THE HONORABLE RICARDO S. MARTINEZ

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

| | |
|---|---|
| UNITED STATES OF AMERICA,<br>Plaintiff,<br><br>v.<br>FEDIR OLEKSIYOVYCH HLADYR,<br>Defendant. | NO. CR17-00276RSM<br><br>**SENTENCING MEMORANDUM OF THE UNITED STATES** |

The United States of America, by and through undersigned counsel, files this Memorandum in anticipation of the sentencing hearing in this matter. Sentencing is scheduled for April 16, 2021, to be held by videoconference with the defendant's consent.

## I. INTRODUCTION

Defendant Fedir Hladyr was a key member of the notorious hacking group commonly called "FIN7." FIN7 was one of the top cybersecurity threats for companies in the retail, restaurant, and hospitality industries and other such consumer-facing businesses that used point-of-sale terminals to process payment card transactions. For this reason, cybersecurity experts have described FIN7 as "one of the most prolific



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

financial threat groups of this decade."[1] The scope of the harm caused by FIN7 is staggering: FIN7 targeted and attacked hundreds of U.S. businesses, stole tens of millions of payment cards, and – by some estimates – caused over a billion dollars of damage.

Defendant Fedir Hladyr was a knowing and willing participant of FIN7. He appears before the Court after pleading guilty to one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer hacking. Defendant admits that he served as a high-level manager and systems administrator for FIN7. In that capacity, he played a central role in aggregating stolen payment card information, supervising FIN7's hackers, and maintaining the elaborate network of servers that FIN7 used to attack and control victims' computers.

For the reasons set forth below and in the government's related filing, the United States joins in the recommendation of the U.S. Probation Office and respectfully recommends that the Court impose a sentence of ***120 months***. The United States further requests the Court order restitution and forfeiture, as discussed below.

## II. FACTUAL BACKGROUND

### A. The FIN7 Criminal Enterprise

Cybercrime has evolved dramatically in the last decade.[2] What was once the province of lone wolf hackers, became a crowded space filled with financially motivated hacking crews led by charismatic hackers such as Roman Seleznev and David Schrooten, who were sentenced in this district to 27 and 14 years respectively. At the peak of their exploits, Seleznev and Schrooten were viewed as pioneers in their field, with Seleznev's crew gaining particular notoriety for selling information for millions of stolen payment cards. In the modern age of cybercrime, these early pioneers have been overtaken by the

[1] https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html (last checked 4/8/2021).

[2] *See generally* Jonathan Lusthaus, Industry of Anonymity: Inside the Business of Cybercrime (2018).



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

next wave of cybercriminals who have brought with them lessons learned from the startup explosion in the business world on how small firms can leverage technology to operate on a massive scale. As a result, rogue actors and loosely affiliated groups of hackers have now been surpassed by sophisticated cybercriminal enterprises that rely on specialization, division of labor, and cyclical malware development to take on the cybersecurity of major businesses.

No hacking group epitomizes the industrialization of cybercrime better than the FIN7 criminal enterprise. FIN7 has had over 70 members who were organized into discrete departments and teams. *See* Presentence Report ("PSR"), ¶12; Plea Agreement ("PA"), ¶9.b. One department developed a full suite of malware tools, while another department designed and sent phishing emails. Yet another department consisted of teams of hackers who surveilled and exploited victim companies that inadvertently had activated malware in the phishing emails. PSR, ¶12. FIN7 even used common project management software to direct workflow and to coordinate the efforts of its distributed workforce. PSR, ¶¶15, 28. This high level of sophistication and organization allowed FIN7 to continuously update not only its malware tools, but also its cutting-edge attack methodologies, in a manner that made FIN7 an increasingly formidable threat to even the most robust cybersecurity systems. As one cybersecurity company has explained, "FIN7 has demonstrated that they are highly adaptable, evading detection mechanisms while impacting a number of large US retail companies over an extended period of time."[3]

Since approximately September 2015, FIN7 has leveraged its workforce and its malware tools to relentlessly launch waves of attacks against hundreds of companies. PA, ¶9.b. FIN7's top-level leadership and managers (like Defendant Hladyr) made sure to extract value from every tool and employee at their disposal. Unable to match the sophistication and sheer manpower of FIN7, numerous restaurant chains, hotels, casinos,

[3] Footprints of FIN7: Pushing New Techniques to Evade Detection, https://www.icebrg.io/blog/old-dog-new-tricks-fin7-pushing-new-techniques-to-evade-detection (last checked 4/8/2021).



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

car dealerships, law firms, and many others, were breached by FIN7's teams of hackers. PSR, ¶8.

**B. Combi Security**

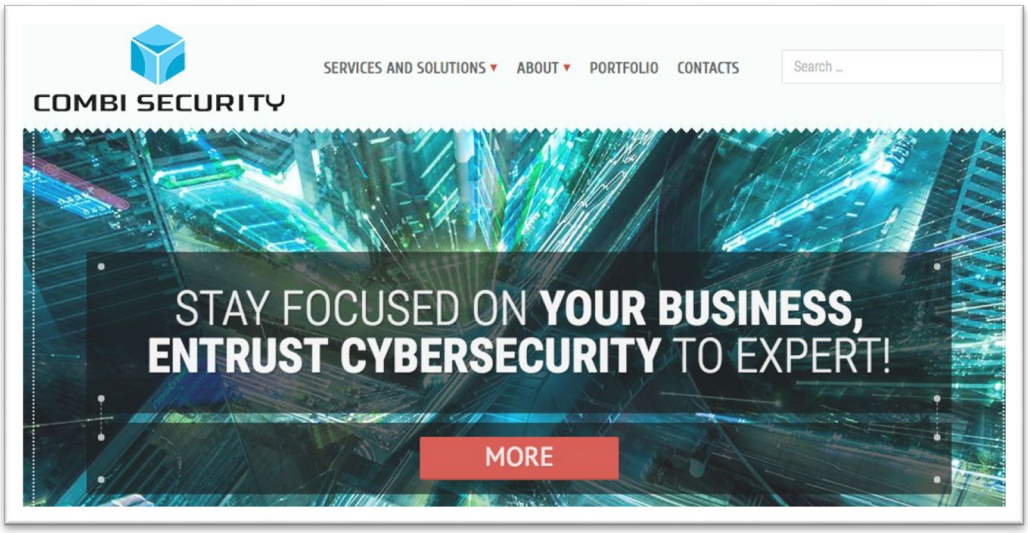
Not only did FIN7 imitate the practices of the business world, it also masqueraded as a legitimate company. Almost comically, FIN7 created a fake cybersecurity business called "Combi Security" to, among other things, recruit and provide low-level members with plausible deniability regarding their involvement in an international hacking scheme. PSR, ¶¶9-10. Technologically skilled individuals, such as Defendant Hladyr, were initially hired by Combi Security and may claim to believe that they thought they were joining a legitimate company. However, anyone performing any meaningful amount of work for Combi Security would have quickly realized that the company was actually a cybercriminal enterprise determined to exploit, rather than protect, the cybersecurity of its victims. *See* PA, ¶9.g.

For a brief period, FIN7 even maintained a public website for Combi Security. PSR, ¶10. The website, which itself exhibited the hallmarks of a sham, stated that the company provided cybersecurity services such as penetration testing:[4]

[4] Further confirming the readily apparent illegitimacy of Combi Security, the website became inactive during the scheme. Moreover, various points, FIN7 used different sham company names in a similar manner.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970




The website also claimed that:

- Combi Security was "one of the leading international companies in the field of information security";
- Combi Security had "a team of top professionals in the field of information security for all kinds of organizations working around the world."; and
- Combi Security's "main mission is to ensure the safety of your activities, minimizing the risk of information technologies. Each call to us for help, we consider very carefully on an individual basis . . ."

To add insult to injury, Combi Security's website included a "portfolio" of purported clients that had the logos of multiple victim companies. Needless to say, there is no evidence that Combi Security performed any legitimate work. PA, ¶9.c. And, surely, none of FIN7's victims hired Combi Security to "test" their security.

**C. FIN7's Attack Methodology**

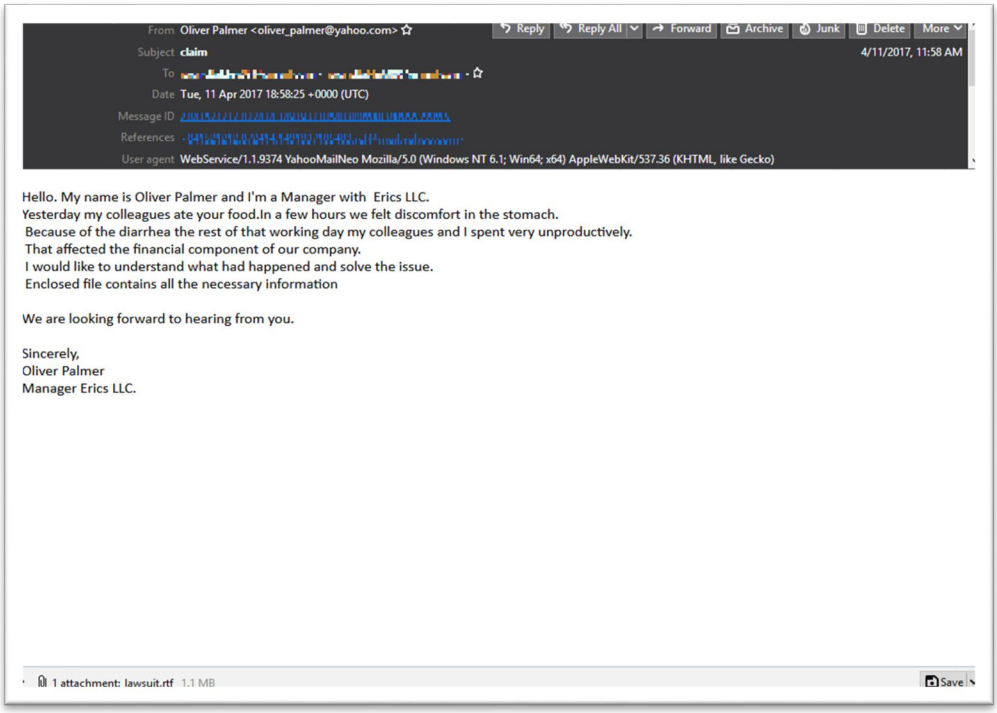
FIN7 typically attacked the weakest element of a company's cybersecurity – the human element. After conducting research on a target company, FIN7 would launch



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

tailored phishing email campaigns against employees of the target company.[5] PSR, ¶16. Although FIN7 has sent phishing emails to employees in a variety of roles, FIN7 is well-known for targeting customer service representatives with emails that exploit the representatives' desire to be responsive to their customers.

FIN7 used a wide variety of phishing emails, some of better quality than others. For example, FIN7 sent emails to restaurant managers, such as the following,[6] that complained about getting food poisoning and exploited public health and safety concerns:



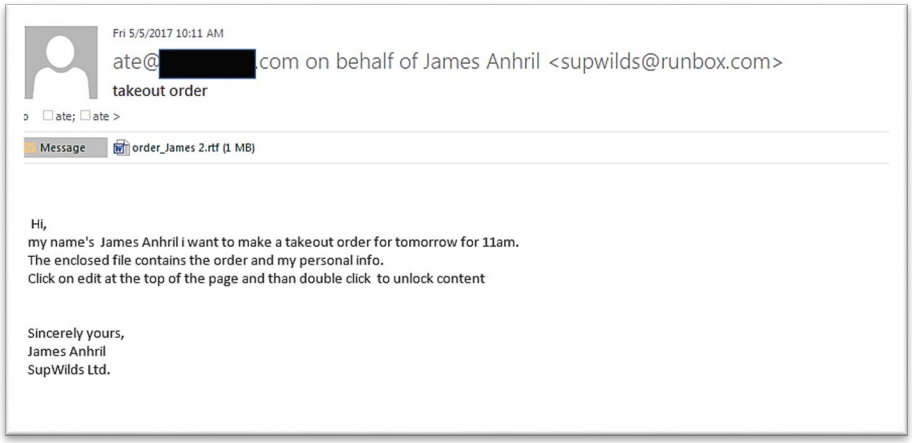

Other emails enticed the recipient to open an attachment purportedly containing a large order:

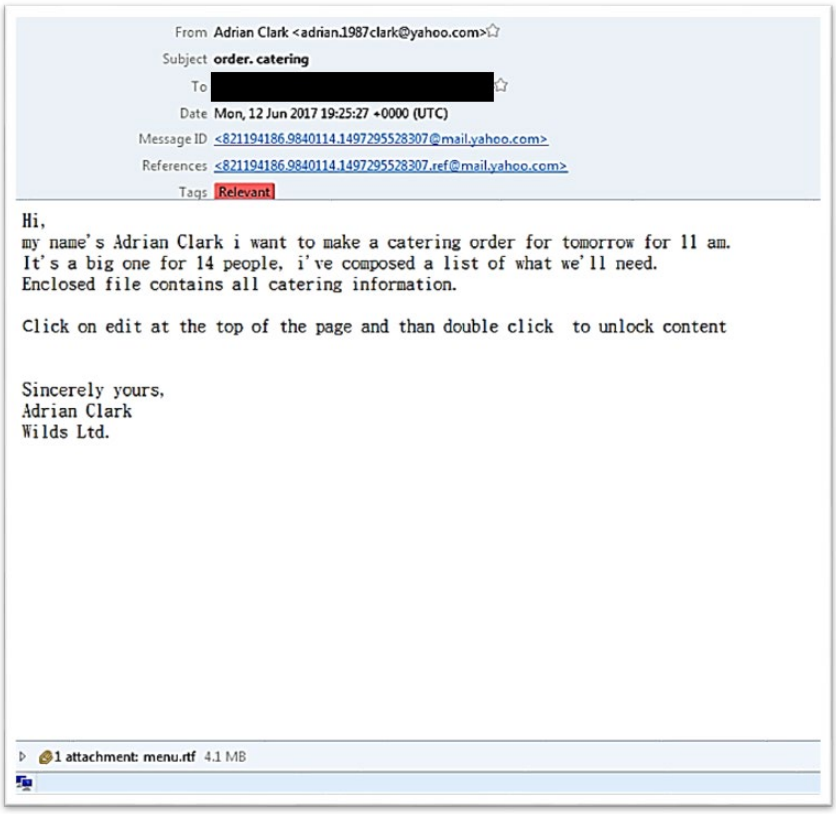
[5] *See generally* Operation Grand Mars: Defending Against Carbanak Cyber Attacks, https://www2.trustwave.com/Operation-Grand-Mars.html (last checked 4/8/2021).

[6] Victim information has been blurred or redacted in the examples contained in this memorandum.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



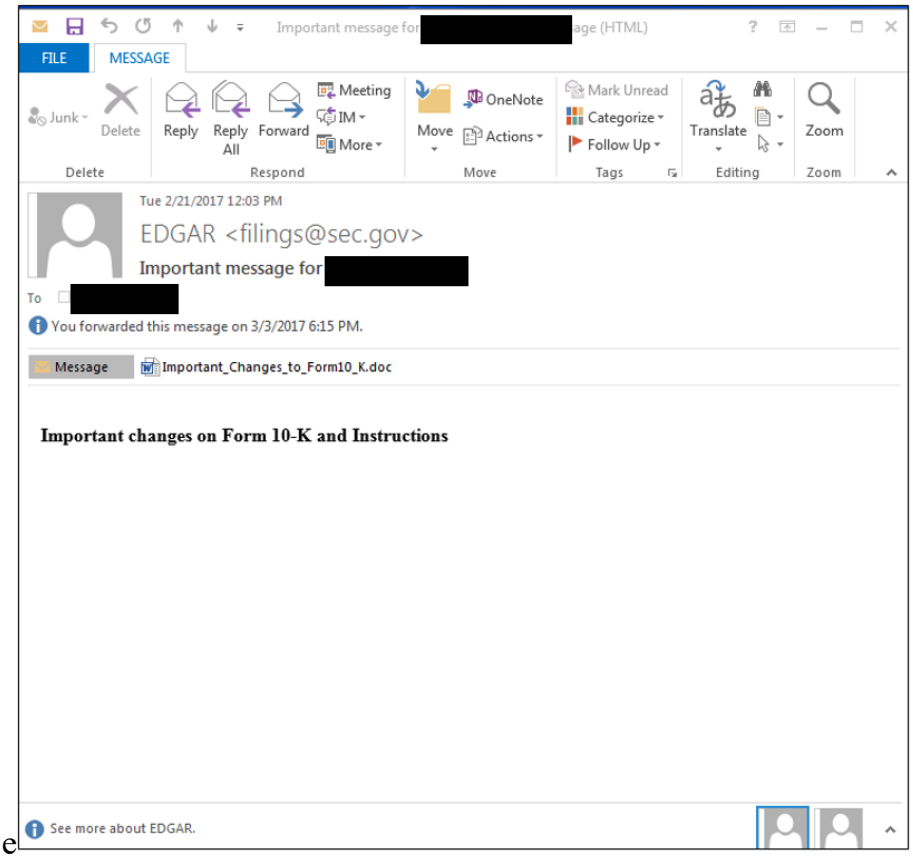




FIN7 also launched phishing attacks aimed at personnel at victim companies who had unique access to proprietary and non-public information. PSR, ¶18. For example, FIN7 targeted employees involved with preparing corporate filings with the United States Securities and Exchange Commission ("SEC"). *Id.* These emails used an email address that spoofed an address associated with the SEC's electronic filing system and induced



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the recipient to open an attachment to the email. The example below was delivered directly to an in-house corporate counsel of a publicly traded corporation, who was responsible for the company's securities filings:



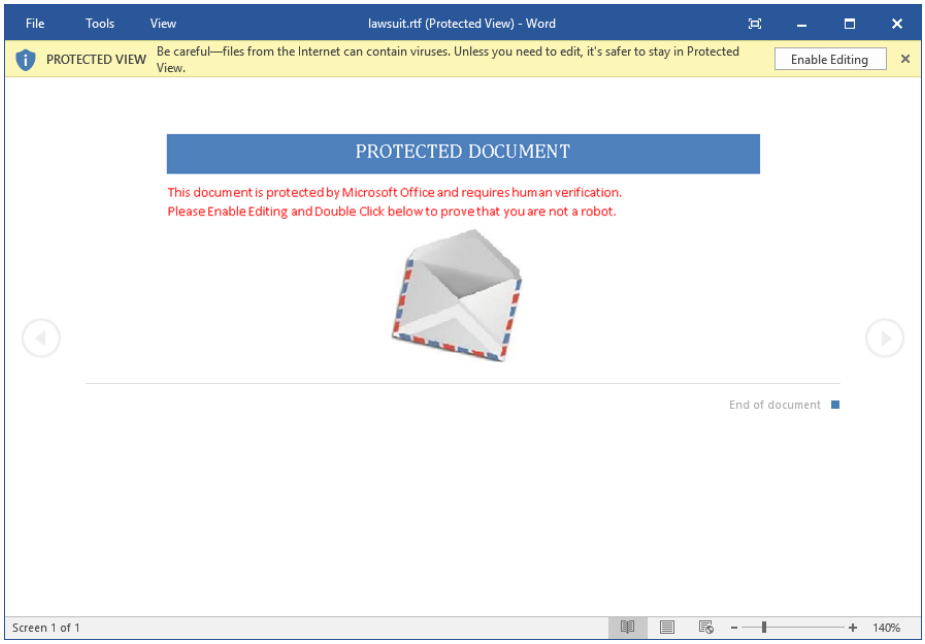

e

Induced by the seemingly legitimate email and the significance of the purported subject, the attorney unknowingly activated the malware and exposed the business' network to FIN7's hackers.

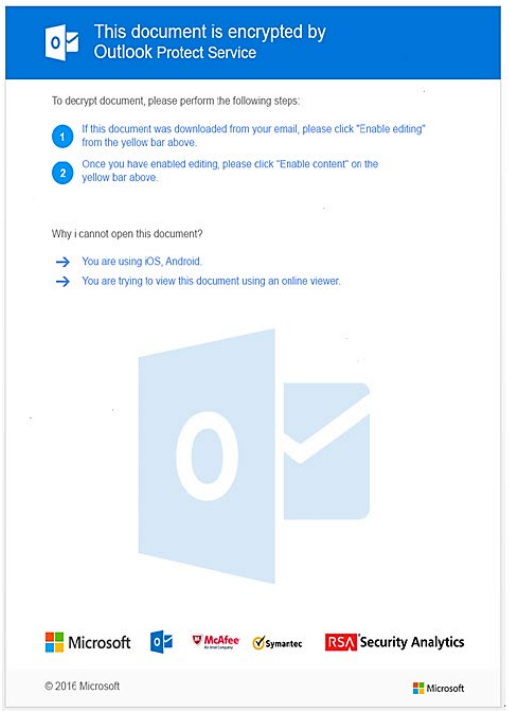
In many of the attacks, a FIN7 member, or someone hired by FIN7, also called the recipients of phishing emails and used social engineering techniques to encourage recipients to first read the emails and then open the email attachments in a manner that inadvertently activated malware embedded in the attachment. PA, ¶9.d, PSR, ¶19. The attachments to the phishing emails started off as rudimentary (but highly effective) Microsoft Word documents or Rich Text Format (.rtf) files with embedded malware:

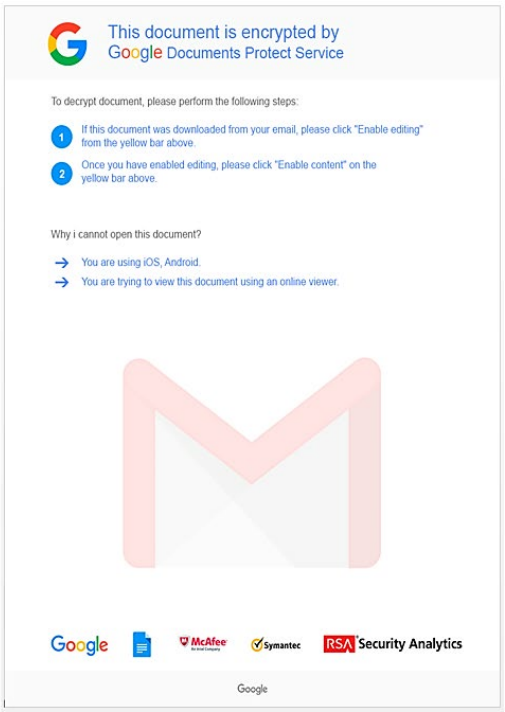


UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970




PSR, ¶17. Over time, the attachments became more and more sophisticated. Among other things, FIN7 improved the graphics in the file and incorporated trustmarks of well-known companies to increase the likelihood that recipients would activate the embedded malware, as exhibited in the examples below:






UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

FIN7 used multiple malware delivery mechanisms in its phishing attachments including, but not limited to, weaponized Microsoft Word macros, malicious Object Linking and Embedding (OLE) objects, malicious visual basic scripts or JavaScript, and malicious embedded shortcut files (LNK files).[7] PSR ¶17, PA, ¶9.d.

**D. The FIN7 Botnet**

Once the initial malware was activated, FIN7 gained a beachhead in the victim's network. PSR, ¶20. From this beachhead, FIN7 could deploy additional malware, conduct reconnaissance, and target systems that contained sensitive financial information. PA, ¶9.d. FIN7 typically used the Carbanak malware as a "backdoor" that allowed the enterprise to maintain persistent and discrete access to the victim company's network. PSR, ¶21. The Carbanak malware has robust data-stealing capabilities and even enables hackers to record activity occurring on the desktops of infected computers. In addition to the Carbanak malware, FIN7 had an arsenal of tools it used to maintain its presence in networks and to steal data. Examples of these tools include Cobalt Strike, DRIFTPIN, HALFBAKED, GRIFFON, Bateleur, and Metasploit Pro. PSR, ¶¶22-23.

FIN7's malware connected infected computers to a network of command and control servers located around the world. PA, ¶9.d. FIN7 regularly incorporated compromised computers or "bots" into a "botnet" that could be controlled through custom administrative control panels. PSR, ¶¶21-22. The control panels gave FIN7 the ability to view, edit, and send commands to a particular bot. PSR, ¶22. The panels also provide an effective means for the group to receive data back from the compromised computers. PSR, ¶23. And, most importantly, perhaps, the panels provided a scalable

---

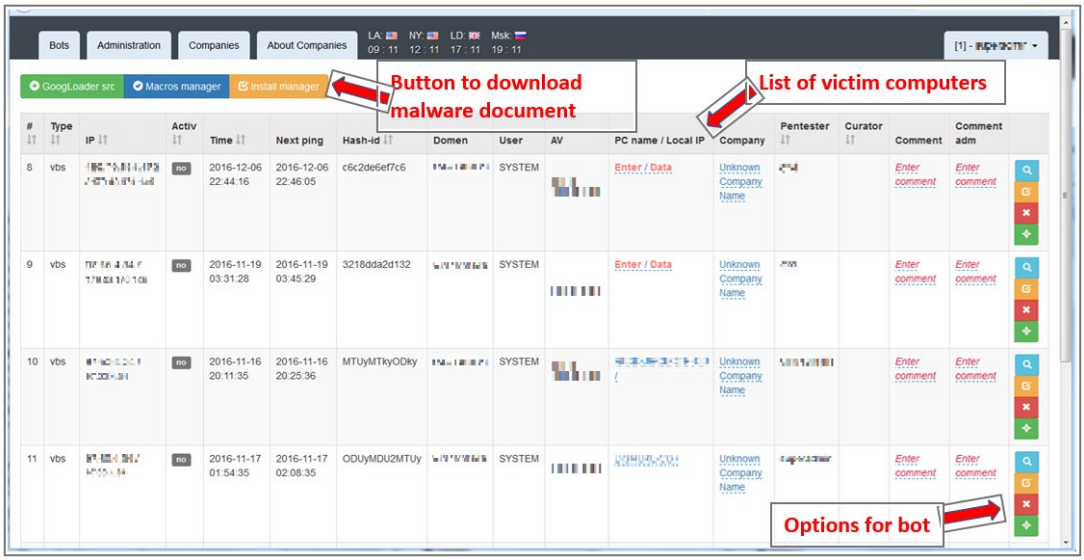
[7] *See* FIN7 Evolution and the Phishing LNK, https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html (last checked 4/8/2021); Footprints of FIN7: Pushing New Techniques to Evade Detection, https://www.icebrg.io/blog/old-dog-new-tricks-fin7-pushing-new-techniques-to-evade-detection (last checked 4/8/2021).



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

way for the enterprise to not only give new members access to breached computers, but also to add an unlimited number bots to the botnet.

The custom user interface for the administrative control panel gave FIN7 convenient access and control over individual bots. The panel listed each bot and provided information, such as the PC name of the bot, domain of the bot, and whether the bot had antivirus software. When a FIN7 member selected an individual bot, the panel allowed them to run a variety of commands, such as generating a list of processes running on the bot, executing programs, and taking a screenshot. The following annotated screenshot shows a version of the control panel and illustrates the functionality of the panel's interface:




In most cases, FIN7 members were tasked with locating and compromising the victims' point-of-sale systems, in order to scrape and steal the financial data of ordinary consumers. According to a study of a sample of just fifteen million payment cards stolen by FIN7, FIN7's hackers were able to locate and exploit the point-of-sale systems of over 3,600 physical locations across the country. PSR, ¶35.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

**E. FIN7's Victims**

Hundreds of victim companies were attacked by FIN7. PA, ¶9.b. These attacks resulted in the theft of troves of financial information, including the exfiltration of information for tens of millions of payment card numbers.[8] PA, ¶9.j. The breaches and the subsequent fraudulent use of the stolen financial information impacted numerous victims including companies who were breached, financial institutions, card brands, merchant processers, insurance companies, retail companies, and individual card holders. PA, ¶9.l; PSR, ¶35.

These victims incurred enormous costs that, according to some estimates, exceeded one billion dollars.[9] The breached companies faced costs associated with remediating the breach, customer notification, lost business, resolving ensuing class action lawsuits, and potentially paying fines to state Attorney Generals and government agencies.[10] PA, ¶9.l; PSR, ¶35. The financial institutions that issued the payment cards faced losses associated with the fraudulent purchases and replacing customers' cards. *Id.* Much of those losses were, in turn, passed onto businesses at which the stolen payment card numbers were used to make purchases.

FIN7 monetized the stolen financial information in various ways. One central way the enterprise sold payment card information was to advertise the sale of "dumps" of the information on underground vending sites such as Joker's Stash. PSR, ¶25. The following screenshot shows an advertisement on Joker's Stash of a dump of four million card numbers stolen by FIN7:

---

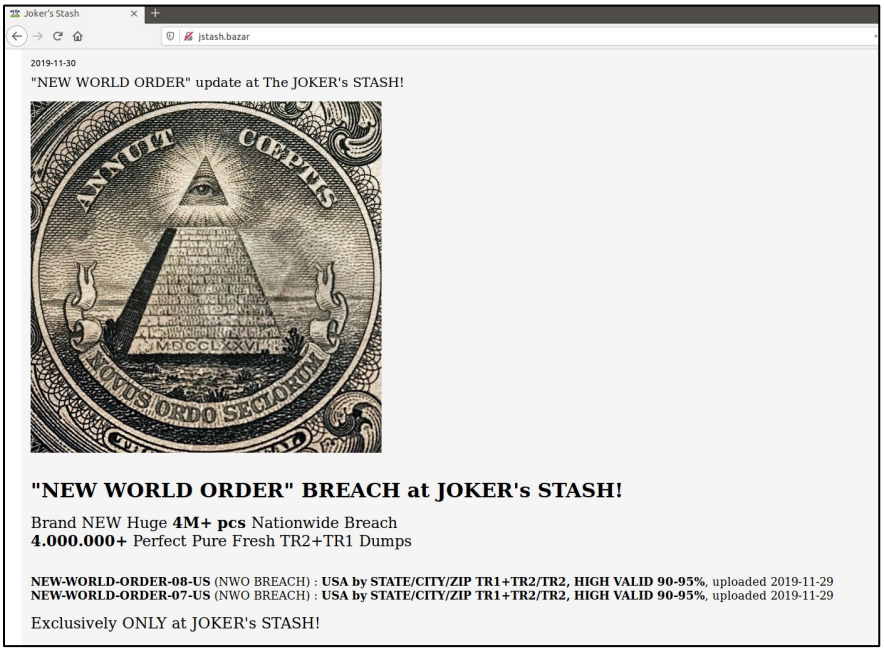
[8] The total number of payment cards that FIN7 stole is not at issue. For the purposes of sentencing, the parties have stipulated that Defendant Hladyr should be held accountable for the theft of 5.9 million payment cards. PA, ¶11.b.

[9] The actual loss number is not at issue. The parties have stipulated that – during Defendant Hladyr's participation in the criminal enterprise – FIN7 caused over $100 million in losses. PA, ¶9.l.

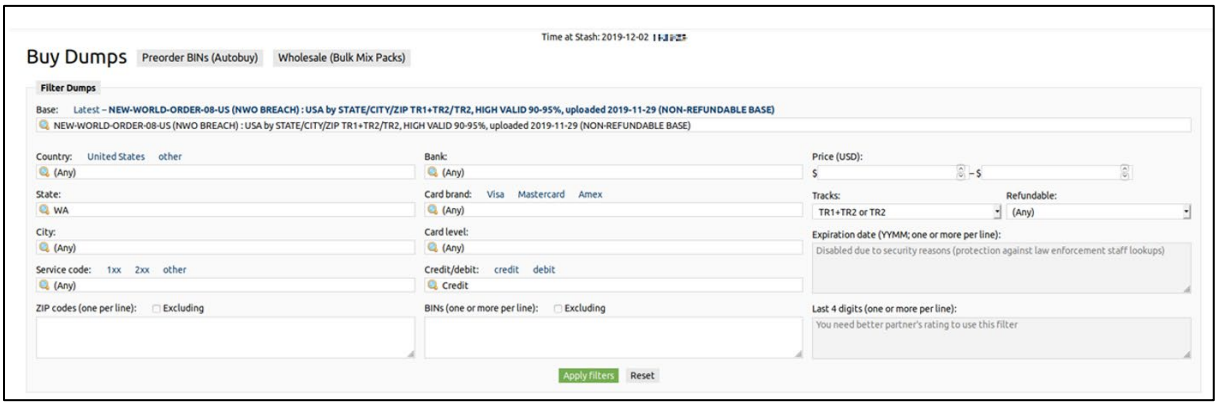
[10] The Ponemon Institute and IBM Security estimate that the average cost of a significant data breach in the United States in 2020 was $6.39 million, with the cost per record of customers' personally identifiable information coming in at $150. However, mega breaches which involved the theft of one to ten million records cost an average of $50 million. https://www.ibm.com/security/data-breach (last checked 4/8/2021).



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970




As shown in the next screenshot, Joker Stash allowed fraudsters to sort through solen payment cards by the type of card stolen (debit or credit), the level of the card (classic or platinum), and the state in which the owner of the card resided:




Fraudsters who purchased the stolen information would then imprint the information on blank payment cards so they could be used to conduct fraudulent purchases. The location of the legitimate card holder assists fraudsters in avoiding fraud alerts and detection mechanisms designed to notify financial institutions when customer cards are used to make purchases outside of the card holder's state of residence.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

**F. Defendant's Role as a FIN7 Manager**

Defendant Hladyr was a high-level manager and systems administrator for FIN7. PA, ¶¶9.f, 9.h-I; PSR, ¶27. Contrary to the statement on page five of the defense's sentencing memorandum, Defendant did not have "limited knowledge and understanding of the consequences of his actions as a system administrator," and his job responsibilities were anything but "typical."[11] As Defendant knowingly and intelligently stipulated during his change of plea hearing, he had full knowledge that he was being paid to be part of a major criminal enterprise:

> Shortly after joining Combi Security, Defendant became aware of the fact that Combi Security was not a legitimate company. Combi Security was the front company for an illegal enterprise that was attempting to breach the network security of victim companies without their knowledge or authorization. At no time during his work with Combi Security did Defendant see: (1) any indication (written or otherwise) that Combi Security had been hired to perform penetration testing; (2) any reports or recommendations written by Combi Security to purported customers explaining vulnerabilities in the customers' network security and offering recommendations on how to fix those vulnerabilities; or (3) any measures taken to appropriately safeguard from misuse the confidential information taken from the victims networks, such as network credentials, network maps, and sensitive business information.

PA, ¶9.g.

A system administrator typically is an IT professional responsible for managing and maintaining multiuser computer environments, such as a company's network environment. Defendant Hladyr was not a typical systems administrator. Defendant was responsible for setting up and maintaining a worldwide network of servers that a notorious cybercriminal enterprise used to carry out cyberattacks against hundreds of victims. PA, ¶9.f; PSR, ¶28. Among other things, these severs hosted the administrative

[11] This statement is inconsistent with the facts stipulated to in the plea agreement and elsewhere. Presumably, this statement was not intended to be a claim that minimized Defendant's role in the criminal enterprise and his knowledge of the illegality of his actions. If, however, the defense chooses to advance this claim at the sentencing hearing, the United States requests the opportunity to present evidence refuting the claim.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

control panels that FIN7 used to control infected computers and exfiltrate information for millions of payment cards. PA, ¶9.f.

Defendant also maintained communication servers used by FIN7, including HipChat, JIRA, Jabber, and servers. PSR, ¶31; PA, ¶9.f. Defendant's activity on these servers demonstrates that he was deeply involved with the illegal work of the enterprise. On the HipChat server, Defendant uploaded malware used by FIN7, stolen credit card information, and stolen data collected from victim computers including stolen usernames and passwords, network maps of internal network infrastructures, internal documents, and internal website server data. PSR, ¶32; PA, ¶9.i. On the JIRA project management server, Defendant was not only the server's administrator, but also an active participant. For example, on approximately September 7, 2016, Defendant created an issue on the JIRA server to coordinate FIN7's efforts to breach Victim-6, a U.S.-based delicatessen chain with hundreds of locations in the United States. That month, Defendant and one other FIN7 member uploaded several files and information about Victim-6's internal network infrastructure and stolen user credentials. A large number of payment card numbers stolen from Victim-6's point-of-sale systems by FIN7 were later offered for sale on Joker's Stash.

Defendant's technical acumen allowed him to rise within the enterprise. He was elevated quickly to a managerial role in which he communicated regularly with FIN7's top-tier leadership – consisting of approximately four individuals – and relayed their orders to subordinate FIN7 members. *See* PA, ¶9.h; PSR, ¶30. In this high-level role, he was responsible for, among other things, "aggregating stolen payment card information, providing technical guidance to FIN7 members, issuing assignment to FIN7 hackers, and supervising teams of hackers." PA, ¶9.h. In return, Defendant Hladyr received increased payments and bonuses, which amounted to a sizeable sum by Ukrainian standards.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

## III. THE PLEA AGREEMENT AND THE SENTENCING GUIDELINES CALCULATION

### A. The Plea Agreement

On September 11, 2019, Defendant Hladyr pleaded guilty to one count of Conspiracy to Commit Wire Fraud (Count 1), in violation of 18 U.S.C. § 1349, and one count of Conspiracy to Commit Computer Hacking (Count 16) in violation of 18 U.S.C. § 371. PA, ¶1 (Dkt. #64). The plea agreement includes an extensive statement of facts setting forth a summary of Defendant Hladyr's central role as a high-level manager and systems administrator for the FIN7 criminal enterprise. *See* PA, ¶9.

#### 1. Dismissal of Remaining Counts

Pursuant to Paragraph 1 of the plea agreement, the United States requests dismissal of Counts 2-15 and 17-26 of the Superseding Indictment.

#### 2. Forfeiture

Defendant stipulated that he made at least $100,000 for his participation in the FIN7 criminal enterprise. *See* PA, ¶9.l. Consistent with that stipulation, Defendant agreed in Paragraph 7 of the plea agreement to forfeit a sum of money in the amount of $100,000. On April 1, 2021, the United States filed a motion for entry of a forfeiture money judgment. Dkt. #71. Subsequently, on April 9, 2021, the Court entered the proposed forfeiture order. Dkt. #84. The United States requests that the Court make the order part of Defendant's sentence at the sentencing hearing.

#### 3. Restitution

The harm caused by Defendant and his FIN7 co-conspirators is enormous. For the purposes of sentencing, the parties have stipulated that the actual loss to financial institutions, merchant processers, insurance companies, retail companies, and individual cardholders exceeded $100 million. *See* PA, ¶9.l. In Paragraph 6 of the plea agreement, Defendant agreed to pay restitution in the apportioned amount of $2,500,000. Accordingly, the United States requests that the Court enter a restitution judgment in this



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

amount and specify that this obligation shall not be joint and several with any other FIN7 defendant.

**4. Appellate Wavier**

In paragraph 16 of the plea agreement, Defendant waived his appellate rights and his rights to collateral attack provided that the Court imposes a custodial sentence that is within or below the Sentencing Guidelines range. Assuming the Court imposes a term of incarceration that is within or below the Sentencing Guidelines range as determined by the Court at the time of sentencing, the United States requests that the Court advise Defendant appropriately regarding his remaining appellate rights, following imposition of sentence.

**B. The Presentence Report and the Offense Level Calculation**

In Paragraph 11 of the plea agreement, the parties stipulated to the following Guidelines calculation:

a. A base offense level of 6, pursuant to USSG § 2B1.1(a)(2).

b. An offense level enhancement of 30 levels (+30), based on a loss amount of more than $550,000,000, pursuant to USSG § 2B1.1(b)(1)(P). For the purposes of sentencing, the parties agreed to limit the number of stolen payment cards to 5.9 million. Pursuant to Application Note 3(F)(i), a $500 loss amount is imputed to each payment card, resulting in a total loss amount, for Guidelines purposes, of $2,950,000,000.

c. An offense level enhancement of 2 levels (+2), because the offense involved more than 10 victims, pursuant to USSG § 2B1.1(b)(2)(A).

d. An offense level enhancement of 2 levels (+2), because the offense involved receiving stolen property, and the defendant was a person in the business of receiving and selling stolen property, pursuant to USSG § 2B1.1(b)(4).

e. An offense level enhancement of 2 levels (+2), because a substantial part of the fraudulent scheme was committed from outside the United States and because



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the offense involved sophisticated means and the defendant intentionally engaged in and caused the conduct constituting sophisticated means, pursuant to USSG § 2B1.1(b)(10).

f. An offense level enhancement of 2 levels (+2), because the offense involved the trafficking in unauthorized access devices and counterfeit access devices and because the offense involved the possession of more than 5 means of identification that were unlawfully obtained, pursuant to USSG § 2B1.1(b)(11).

g. An offense level enhancement of 3 levels (+3), because the defendant was a manager (but not an organizer or leader) and the criminal activity involved more than five participants and was extensive, pursuant to USSG § 3B1.1(b).

h. An offense level reduction for acceptance of responsibility, pursuant to USSG § 3E1.1.

The stipulated Guidelines range results in in a total offense level of 43 after crediting Defendant Hladyr with three points (-3) for acceptance of responsibility. Defendant Hladyr falls within criminal history category I, as he has no countable criminal convictions.

The United States Probation Office prepared a final presentence report on April 2, 2021 with a Guidelines calculation that is consistent with the parties' stipulations. A total offense level of 43, even coupled with a criminal history category I, would result in a life sentence under the advisory Guidelines. However, in this case, the Guidelines range of imprisonment is the statutory maximum sentence of 25 years, pursuant to USSG § 5G1.1.

**C. Defendant's Time in Custody**

It is the government's understanding that the Bureau of Prisons will give Defendant Hladyr credit for the time he has spent in law enforcement custody since his initial arrest in Germany on January 10, 2018. PSR, ¶33. At the time of the sentencing hearing on April 16, 2021, Defendant will have been in law enforcement custody for approximately 39 months.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

## IV. SENTENCING RECOMMENDATION

The United States joins the Probation Office in recommending a ten-year custodial sentence for Defendant Hladyr. Specifically, the United States recommends 120 months of imprisonment for Count 1 and 60 months of imprisonment for Count 2, to be served concurrently. As discussed below, the United States submits that this recommended sentence is sufficient but not greater than necessary, and is justified by a balancing the factors set forth in Title 18, United States Code, Section 3553(a).

As the Ninth Circuit and the Supreme Court have explained, the Sentencing Guidelines are "the 'starting point and the initial benchmark' . . . and are to be kept in mind throughout the process." *United States v. Carty*, 520 F.3d 984, 996 (9th Cir. 2008) (internal citations omitted). Title 18, United States Code, Section 3553(a), sets forth factors for the Court to consider alongside the advisory Guidelines range. The United States submits that the recommended sentence is appropriate particularly in light of "the nature and circumstances of the offense," "the history and characteristics of the defendant," and the need for the sentence "to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense," "to afford adequate deterrence to criminal conduct," and "to avoid unwarranted sentence disparities." 18 U.S.C. §§ 3553(a)(1), (a)(2), and (a)(6).

### A. The Nature and Circumstances of the Offenses

The nature and circumstances of Defendant Hladyr's offenses are unprecedented in this district. Defendant was a key member of one of the most sophisticated and successful hacking groups in modern times. Under the advisory Guidelines, Defendant is accountable for a loss amount of $2,950,000,000. No defendant in memory has been accountable for a larger loss amount in this district.

Although the aggregate loss amount under the Guidelines is astronomical, it does not adequately convey the harm that Defendant and his FIN7 co-conspirators caused to victims around the world. FIN7 was relentless in its repeated attacks against hundreds of



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

companies. As explained in Section II.E, *supra*, these attacks negatively impacted numerous parties including the companies whose security was breached, the card brands and financial institutions associated with the stolen payment cards, the individual card holders who had their information stolen, and the businesses at which the stolen payment cards were later used to make fraudulent purchasers. Defendant Hladyr deserves a sentence that reflects the enormity of the harm he caused to these victims.

The scale and sophistication of the FIN7 criminal enterprise is also an aggravating factor. Unlike groups of rogue cybercriminal actors, FIN7 approached hacking with the premeditated discipline and refinement of a multinational business operation, which it essentially was, albeit with an illegal and nefarious business plan. FIN7's structure assigned discrete aspects of the hacking and monetization processes across members and groups, all subject to a management hierarchy comprised of managers and top-level bosses, who operated like executives. For instance, while certain members continued to develop and improve the phishing email messaging and social engineering techniques, others continued to build upon the enterprise's suite of malware tools. Others, including Defendant Hladyr, managed the physical infrastructure of the operation, while also providing mentorship and technical training to subordinates. Only a complex and disciplined enterprise like FIN7 could have integrated these diverse roles in a cohesive and scalable manner that allowed the enterprise to have a devastating worldwide impact.

Defendant Hladyr was not a peripheral player in the criminal enterprise. To the contrary, for the 29 months from when he joined the group in August 2015 to when he was arrested in January 2018, Defendant was a high-level manager who directed other members of the group and who controlled FIN7's extensive server infrastructure and encrypted channels of communication. Quite literally, Defendant held the keys to the kingdom. It was Defendant who had the ability to grant new members access to the communication servers that FIN7 used to coordinate its attacks. And, it was Defendant who set up and managed the complex web of servers located around the world that FIN7



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

used to deploy its malware, control infected computers, and steal payment card information and other financial information. Just as Defendant Hladyr had the ability to setup these servers, he had the ability to disable them. Only his greed prevented him from pulling the plug on the entire operation and turning over valuable evidence to law enforcement. There should be little doubt that Defendant would still be working for FIN7 today if he had not been arrested.[12]

The defense contends that a ten-year sentence is disproportionate to Defendant's role and the proceeds he received. However, a sophisticated cybercriminal like Defendant Hladyr should not be permitted to raise disproportionality as a shield for at least three central reasons.

***First***, the asymmetry between the relatively limited investment of resources by cybercriminals and the enormous harm they cause is exactly what makes cybercrime so alluring. Cybercriminals like Defendant Hladyr pose such a great threat because they use their specialized skills and training to *amplify* the reach and impact of their criminal activity. Instead of having to physically rob a thousand individual locations of a major restaurant chain one by one, FIN7 hackers were able to deploy a single methodology to rob *all* of the locations of *multiple* restaurant chains *simultaneously* from the comfort and safety of their keyboards in distant countries. Consequently, Defendant Hladyr cannot fairly invoke disproportionality when he made a deliberate decision to leverage his technological expertise to carry out his criminal activity on a massive scale.

***Second***, and relatedly, the asymmetrical harm caused by Defendant's offenses were the foreseeable and intended consequences. This is not a case where a defendant

---

[12] As previously mentioned, there was a level of leadership above Defendant Hladyr who likely received the lion's share of the criminal proceeds. In recommending only a ten-year sentence, the United States weighed heavily the fact that Defendant was not a top-level leader in the criminal enterprise and, as a result, did not make millions in profit. Although the proceeds Defendant received were modest by Western standards, they were substantial by Ukrainian standards and allowed him to afford luxuries like a European tour and visit to Disneyland Paris. Fittingly, it was that trip that led Defendant's arrest on his return route through Germany.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

takes a simple action that cascades into a series of unpredictable events. To the contrary, Defendant Hladyr and his co-conspirators knew exactly what they were doing and the harm that they would cause. FIN7's methodology relied on volume – to hack and harvest the maximum amount of financial data, and in turn to indiscriminately impact the maximum number of individual victims. Defendant and his co-conspirators fully understood the devasting harm the data breaches would cause and the large amount of fraudulent purchases that would be made with the stolen payment card information. Because this was the intended result of FIN7's relentless attacks, Defendant cannot now claim to be a victim of his own success in helping to accomplish this goal.

***Third***, criminal proceeds from cybercrime are almost always substantially less than the harm incurred by victims. This is particularly true when hackers attempt to profit from stolen payment card information. FIN7 monetized the stolen payment card information by selling it in bulk sales on underground forums such as Joker Stash. As a result, the proceeds that FIN7 received per stolen payment card was relatively low (compared to the ensuing fraudulent purchases made using the stolen card information), particularly after middlemen who facilitated the sales took their cut. Defendant Hladyr cannot reasonably contend that he is entitled to a sentencing discount because he received only a portion of the overall profits made by all the criminals who exploited the stolen payment card information.

**B. Defendant's History and Characteristics**

Defendant Hladyr's history and characteristics suggest a sentence below the advisory Guidelines range would be appropriate. The recommended ten-year sentence appropriately considers that Defendant has no prior criminal history and held legitimate jobs before he joined FIN7. However, the recommended sentence also considers the fact that Defendant still poses a risk of recidivism. After Defendant is released, he will be deported and likely will return to Ukraine. The same financial hardships that he claimed forced him to join FIN7 will be present when he reenters society after serving his



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

sentence. It remains to be seen whether Defendant will resist the lure of the asymmetrical rewards he could reap by again leveraging his technical expertise to commit crime.

### C. The Need for the Sentence to Reflect the Seriousness of the Offenses, to Promote Respect for the Law, and to Provide Just Punishment

These factors weigh strongly in favor of a judgment that imposes a lengthy term of incarceration. Given FIN7's notoriety, this case will be used nationally as benchmark for sentences in other major cybercrime cases. Crimes like those committed by Defendant Hladyr are a serious threat to the viability of businesses and financial institutions everywhere, as well as to the security of their customers. A ten-year custodial sentence would send a message that there are harsh consequences for joining a cybercriminal enterprise like FIN7.

The need to promote respect for laws that prohibit cybercrime is particularly high given the major increase in attacks against U.S. interests that are launched by foreign actors. It is rare that a member of a sophisticated cybercriminal organization is identified, arrested, and extradited for prosecution in the United States. Too often, international cybercriminals can conceal their identities or hide in countries in which they are beyond the reach of law enforcement. Accordingly, this case presents a rare opportunity to demonstrate that not only can law enforcement identify and arrest sophisticated cybercriminals, but also that such cybercriminals face harsh consequences for attacking U.S. businesses and consumers.

Finally, no discussion of these factors would be complete without additional mention of the enormous harm that Defendant Hladyr caused to numerous victims. These victims included, at a minimum, "financial institutions, merchant processers, insurance companies, retail companies, and individual cardholders."[13] PA, ¶9.l. A ten-

[13] It is important to note the general public bears much of the cost caused by cybercriminal enterprises. When businesses sustain fraud-related losses or expenses, they generally pass these costs on to the average American in the form of higher prices, fees and other indirect charges. *See* Lydia Segal, *Credit Card Fraud: A New Perspective on Tackling an Intransigent Problem*, 16 FORDHAM J. CORP. & FIN. L. 743, 754, 775 (2011) (banks and credit card companies pass on costs of fraud to consumers in the form of higher prices, banking costs, and other charges); *see*



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

year sentence is needed to provide just punishment and to vindicate the interests of these victims.

**D. The Need to Afford Adequate Deterrence to Criminal Conduct**

High rewards and a relatively low risk of detection are basic features of modern cybercrime. However, appropriately severe sentences can impact the cost-benefit analysis of would-be cybercriminals. Computer hackers are among the most sophisticated criminals in the world and are known to closely monitor U.S. authorities' response to cybercrime and plan accordingly. Achieving general deterrence in this area, therefore, appears somewhat promising. *See United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (because "economic and fraud-based crime are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence").

This case demonstrates that there is an acute need to impose a sentence that deters others from joining cybercriminal organizations. Criminal enterprises such as FIN7 rely on the ability to recruit technologically skilled individuals such as Defendant Hladyr. A ten-year sentence will put potential recruits on notice that engaging in cybercrime will subject them to significant prison sentences that are commensurate with the harm they cause. A ten-year sentence will also send a message to FIN7 members who are still engaged in criminal activity. Intercepted communications between these members show that they are closely watching the progression of the cases against their former colleagues. It is important that they know the severe consequences they face not just for their past crimes, but any future crimes they should commit. Giving one of their valued colleagues a decade of jail time will convincingly show at least some that the cost of doing business is too high.

---

*also* Ronald Mann, *Credit Cards and Debit Cards in the United States and Japan*, 55 VAND. L. REV. 1055, 1093-94 (2002) (credit card companies pass on costs of fraud to cardholders and merchants).



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

**E. The Need to Avoid Unwarranted Sentencing Disparity**

Cybercrime takes many forms, and it is difficult to compare cybercriminal schemes that utilize different methodologies and that impact different groups of victims. For this reason, it is difficult to compare sentences imposed on defendants who participated in different cybercriminal enterprises. Nevertheless, two cases from the Western District of Washington provide important reference points.

In the first case, *United States v. Schrooten*, CR12-085RSM, this Court sentenced a prominent hacker and payment card thief to 12 years pursuant to a Rule 11(c)(1)(C) plea agreement. Although Schrooten's carding ring was considered substantial at the time, he had in his possession only 100,000 stolen payment card numbers. In the second case, *United States v. Roman Seleznev*, CR11-70RAJ, Judge Jones sentenced the leader of an extensive payment card trafficking ring to 27 years after he was convicted at trial. Seleznev's carding ring was substantially smaller in scope than FIN7, and he ultimately was held responsible for only 2.9 million stolen payment cards that were found in his possession. However, there were many aggravating factors in Seleznev's case including his leadership role, the enormous amount of proceeds he received, his extensive efforts to obstruct justice, and evidence that he had stolen many more payment cards.

The *Schrooten* and *Seleznev* cases involved schemes that were orders of magnitude smaller than the FIN7 criminal enterprise. However, both defendants were deserving of harsher sentences than Defendant Hladyr because they were the leaders of their respective schemes and reaped most of the illegal proceeds. Although Defendant Hladyr was a key member of FIN7, he was not the driving force behind his criminal enterprise as were Schrooten and Seleznev. Accordingly, a sentence of ten-years appropriately balances the differences between these three cases and reaches a just result.

In contrast, the defense's recommendation of time-served (approximately 39 months) would create a severe disparity with not only the *Schrooten* and *Seleznev* cases, but also with cases involving less sophisticated schemes or much smaller fraud amounts.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

For example, in *United States v. Guthrie*, CR16-253JLR, Judge Robart imposed four-year sentences on two identity thieves who used stolen, personally identifiable information to generate approximately $213,521 in wire fraud proceeds. Similarly, in the *Schrooten* case, this Court imposes a seven-year sentence on Christopher Schroebel, a lower-level member of the carding ring who had possession of only 86,400 stolen payment cards. Defendant Hladyr deserves a substantially higher sentence than the sentences in posed in these cases, particularly given Defendant's significant role in a criminal enterprise that caused such a devasting impact worldwide.

//

//

//

//

//

//



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

## V. CONCLUSION

For the reasons set forth above and in the government related filing, the United States respectfully requests that the Court impose a total sentence of 120 months on Counts 1 and 16 (with credit for time served in international and domestic custody), order restitution in the amount of $2,500,000, order Defendant to forfeit a sum of money in the amount of $100,000, and impose a $200 special assessment.

DATED this 9th day of April, 2021.

Respectfully submitted,

TESSA M. GORMAN
Acting United States Attorney

*/s/ Francis Franze-Nakamura*
FRANCIS FRANZE-NAKAMURA
STEVEN MASADA
Assistant United States Attorneys
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Telephone: 206.553.4402
Fax: 206.553.4440
Email: francis.franze@usdoj.gov

ANTHONY TEELUCKSINGH
Senior Trial Attorney
Computer Crime and Intellectual Property Section, U.S. Department of Justice