U.S. Department of Justice

United States Attorney
Eastern District of New York

271 Cadman Plaza East
Brooklyn, New York 11201

SK
F.#2014R00048

October 3, 2018

By Hand and ECF

The Honorable Eric N. Vitaliano
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: United States v. Djevair Ametovski
Criminal Docket No. 16-409 (ENV)

Dear Judge Vitaliano:

The defendant, Djevair Ametovski, is scheduled to be sentenced on October 5, 2018, for his operation of a global cybercrime enterprise. From behind a keyboard in Macedonia, the defendant obtained stolen credit card data and account information from individuals and businesses around the world, through hacking and fraud, and sold that information to other criminals to use in fraudulent transactions. Importantly, the defendant did not just steal and sell credit card data—he created a global marketplace for that data that made it possible for other criminals to efficiently search for and buy stolen credit card data through a process as easy as buying a book on Amazon, and do so rapidly, anonymously, and using hard-to-trace digital currencies. Over the span of the more than three years that he ran the Codeshop website, the defendant trafficked in more than 1.3 million stolen credit cards and catered to more than 28,000 criminal customers.

There is tremendous public interest in deterring cybercrime. Credit card fraud imposes devastating costs on individuals, businesses, and financial institutions, and erodes confidence in the modern financial system. Criminals like the defendant who manage these criminal enterprises involving hacking and theft hide behind keyboards in foreign countries and are careful to avoid putting themselves at risk of extradition. They use increasingly sophisticated tools and techniques to obfuscate their true identities, and their infrastructure is frequently scattered across multiple international jurisdictions. Identifying these criminals and bringing them to justice—when it is possible at all—requires a massive commitment of law enforcement resources. Now that law enforcement has succeeded in bringing a top-tier cybercriminal to justice, it is imperative to deter other would-be cybercriminals around the world by sending a clear message that attacking and victimizing U.S. citizens, U.S. businesses, and the U.S. economy will result in severe penalties.

For the reasons set forth below, the government respectfully requests that the Court impose a cumulative sentence of 204 months' imprisonment—180 months' imprisonment on Count Two and 24 months' imprisonment on Count Three, to run consecutively—and respectfully submits that such a sentence would be sufficient, but not greater than necessary, to achieve the purposes set forth in 18 U.S.C. § 3553(a).

I. **Background**[1]

The defendant created and operated the Codeshop website—a global marketplace for selling stolen credit and debit card data, bank account credentials, and personal identification information of victims around the world. The website was no ordinary carding forum; it was incredibly sophisticated and cutting-edge in its handling of stolen data. The website required users to pay a registration fee to create a shopping account. Once an account was created, the user could search databases of stolen account data in a variety of ways, including by bank identification number, financial institution, country, state, and card network (such as Visa, MasterCard, and American Express). In this way, the user could tailor his search of stolen account data to suit his specific criminal purpose. To purchase the stolen account data, the user could simply add the stolen account to his cart and, upon checkout, pay for the stolen account data with funds associated with his user profile. The user would then receive the stolen account data via a webpage or via an email generated at the end of the transaction.

To create and maintain the Codeshop website, the defendant enlisted the assistance of other criminals and experts online. Email communications revealed that, on or about March 7, 2011, the defendant communicated with the administrator of another carding site—Freshshop—and inquired: "Hey, Im Intersted about the webshop script to buy . . . .," effectively inquiring about purchasing the computer code (or "script") necessary to run a carding website. After creating the Codeshop website, the defendant advertised it by email to other carders: on or about April 9, 2011, the defendant sent an email to a supplier of stolen data announcing "IMPORTANT NEW ONLINE CC WEBSHOP" and directing the recipient to the "codeshop.su" website. The defendant sent a follow-up message specifying that the Codeshop website contained "canadian cvvs," "USA Fulls," and "usa cvvs"—references to credit card data stolen from U.S. and Canadian victims. After running the Codeshop website for some time, the defendant engaged in a redesign: in or about May 2012, the defendant communicated with co-conspirator "elance.web.temple" about the design of the Codeshop website. The defendant asked when the computer code for the site would be ready. The co-conspirator "elance.web.temple" responded: "New design is attached. If you want to proceed

[1] The government incorporates by reference the facts set forth in its initial Complaint in this matter and in the Probation Department's Presentence Investigation Report ("PSR").

with multiple bins search mod[e], please, make a payment to my LR [Liberty Reserve] account." The co-conspirator's message contained an attachment ("codeshop-design.tgz") containing a complete draft of the template and scripts associated with the Codeshop website.

To supply the Codeshop website with stolen credit card and account data, the defendant enlisted the services of criminal hackers and fraudsters. There were two primary means of theft. First, the defendant enlisted his co-conspirators to hack into the computer databases of financial institutions and other businesses, including businesses in the United States. Computer forensic evidence obtained during the investigation revealed that the defendant and his co-conspirators stored various hacking tools on the servers associated with their operation and communicated about the use of those tools. For example, one server contained a SQL-injection, a type of malicious software used to extract backend credit card databases from online merchant websites that accept credit card payment. The servers also contained the results of successful hacks, including multiple "data dumps" containing the credit card information of victims around the world, as well as other personal identifying information obtained through hacking, including copies of U.S. passports and driver's licenses.

Second, the defendant enlisted his co-conspirators to conduct "phishing" scams wherein the conspirators sent forged emails to unwitting accountholders that fraudulently induced the accountholders to surrender private information. Computer forensic evidence obtained during the investigation revealed that the defendant and his co-conspirators saved copies of their phishing emails on the servers associated with their operation. For example, one server contained a copy of a phishing email purporting to be from the U.S. payment processor PayPal and targeting German users of PayPal.

The defendant relied on these and other individuals for additional administrative tasks related to the stolen account data, including the registration of servers and domains in various locations around the world and the packaging the stolen data by formatting it to conform to the layout of the Codeshop database. For example, on or about May 11, 2011, the defendant received an email from "applelover138" with an attachment containing approximately 100 stolen Visa and Mastercard accounts. On or about June 20, 2011, the defendant received an email from "swpower" with two attachments ("AMEX.txt" and "MC.txt") containing approximately 980 stolen American Express Accounts and 945 stolen Mastercard accounts, in a format that included primary account number, expiration date, CVV code, account holder name, and account holder address. On or about Mary 27, 2013, the defendant received an email from "swpower" with an attachment ("BANKS.txt") containing approximately 20 compromised bank accounts, in a format that included financial institution, account value, URL for account access, and account holder username and password.

The defendant also communicated with the criminal customers of his website. Email communications revealed that the defendant's Codeshop12 email account had more than 16,000 messages in it between April 2011 and July 2013, the majority of which represented communications between the defendant and the users of the Codeshop website.

Throughout the duration of the scheme, the defendant used multiple aliases to hide himself during his operations, including "codeshop," "sindrom," "sindromx," "xhevo," and "xhevoking," and maintained more than a dozen email accounts to diversify his methods of communication. The defendant and his co-conspirators communicated about the scheme and payments from the scheme via encrypted applications like Viber and Jabber.

Viber conversations captured on the cellphone of co-conspirator "swpower" reveal the defendant managing his co-conspirators: instructing "swpower" to format the stolen account data in a certain way ("go to manage card and there is the format"); regularly checking in how many cards have been added ("how much have you placed[?] . . . only that[?]"; "how much did you add"; "did you do 25k or nothing . . . whats up with you"); enlisting "swpower" to engage in hacking and phishing to bring additional supply to the scheme (defendant complaining "you don't even try to find stuff any longer . . . I have a guy who has shells"; defendant instructing "swpower" to "hack this and then we will truly get millions"; "swpower" stating that he "started to hack sites again . . . that something big will fall" and the defendant responding "I hope that it will"; the defendant giving direction to "see what is he phishing and make . . . it is easy to make that shit"; the defendant, in reference to phishing, "do you think you could do that . . . so if you think that you can why don't you"); and coordinating the co-conspirators ("see with ryan on that government site where there were big transactions"; "have ryan make it and we will pay him"; "talk to him [gzero] so that he will decrypt . . . tell him that he will get big money"). Jabber communications captured on the scheme's servers reveal discussions about payment. In one Jabber communication, the defendant's co-conspirator lists how many valid cards he and another supplier of stolen credit card data provided and indicates the amount of money the defendant needed to distribute to the two suppliers. In another Jabber communication, two of the defendant's co-conspirators discuss the distribution of proceeds from the scheme and note that the defendant "is admin, and admins take 50%" while the other two (who are data suppliers) receive only 25%.

The defendant directed monetary transactions related to the scheme through anonymous and digital online currencies, such as Bitcoin, Webmoney, Perfect Money, and Liberty Reserve, that served to further conceal the participants' identities, including his own.

As part of the investigation in this case, law enforcement agents seized various servers associated with the operation of the Codeshop website, some of which were located in the Netherlands and the Czech Republic. One of the seized servers was the server that hosted the Codeshop website itself. A forensic analysis of the server revealed that the server contained a database of stolen credit card data, which was the data being sold on the Codeshop website. The seized copy of the Codeshop server preserved a snapshot of this database at the time of seizure. The forensic analysis of the server revealed that a counter function on the database that recorded the number of entries that had been made over the lifetime of the server indicated that the database had contained more than 1.3 million stolen credit cards over its lifetime. The forensic analysis also revealed that, at the time of seizure, the database contained more than 400,000 stolen credit cards still preserved on the server—including, data entries with the card number and expiration date, the name and address of the true cardholder, and the date that the credit card had been added to the database.

The forensic analysis further revealed that there were more than 28,000 criminal users registered with the Codeshop website, logging in with email addresses and IP addresses associated with locations around the world. Finally, the forensic analysis revealed that there were four individuals with uploading privileges to the database: "nora," an alias for Eleanora, the defendant's co-conspirator and girlfriend; "ink," an alias for Edward Pearson, the defendant's co-conspirator; "swpower," an alias for Blaz Mijic, the defendant's co-conspirator; and "Admin," the defendant himself.

The defendant remained beyond the reach of U.S. law enforcement for a significant period of time due to his residency in Macedonia. However, through the extraordinary efforts of the United States Secret Service, working with foreign law enforcement officials in Slovenia, U.S. law enforcement authorities received information that the defendant would be traveling through Slovenia and rapidly coordinated an international arrest. The defendant was arrested in Ljubljana, Slovenia, on January 23, 2014. After fighting extradition for more than two years, the defendant was ultimately extradited from Slovenia to the United States on May 20, 2016.

On August 25, 2017, the defendant pled guilty, pursuant to a plea agreement, before United States Magistrate Judge Steven Tiscione to one count of access device fraud, in violation of 18 U.S.C. § 1029(a)(5), and one count of aggravated identity theft, in violation of 18 U.S.C. § 1029A(1)(A). On September 8, 2017, this Court accepted the defendant's guilty plea.

II. Legal Standard

In the Supreme Court's opinion in United States v. Booker, 125 S. Ct. 38, 743 (2005), which held that the Guidelines are advisory and not mandatory, the Court made clear that district courts are still "require[d] . . . to consider Guidelines ranges" in determining a sentence, but also may tailor the sentence in light of other statutory concerns. See 18 U.S.C. § 3553(a). Subsequent to Booker, the Second Circuit held that "sentencing judges remain under a duty with respect to the Guidelines . . . to 'consider' them, along with the other factors listed in section 3553(a)." United States v. Crosby, 397 F.3d 103, 111 (2d Cir. 2005).

In Gall v. United States, 128 S. Ct. 586 (2007), the Supreme Court elucidated the proper procedure and order of consideration for sentencing courts to follow: "[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, 128 S. Ct. at 596 (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 so doing, [the district court] may not presume that the Guidelines range is reasonable. [It] must make an individualized assessment based on the facts presented." Id. at 596-97 (citation and footnote omitted).

Section 3553(a) requires a court to consider a number of factors in imposing a sentence, including: the nature and circumstances of the violation and the history and characteristics of the defendant (§ 3553(a)(1)); the need for the sentence to reflect the seriousness of the violation, to promote respect for the law, and to provide a just punishment for the violation (§ 3553(a)(2)(A))); the need for the sentence to afford adequate deterrence to criminal conduct (§ 3553(a)(2)(B)); to protect the public from further crimes or violations of the defendant (§ 3553(a)(2)(C)); and to provide the defendant with needed education or vocational training, medical care or other correctional treatment in the most effective manner (§ 3553(a)(2)(B)). The court must also consider the kinds of sentences available (§ 3553(a)(3)), the applicable sentencing guideline and pertinent policy statements (§ 3553(a)(4)(B) and § 3553(a)(5)), and the need to avoid unwarranted sentencing disparities (§ 3553(a)(6)).

III. **The United States Sentencing Guidelines**

The government agrees with the Guidelines calculation set forth in the PSR, which initially results in an advisory Guidelines range of life imprisonment, but thereafter defaults to the statutory maximum of 204 months' imprisonment.

A. The Defendant Stipulated to the Effective Applicable Guidelines Range

The defendant has stipulated to the effective applicable Guidelines range of 204 months. See Plea Agreement, ¶ 2. He nevertheless lodges various objections to the Guidelines calculation in advance of sentencing. The defendant does not specify his desired re-calculation of the Guidelines or whether he intends to breach the plea agreement. As the government explains below, the defendant's objections contradict the plain evidence in the case and, even if the Court were to accept various lower estimates of access devices at issue, the resulting loss enhancement would leave intact the final effective applicable Guidelines range of 204 months. This is because the nature and extent of the defendant's criminal conduct is so wide-ranging that, in any scenario supported by the evidence, the advisory Guidelines range would far exceed the statutory maximum in this case. The statutory maximum (of 204 months) therefore becomes the effective applicable Guidelines range. See U.S.S.G. § 5G1.1-5G1.2.

B. The Defendant's Objections to the Guidelines are Without Merit

The defendant's objections to the Guidelines calculation are without merit and are merely an attempt to minimize his conduct.

First, the defendant disputes the number of cards that were trafficked on the Codeshop website. As explained above, law enforcement agents seized the Codeshop server, which indicated that more than 1.3 million stolen credit cards had been uploaded to the

Codeshop website over its lifetime. The defendant's retained expert confirmed that the last row of the database has a line ID of 1,374,664, consistent with the data from the database's counter. The defendant's retained experts does not comment on the validity of the overall counter. The loss enhancement that results from the more than 1.3 million stolen credit cards uploaded to the Codeshop website over its lifetime is +30, consistent with the Probation Department's calculation.

Moreover, the seized copy of the server preserved for posterity the stolen credit cards that were being offered on the Codeshop website at the time of the takedown—more than 400,000—and the Court can see for itself the numerous individual victims in the United States and around the world whose financial and personal data the defendant was offering up for sale. The defendant's retained expert agrees that there are more than 400,000 distinct rows in the preserved copy of the database. The loss enhancement that results if one accounts only for the 400,000 stolen credit cards in the preserved copy of the database is +26.

The defendant attempts to minimize the number of cards further by claiming that, although he offered more than 400,000 stolen credit cards for sale on his website, he refunded customers for cards that were expired or otherwise defunct, and those refunded cards should be subtracted from the total, bringing the number of credit cards down to approximately 164,000. However, that is a step too far. The law holds the defendant responsible for the full extent of the access devices that he trafficked and attempted to traffic, regardless of whether those devices were expired, revoked, or canceled. See 18 U.S.C. § 1029(e)(3).

Therefore, the evidence overwhelmingly establishes that the defendant trafficked in so many access devices that the resulting loss enhancement would render an advisory Guidelines range that exceeds the statutory maximum in this case.

Second, the defendant disputes the enhancement for being a leader and organizer of the offense. The Guidelines provide that the four-point enhancement applies if the defendant was "an organizer or leader of a criminal activity of five or more participants or was otherwise extensive." U.S.S.G. § 3B1.1(c). The evidence established that the defendant was an organizer and leader of the criminal activity. The defendant obtained the code to build the Codeshop website; he received a bigger share of the proceeds from the Codeshop website than his co-conspirators; and he was the "Admin" of the website. From beginning to end, the defendant was the mastermind of the Codeshop operation, whereas he recruited other co-conspirators to provide component parts and services (such as website design, formatting, and obtaining stolen credit card information through computer intrusions and other means).

The evidence also showed that the criminal activity was "extensive" within the meaning of U.S.S.G. § 3B1.1(a). As an initial matter, there were at least four other participants in the conspiracy: "swpower" (Blaz Mijic); "Gzer0" (Edward Pearson); "ryan" (Julius Kiwimaki); "f0x" (Ionut Radoui); "off-sho.re" (FNU LNU); "k!ngs0pe" (FNU LNU);

"elance.web.temple"; and "applelover138.". Moreover, in determining whether a criminal activity is "extensive," the Court's consideration is not limited to the size of the criminal organization itself. Rather, "all persons involved during the course of the offense are to be considered. Thus, a fraud that involved only three participants but used the unknowing services of many outsiders could be considered extensive." The Codeshop website served as a hub for the criminal activity of a large number of people, even if only a handful of them worked directly with the defendant. U.S.S.G. § 3B1.1(a) cmt. 3. Indeed, the Codeshop database showed that the defendant sold stolen credit card data to more than 28,000 criminal customers, from whom the defendant profited. The defendant also used numerous other services (both criminal and legitimate) to facilitate his criminal enterprise, including the individual who first provided him with the computer code to build the website (the Freshshop administrator), server providers, and online currency services. By any measure, the criminal activity was extensive, and coupled with the defendant's role as organizer or leader, this supports a four-level aggravated role adjustment.

The defendant's remaining objections to the PSR's descriptions of his offense conduct are refuted by the facts set forth above.

C. The Defendant's Arguments Regarding the Guidelines are Unavailing

In addition to his objections to the Guidelines calculation, the defendant makes various arguments criticizing the Guidelines themselves. These arguments are equally unavailing.

First, the defendant argues that the Second Circuit and courts in the Eastern and Southern Districts of New York have criticized the application of a significant loss enhancement and encouraged the consideration of a non-Guidelines sentence where the Guidelines assign "a rather low base offense level to a crime and then increase[] it significantly by a loss enhancement." United States v. Algahaim, 842 F.3d 796, 800 (2d Cir. 2016). However, the defendant's argument is misplaced in this case. First, as an initial matter, it is important to note that the statutory maximum in this case already significantly resets the final Guidelines range to a number far lower than it would otherwise be, effectively eliminating a portion of the loss enhancement. Second, the concerns expressed by the judges the defendant cites refer to select circumstances where the loss amount does not correlate to the extent of actual victimization. See Algahaim, 842 F.3d at 798 (food stamp fraud defendants' loss enhancements based on amount of cash defendants exchanged with confidential informant and customer in return for benefits); United States v. Corsey, 723 F.3d 366, 368 (2d Cir. 2013) (wire fraud defendant's loss enhancement based on "conspiracy to defraud a non-existent investor of three billion dollars"); United States v. Gupta, 904 F. Supp. 2d 349, 350 (S.D.N.Y. 2012) (securities fraud defendant's loss enhancement based on unpredictable monetary gains made by others); United States v. Emmenegger, 329 F. Supp. 2d 416, 427 (S.D.N.Y. 2004) (securities fraud defendant's loss enhancement based on "a kind of accident" related to a single victim's security procedures); United States v. Adelson, 441 F. Supp. 2d 506, 509 (S.D.N.Y. 2006) (securities fraud defendant's loss enhancement based on decline in stock price multiplied by millions of outstanding shares); United States v.

Johnson, No. 16-CR-457, 2018 WL 1997975, at *3 (E.D.N.Y. Apr. 27, 2018) (wire fraud defendant's loss enhancement based on gain from fraudulent trades).

Those same concerns—of loss being untethered to concrete victimization—do not pertain to this case. The loss enhancement in this case is based on a special rule of thumb intended to assist district courts in estimating actual and intended losses in access device fraud cases, and the rule is specifically keyed to victimization. The special rule provides that "[i]n a case involving any . . . unauthorized access device, loss includes any unauthorized charges made with the . . . unauthorized access device and shall be not less than $500 per access device." U.S.S.G. § 2B1.1, Application Note 4(F)(i). The Second Circuit has affirmed the application of this special rule as appropriate. See United States v. Volynskiy, 431 F. App'x 8, 9-10 (2d Cir. 2011) (summary order); United States v. Dodson, 357 F. App'x 324, 325-26 (2d Cir. 2009) (summary order). None of the cases the defendant cites in support of his argument address it.

As the Sentencing Commission has explained, the special rule's $500 per access device is a conservative estimate of loss—"a floor, not a ceiling." See United States Sentencing Commission, Primer on Loss Calculations under § 2B1.1(b)(1), at 20-21 (June 2016). A more fulsome estimate of intended loss would aggregate the total amount of the credit limit of all stolen credit cards. See id.; see also, e.g., United States v. Alli, 444 F.3d 34, 37-39 (2006) (affirming application of loss enhancement calculated by adding together the credit limits of the stolen credit cards); United States v. Mohammed, 315 F. Supp. 2d 354, 358-61 (S.D.N.Y. 2003) (Lynch, J.) (same). Neither the government nor the Probation Department have taken that more hefty approach here; instead, we have applied the more conservative estimate of loss provided for by the Guidelines' special rule. The loss enhancement in this case remains significant despite the application of this conservative estimate for one simple reason—because the defendant stole, possessed, and offered for sale so many stolen credit cards in the first place, from so many individuals and businesses around the world—and not because of any flaw in the Guidelines.

Indeed, this conservative estimate of loss is remarkable for its restraint. As Judge Lynch noted in a similar case, such loss number make no "pretense of measuring the actual harm inflicted by this crime, including the damage actually or potentially inflicted on the reputations and credit ratings of the affected individual victims; the time, effort and expense incurred by those individuals and the credit agencies involved to unravel the false information created by the conspirators; or the damage done to the trust essential to commercial relationships in an economy in which credit plays such a large part. No simple calculation of dollar 'loss' will adequately measure the seriousness of this crime." Mohammed, 315 F. Supp. 2d at 358.

Second, the defendant argues that courts regularly impose below-Guidelines sentences in fraud cases and that giving the defendant a Guidelines sentence here would be out of line with other fraud sentences. Importantly, none of the cases the defendant cites involve credit card hacking schemes, and the driving concern behind many of these sentences (that the "intended loss" is untethered) does not apply here. The government sets forth below (infra Part IV.E) several examples of cases that more closely reflect the nature of the defendant's scheme. As discussed more fully below, these examples illustrate that imposing a sentence of 204 months' imprisonment would be within the contours of sentences imposed in other credit card hacking schemes and not create unwarranted sentencing disparities.

Third, the defendant argues that his conduct caused no harm to individual victims and no loss to financial institutions. This is patently false. The theft and resale of credit card data and other account information compromises the identity and security of individuals and shakes their confidence in the financial systems that they must rely on to operate in the modern world.[2] The financial institutions that commonly reimburse these victims suffer financial losses. The government is continuing to engage with these financial institutions in order to obtain final loss numbers for purposes of restitution—a process that is complicated by the fact that the defendant's scheme victimized multiple different card issuers and networks scattered across the country and the world. It is important to note for purposes of this argument, however, that those losses are non-zero. For example, one U.S.-based credit card network recently reported losses exceeding $29 million in connection with accounts compromised by the defendant's scheme.

Fourth, the defendant argues that the Guidelines enhancement for committing a substantial part of the scheme outside the United States "falls squarely outside the spirit of this provision" because it is only warranted where the defendant "uses a foreign jurisdiction as part of the scheme as a sophisticated concealment effort to evade law enforcement or regulatory officials." In making this argument, the defendant conflates two separate, and alternative, bases for satisfying the enhancement. See U.S.S.G. § 2B1.1(b)(10)(A)-(B). Committing the scheme from outside of the United States is, alone, an important and sufficient basis to honor the enhancement because when a foreign cybercriminal chooses to target U.S. individuals, computers, and companies for victimization, he is doing so with the advantage of knowing that his location abroad makes it more difficult for him to be caught. In any event, the facts support the application of this enhancement on the other, alternative, prongs set forth in the enhancement—the facts in this case show that the defendant relocated part of the scheme to evade law enforcement. As explained above, the defendant and his co-conspirators rented servers for their operation in locations where they did not live to perpetuate the scheme. By using these foreign servers to store hacking tools and data dumps, rather than storing all of that information on their home computers, the defendant and his co-conspirators obfuscated their true location. The offense also involved sophisticated means.

Fifth, the defendant argues that the Guidelines enhancement that is applied because the offense involves access devices amounts to double-counting. However, the Second Circuit has stated that "double counting is legitimate where a single act is relevant to two dimensions of the Guidelines analysis." United States v. Jackson, 346 F.3d 22, 25 (2d

[2] The government encloses herewith victim impact statements from one of the companies that was breached and five individual cardholders whose data was stolen.

Cir. 2003). Here, the loss amount calculation accounts for the credit card data that the defendant trafficked, while the access device enhancement accounts for the other information—bank account credentials and personally identifiable information—that the defendant trafficked.

Sixth, the defendant argues, without any basis in the evidence, that one of his co-conspirators was "the brains behind Codeshop." These self-serving statements in advance of sentencing are unsupported and, furthermore, belied by the extensive evidence produced in this case. As explained above, the evidence demonstrates that the defendant started the Codeshop website and was the organizer and manager of the site. His co-conspirators performed functions to facilitate the operation of the Codeshop website, including hacking, phishing, and formatting of data, but those individuals were merely spokes of the wheel—the defendant was the hub, coordinating all of the pieces and creating the online platform that drove the criminal scheme.

IV. **The Section 3553(a) Factors**

The government respectfully requests that the Court impose the statutory maximum sentence of 204 months' imprisonment—which already represents a significant downward revision from what would otherwise be the advisory Guidelines range—and respectfully submits that such a sentence would appropriately reflect the sentencing factors set forth in 18 U.S.C. § 3553(a).

A. The Nature and Circumstances of the Offense

A sentence of 204 months' imprisonment would reflect the serious, sophisticated, and wide-reaching nature of the defendant's criminal enterprise.

The defendant's conduct was serious and long-running. He developed a criminal enterprise that was illegal on its face and made no pretense of legitimacy: the Codeshop website was wholly dedicated to the sale of stolen credit card and account data, and it was one of the most sophisticated carding marketplaces available online. The seriousness of the defendant's operation is particularly acute because, unlike more mundane and traditional schemes involving one-off fraud or street-level identity theft, the defendant used the power of the internet to magnify the effectiveness of his enterprise, manage hackers and co-conspirators in different countries, attack individuals and businesses from afar, steal massive volumes of personal data in minutes, and sell that data to a global network of criminals.

The defendant engaged in careful and sophisticated preparation and planning to operate the marketplace: email communications show that the defendant reached out to other carding website operators for the computer code necessary to build the Codeshop website, and computer forensic evidence shows that the defendant and his co-conspirators set up an infrastructure of computers and servers around the world to hold the hacking tools and data necessary to run the website and supply it with stolen data. The defendant further took measures to protect his and his co-conspirators' identities and evade detection: the defendant obfuscated his and his co-conspirators' true locations by running the Codeshop website from servers located around the world; he used numerous aliases, fake names, and alternative email accounts to conduct his criminal activities; he used encrypted applications to communicate with his co-conspirators; and he used anonymous and digital currencies to conduct monetary transactions related to the scheme.

The defendant's efforts fueled widespread criminal activity: in order to supply the Codeshop website with stolen data, the defendant and his co-conspirators hacked and phished a multitude of individuals and businesses around the world. This behavior was particularly predatory where they targeted small businesses generally less equipped to defend against such attacks. Overall, the defendant compromised the identities and financial data of more than 1.3 million individuals around the world; and after supplying that data on the Codeshop marketplace, the defendant enabled more than 28,000 criminals to further misappropriate, purchase, and profit from that stolen data.

B. The Defendant's History and Characteristics

A sentence of 204 months' imprisonment would also account for the defendant's history and characteristics.

The defendant's involvement in the online trafficking of stolen credit card data shows that his interest was not one-off or transient—it lasted for years. Email communications show that he began engaging in such activity since at least as far back as 2010, a year before he registered the Codeshop website. In August 2010, the defendant received approximately 200 stolen Wells Fargo Visa accounts by email from "thebourne9." He was also active on other carding sites, like L33t—an email message on or about July 14, 2012, reveals the defendant inquiring about his user account on the L33t carding site. The defendant then operated the Codeshop website for more than three years, from 2011 to 2014. This long-running pattern of conduct reflects an individual with an unflinching willingness to steal from others. Although the defendant has no official prior criminal history in the United States, he is a long-time cybercriminal who acted with impunity until this prosecution.

Once apprehended in 2014, the defendant did not seek to accept responsibility or resolve his U.S. charges right away, but rather chose to stay in foreign custody and fight extradition for approximately two years.

Given the defendant's background, he also poses a high risk of recidivism. Once he has served his prison sentence in the United States, he will return to Macedonia, where post-release supervision will be completely absent and he will once again be beyond the reach of U.S. law enforcement. His demonstrated abilities to obtain tools and advice from online sources, recruit hackers and co-conspirators to his cause, and build complex digital infrastructures to commit cybercrime will once again have free reign. It is important that the sentence imposed shows the defendant that the costs of engaging in these crimes significantly outweigh the benefits that he enjoyed for so many years.

C. The Need for the Sentence Imposed to Reflect the Seriousness of the Violation, to Promote Respect for the Law, and to Provide a Just Punishment

A sentence of 204 months' imprisonment is necessary to reflect the seriousness of the violation, promote respect for the law, and provide just punishment.

The defendant's criminal enterprise undermines the innovation and advancements that make up the modern U.S. economy. Computers, the internet, and electronic information storage are an integral part of the U.S. economy. Consumers and businesses alike transmit and store ever increasing quantities of private information and financial data over the internet every day. The expansion of the internet and computer networks has brought great benefits to the economy and opened up new opportunities for millions of people. Unfortunately, this digital revolution has also created new and unprecedented opportunities for criminals to steal and traffic in information and money on a scale and at speeds that were impossible in the physical world. The internet has opened a new frontier for criminals unbounded by traditional mores or physical barriers. Cybercriminals like the defendant can commit their crimes from around the world without ever facing their victims face-to-face, and can use any number of techniques to conceal their identities.

Carding site operators, in particular, maximize their profits by quickly and efficiently bringing their stolen goods to market before banks have an opportunity to shut down the stolen credit cards. The defendant built and operated an easy-to-use searchable website that facilitated these rapid and profitable sales and, in doing so, he helped to create a sustainable market for more than a million stolen credit cards causing untold damage to individuals, banks, and businesses. Yet, the damage that the defendant was capable of causing in just hours takes victims and law enforcement months, and sometimes years, to understand, analyze, and successfully investigate and prosecute.

Online theft and trafficking of credit card data, banking credentials, and personally identifying information, in the nature of what the defendant committed, presents a serious threat to the viability of businesses and financial institutions all over the world, as well as to the security of their customers' private financial data. Such crimes undermine consumer confidence and trust in the systems and networks necessary for the healthy operations of businesses in the modern world. Those who would commit such crimes should be put on notice that the rule of law applies in cyberspace just as it does on the street, and they will face substantial prison sentences that are commensurate with the losses and damages they cause.

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

A sentence of 204 months' imprisonment is also necessary to afford adequate general deterrence and protect the public specifically from further crimes of the defendant.

As the circumstances of this case demonstrate, it is all too easy for cybercriminals to profit from cybercrime schemes. Cybercriminals like the defendant can make millions of dollars in a very short time period hacking computers and stealing personal financial records. The lure of such easy money in countries with spotty records of cooperating with U.S. law enforcement is substantial. Many may make the calculation that the rewards are worth the risk when their government is unlikely to extradite them to face justice in the United States. As explained above, the defendant himself will return to a realm of impunity once he is released from incarceration. After he is back in his home country, he will once again have access to the computer and criminal networks that enabled him to build his cybercriminal enterprise in the first place.

At the same time, it is all too difficult for law enforcement to identify and capture international cybercriminals like the defendant. Cybercrimes are extremely difficult to solve. Identifying the mastermind behind the keyboard takes unique investigative expertise and attention to detail. The investigations almost universally require the collection of evidence from sources all over the world. Electronic evidence often disappears before the legal and diplomatic procedures necessary to retrieve the evidence can be completed. Even when law enforcement can successfully identify a cybercriminal, many hackers reside in countries that will not extradite their citizens to face justice in the United States even where their crimes have victimized U.S. individuals and businesses.

In the rare instances in which the United States can bring a cybercriminal of the defendant's stature and significance to justice, the sentence must be significant to afford adequate general and specific deterrence. A statutory maximum sentence will unequivocally convey the message that U.S. courts will not tolerate the victimization of U.S. individuals and businesses by cybercriminals hiding abroad.

E. The Need to Avoid Unwarranted Sentencing Disparities

A sentence of 204 months' imprisonment would avoid unwarranted sentencing disparities among defendants with similar records who have been found guilty of similar conduct.[3]

[3] The government refers to the cases discussed in this subsection to inform the Court of other prosecutions that are pertinent to the issues of sentencing disparity. However, the government is mindful that each defendant was sentenced on the unique facts of his case and that aggravating or mitigating circumstances in one case may not be present in others.

U.S. prosecutions of international carding website operators are relatively rare, given the difficulties in identifying and apprehending such individuals. However, there are several cases in this district and others that demonstrate that in those select instances when U.S. law enforcement successfully apprehends and convicts such cybercriminals, a severe sentence is warranted.

In United States v. Roman Seleznev, No. 11-CR-070 (W. D. Wa. 2017), the Honorable Richard A. Jones sentenced Roman Seleznev to 27 years' imprisonment, following a jury trial. Seleznev operated the Carder.su website, where he trafficked in stolen credit card data, and had a laptop computer in his possession with approximately 1.7 million stolen credit cards. Seleznev was arrested in and extradited from the Maldives.

In United States v. Roman Vega, No. 07-CR-707 (E.D.N.Y. 2013), the Honorable Allyne R. Ross sentenced Roman Vega to 18 years' imprisonment, following a guilty plea and cooperation. Vega operated the CarderPlanet website, where he trafficked in stolen credit card data, and had a laptop computer in his possession with approximately 500,000 stolen credit cards. He was arrested in and extradited from Cyprus. Vega pled guilty in this district to a cooperation agreement and provided historical information regarding his co-conspirators; he later breached his cooperation agreement by moving to withdraw his plea and contradicting prior statements.

In United States v. Albert Gonzalez, No. 08-CR-10223 (D. Mass. 2010), the Honorable Patti B. Saris sentenced Albert Gonzalez to 20 years' imprisonment, following a guilty plea and failed cooperation. Gonzalez and his co-conspirators were involved in hacking schemes in which they stole approximately 7,000 credit cards from one company and 45 million credit cards from another. Gonzalez was arrested in the United States.

Vega and Gonzalez's efforts to cooperate with law enforcement contrast sharply with the defendant's conduct in this case, in which he fought extradition for more than two years and now seeks to minimize his conduct.

U.S. courts have also imposed significant sentences on lower-level individuals affiliated with carding, such as those individuals who are involved in the initial security compromise that enables them to obtain the credit card data of others, and those individuals who are involved in taking stolen data and using it to further steal a victim's identity and funds. See, e.g., United States v. David Camez, No. 2012-CR-004 (D. Nev. 2014) (purchaser and user of stolen credit cards and counterfeit identification documents sentenced to 20 years' imprisonment); United States v. Jonathan Oliveras, (E.D. Va. 2011) (user of stolen credit cards, who encoded stolen account information purchased online onto plastic cards and used it to buy gift cards, sentenced to 12 years' imprisonment); United States v. Tony Perez III, No. 11-CR-122 (E.D. Va. 2011) (seller of counterfeit credit cards encoded with stolen account information sentenced to 14 years' imprisonment); United States v. Juan Cardena, No. 10-CR-20501 (S.D. Fl. 2010) (individual who purchased stolen credit card information from one counterparty online and sold it to others, and found in possession of more than 26,000 stolen credit cards on his computer, sentenced to more than 10 years' imprisonment).

Unlike those defendants, the defendant in this case is not merely a street-level hacker or casher of stolen credit cards. He operated a global online marketplace that created the demand for such hacking, provided the supply for such theft, and hosted a platform that enabled these crimes to occur in rapid speed and on an international scale, and he is therefore deserving of a more severe sentence.

V. **Conclusion**

For the foregoing reasons, the government respectfully requests that the Court impose a cumulative sentence of 204 months' imprisonment—180 months' imprisonment on Count Two and 24 months' imprisonment on Count Three, to run consecutively—and respectfully submits that such a sentence would be sufficient, but not greater than necessary, to achieve the purposes set forth in 18 U.S.C. § 3553(a). The government further requests that the Court set a date 90 days after sentencing for the final determination of victim losses for purposes of restitution. See 18 U.S.C. § 3664(d)(5).

Respectfully submitted,

RICHARD P. DONOGHUE
United States Attorney

By: /s/
Saritha Komatireddy
David K. Kessler
Assistant U.S. Attorneys
(718) 254-7000