Specifically, when Lacroix was 22, he illegally obtained payment card data and personally identifiable information of victims, and at 23, he repeatedly hacked into law enforcement computer servers and obtained sensitive data. *Id.* At the same time, he hacked into his college's computer servers and changed grades for himself and two other students. *Id.* Lacroix was also convicted in a separate case for hacking Twitter accounts. *Id.* Lacroix was sentenced to 48 months in prison for all these crimes. *Id.* Yet, following his release from custody and while on supervised release, Lacroix compromised his employer's computer network in an elaborate prepaid debit card scheme, for which he was sentenced to an additional 24 months in prison. *Id.* The *Lacroix* case demonstrates the need for a meaningful sentence to deter a young, sophisticated cyber attacker like Lane from continuing to engage in crimes that, for someone with his skill, result in easy money and are hard to trace.

Likewise, a significant term of imprisonment is necessary to deter the many others sitting behind their computer screen ready to attack and extort. According to Federal Bureau of Investigation's Internet Crime Complaint Center, in 2024, there were $16 billion in reported losses from internet crime in 2024, up 33% from 2023.[1] Cybersecurity firm CrowdStrike reported that access brokers—specialists who acquire access to organizations and sell it to other threat actors, such as the individual(s) who acquired the credentials Lane used to access Victim 2's network—increased their activity in 2024, including via a 50% surge in advertising between 2023 and 2024.[2] These figures do not account for the likely millions if not more of unreported losses. Indeed, victims may not report attacks for fear of being re-victimized, as occurred with Victim 1, or concerns about retribution, as Victim 2 experienced after the cyber extortionist learned Victim 2 had contacted law enforcement, as required by various laws and regulations. PSR ¶ 38. Further, as demonstrated by Lane himself, cyber threat actors can and do take careful steps to conceal their identity, making investigations difficult. Given the obstacles to receiving reports of and

[1] Available at https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report.

[2] Available at https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0.

investigating cyberattacks, deterrence plays a key role in protecting the public from additional cybercrime.

Avoiding Sentencing Disparities and Providing Just Punishment

The government's 84-month recommendation falls squarely within the range of sentences imposed on defendants within the past five fiscal years whose primary Guideline was § 2B1.1 and who were convicted of at least one count of 18 U.S.C. § 1028A, with a Final Offense Level of 27 and a Criminal History Category of I, after excluding defendants who received a §5K1.1 substantial assistance departure. Of the 23 defendants in this category, the average sentence (which includes outliers) was 77 months, and the median sentence (that is, the midpoint for all 23 defendants) was 84 months—the same as the government's recommendation.

Lane's sentencing memorandum highlights sentences imposed in two hacking cases to suggest that a shorter sentence is appropriate in this instance. First, such cases are clearly outliers given the JSIN data. Second, each case is distinguishable. Among other things, the defendants in the cited cases caused approximately one-third of the more than $14 million loss Lane caused. *See* Judgment, *United States v. Ahmed*, No. 23-cr-00340 (S.D.N.Y.) (Dkt. 50) (approx. $5 million in restitution); Judgment, *United States v. Raoult*, No. 21-cr-00109 (W.D. Wash.) (Dkt. 61) (approx. $5 million in restitution). Additionally, in *Ahmed*, the defendant was sentenced to 36 months on a single count of computer fraud in violation of 18 U.S.C. § 1030. *See* Judgment, *Ahmed*, No. 23-cr-00340 (Dkt. 50). In contrast, Lane is facing two counts under Section 1030 for two separate schemes, plus a related conspiracy count under 18 U.S.C. § 371 and an aggravated identity theft charge under 18 U.S.C. § 1028A. Had the defendant in *Ahmed* also faced an aggravated identity theft charge, his sentence would have increased to 60 months (36 months on the Section 1030 offense, plus 24 months consecutive on the Section 1028A offense). Further, the *Ahmed* court found the defendant's expression of remorse and acceptance of responsibility to be "exceptional," *see* Sentencing Tr. at 36:5-7, *Ahmed*, No. 23-cr-00340 (Dkt. 53), in contrast to Lane who lied to investigators about the scope of his conduct not once, but twice.

In *Raoult*, the defendant was sentenced to 36 months in prison on one count of conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1349 and 3559(g), and one count of aggravated identity theft, in violation of 18 U.S.C. § 1028A. Judgment, *Raoult*, No. 21-cr-00109 (Dkt. 61). Unlike Lane, Raoult was initially detained in Morocco, where he was held in isolation and substandard conditions for 8 months while awaiting extradition. Def. Sent. Mem., *Raoult*, No. 21-cr-00109 (Dkt. 58) at 12. Further, as a foreign national, Raoult was not eligible to be assigned to a minimum-security prison camp, nor was he eligible for early release through completion of First Step Act programming. *Id.* at 13. In contrast, Lane can earn up to 12 months toward early release under the First Step Act, as well as 54 days per year for good time credit. Finally, the *Raoult* court likely factored in the defendant's difficult childhood, including becoming the primary caregiver for his mother when she was diagnosed with cancer when he was 15, helping his brother battle a heroin addiction, and experiencing trauma when another brother was severely wounded when shot in a terrorist attack at a Christmas market in Strasbourg, Germany. *Id.* at 3. While Lane's childhood was not without challenges, the government has accounted for these factors in recommending a below-Guideline sentence.

Conclusion

For the reasons discussed herein and in the Presentence Report, the United States respectfully recommends the Court sentence Lane to 84 months in prison, 36 months of supervised release, restitution of $14,075,540.58, and forfeiture as laid out in the government's Motion for Forfeiture (Dkt. 12).

Respectfully submitted,

LEAH B. FOLEY
United States Attorney

By: *<u>/s/ Kristen A. Kearney</u>*
Kristen A. Kearney
Assistant United States Attorney

Date: October 7, 2025

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

Dated: October 7, 2025

<u>/s/ Kristen A. Kearney</u>
Kristen A. Kearney