UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

UNITED STATES OF AMERICA	**)**	
	)	
v.	**)**	**1:11-cr-64-01-SM**
	)	
ADRIAN-TIBERIU OPREA	**)**	

GOVERNMENT'S SENTENCING MEMORANDUM
AS TO DEFENDANT ADRIAN-TIBERIU OPREA

The Government submits this Sentencing Memorandum for the upcoming sentencing of Adrian-Tiberiu Oprea, who was the ringleader of a massive, international computer hacking and credit card data theft scheme that, over the course of several years, victimized hundreds and hundreds of U.S. merchants, and hundreds of thousands of U.S. payment cardholders and their banks. Oprea's uninterrupted course of computer crimes, wire frauds, and access device crimes resulted in actual losses of at least $17.5 million and ended only when he was eventually extradited from his home country of Romania to the United States. Oprea pleaded guilty, without a plea agreement but with a signed Acknowledgment and Appeal Waiver, to all four counts in the indictment, charging him with conspiracy to commit computer-related fraud in violation of 18 U.S.C. § 371 (Count One), conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349 (Count Two) and with conspiracy to commit fraud in connection with access devices, in violation of § 1029(b)(2),(a)(2) (Counts Three) and § 1029 (b)(2), (a)(3) (Count Four).

As set forth below, the seriousness of Oprea's crimes, coupled with the profound need to provide adequate specific deterrence to Oprea as well as to provide general deterrence to other hackers, dictate the government's recommendation that he be sentenced to not less than 15 years.

Moreover, a 15-year sentence would be in line with other sentences meted out to co-conspirators in this case as well as in other courts around the country that involved similar conduct.

1. Nature and Scope of Oprea's Criminal Conduct and Seriousness of Offense

As set forth in the Pre-Sentence Investigation Report ("PSI") and the indictment, from 2009-2011, Oprea, operating from his home base in Romania, was the mastermind of a widespread, international scheme that targeted and hacked into hundreds of U.S. merchants' "point-of-sale" ("POS") systems (in essence internet-connected, computerized cash registers) and then stole over a hundred thousand customers' credit, debit, and other payment card data that were stored on those POS systems. Oprea and his co-conspirators then either used the stolen payment card data themselves to make unauthorized charges on the cardholders' compromised accounts or they re-sold the data on the black market to others who would do the same. One of the primary victims of Oprea's hacking scheme was the Subway restaurant franchise system, including a franchise located in New Hampshire.

Ultimately, Oprea and his co-conspirators successfully hacked into over 800 different merchants' computer networks. Of those hacking victims, approximately 250 were Subway restaurant franchises, and over 150,000 cardholder accounts were compromised from Subway restaurant franchises alone. As set forth in more detail below, looking at the Subway-related losses alone, Oprea and his co-conspirators caused an estimated $12.5 million in unauthorized charges to be made on the accounts that they had compromised at Subway restaurants. In addition, they caused Subway to spend over $5 million in remediation expenses responding to the hacking scheme.

Oprea essentially wreaked havoc on Subway, both at the corporate level and at the individual franchise level. Subway launched a massive investigation to try to locate the source of the breach and scrambled to implement software and hardware adjustments to try to block the flow of card data out of its hacked POS systems. With over 25,000 different Subway restaurant franchises potentially exposed and 150,000 cardholders' account information at risk, Subway expended close to $200 per franchise to try to find the hole and stop the leak.

2. Oprea's Role in the Conspiracy

Oprea was at the center of a prolonged assault on close to 1,000 U.S. merchants' computer networks, and he knowingly victimized hundreds of thousands of U.S. cardholders whose data was exposed as a result. He has a background in computers, and as set forth below, he is well known to Romanian law enforcement as a hacker who specializes in "carding" activities (hacking into computers primarily to steal payment card data and then fraudulently using that payment card data to make unauthorized charges on the compromised accounts). Oprea was responsible for (1) targeting U.S. merchants' POS systems, (2) hacking into those POS systems and installing the "keystroke logging" software programs on those POS systems, which recorded and stored the stolen payment card data, (3) ex-filtrating the stolen card data to himself, (4) setting up "dump sites" (using stolen credit cards), or computer servers in the U.S. and in Cyprus, to store the stolen card data, hacker tools, and other items that he used, and (5) monetizing his efforts by making unauthorized charges on the compromised accounts or selling the data to others on the black market who would re-sell to others or make unauthorized charges themselves.

In order to expand his hacking and carding empire, Oprea recruited others to help him. He recruited his co-conspirator and friend, Iulian Dolan, to help him on the front-end of the operation, with the hacking and the exfiltrating of the card data. Oprea instructed Dolan to do the same thing he was doing—hack into U.S. merchants' POS systems, install keystroke logging software on them, and then send the stolen payment card data to Oprea's "dump sites." He paid Dolan several thousand dollars for Dolan's help. He also recruited trusted buyers, including his co-conspirators Cezar Butu and Florin Radu, as well as several others who were known by their screen names, which included "tonymontana," "helldump," and "brololo." These individuals would pay Oprea for the payment card data and then re-sell the stolen card data on the black market and in some cases also use the cards themselves to make unauthorized charges.

In order to ensure the continued "success" of his hacking operation, Oprea, who was no stranger to Romanian law enforcement, also employed several techniques to avoid detection, and he instructed his co-conspirators to follow suit. (Indictment ¶ 20). He opened dozens and dozens of constantly-changing e-mail and instant messaging accounts, and then assigned those e-mail accounts to be used by himself and his co-conspirators in their communications about their POS system hacking scheme. He used stolen identities and credit card numbers to open and pay for the "dump sites" at a U.S.-based webhosting company, as well as in Cyprus. He utilized an innocent hacked business computer in Mechanicsburg, Pennsylvania, co-opting this computer to hide his identity and his location in Romania during the scheme. He used the "dump sites" and the hacked business computer not only to hide his identity but also to store his hacker tools, stolen payment card data, and other valuable tradecraft. (*Id.*). Oprea also devised a way to issue "delete" commands to the various dump sites and to use other techniques on the POS systems to

hide his tracks. He instructed his co-conspirators to employ these same evasive techniques to avoid detection.

3. Oprea's Relevant Conduct in Prior Credit Card Theft Schemes

Although Oprea has no known criminal history in the United States (given that he has, until his extradition, resided in Romania), Oprea has a criminal record in Romania for engaging in carding activity. The government is aware of two ongoing criminal prosecutions against Oprea from two different districts in Romania. Both involve stolen credit cards. In his conversations with his co-conspirators, Oprea repeatedly mentioned that he needed to take extra precautions to avoid detection because he had been arrested before and had his computers searched and seized by Romanian law enforcement.

4. The Government's Guideline's Calculation

The Government believes that the following Guideline calculation applies:

§2B1.1 – Conspiracy, Computer Fraud, and Access Device Fraud

§2B1.1(a)(2)	Base	7
§2B1.1(b)(1)(L)	Loss $50-100 million	24
§2B1.1(b)(2)(C)	250 or more victims	6
§2B1.1(b)(9)(B)	Sophisticated means/overseas ops	2
§2B1.1(b)(11)	Access device offense	2
§2B1.1(b)(17)	1030(a)(5)(A) offense	4

§3B1.1(a)	Leader/organizer	4
§2B1.1 Total		49
Acceptance of responsibility adjustment		-3
Adjusted offense level		46

The government has also reviewed the Pre-Sentence Investigation Report ("PSI"), and it agrees with the Probation Office's guideline's calculation. As indicated in the PSI, Oprea's guideline's calculation, with three points off for acceptance, is a level 46, which gets treated as a total offense level of level 43, pursuant to U.S.S.G. 3E.1(b). This corresponds to a life sentence.

The PSI notes one factor that might warrant a departure or variance, namely, that the $50-$100 million loss amount is driven in large part by a statutorily defined loss calculation of $500 per account for 150,000 compromised accounts. This $50-$100 million number may well overstate the actual losses that resulted from Oprea's extensive criminal activity, thereby overstating the seriousness of the offense. Although the government agrees with the PSI's calculation, it also agrees that the $50-$100 million loss may overstate the seriousness of the offense. As the defendant will no doubt argue, there is an alternative loss calculation that the Court could adopt, based on actual losses identified with respect to approximately 25,000 of the 150,000 accounts compromised. Using those numbers, as set forth below, the Court could find the loss amount to be approximately $17.5 million. That number includes approximately $5 million in remediation expenses incurred by one of the principal victims, the Subway restaurant franchise company. It also includes an estimated $12.5 million in extrapolated fraudulent charges that were made on the accounts that were compromised at various Subway restaurants. It bears noting that this $12.5 million still understates the actual losses because, although Subway

was the primary victim of Oprea's hacking and payment card data theft scheme, it was by no means the only victim. Of the 800 different merchants that Oprea and his co-conspirators hacked into, only 250 of those were Subway restaurant franchises.

Using the $17.5 million loss amount (and a corresponding guideline's increase of 20 instead of 24 levels) would bring Oprea's adjusted total offense level to 42. This corresponds to a sentence of 360 months-life. Significantly, the combined statutory maximum is 35 years (five years each for the conspiracy, computer fraud and access device fraud counts, and 20 years for the wire fraud count).

5. Loss Calculation

In calculating the loss figure, the government has used both the statutory loss amount of $500 per stolen card, as provided in 2B1.1(F)(i), as well as an estimate of the actual losses that Oprea caused. As far as the $50-$100 million statutory loss amount, that number is driven in large part by the large number of compromised payment card accounts. In terms of quantifying the number of accounts that were compromised, Subway alone has identified approximately 150,000 compromised accounts (112,000 Visa and Mastercard accounts and 33,000 American Express and Discover Card accounts). The number of compromised accounts refers to the number of accounts that Oprea actually stole hacking into the Subway POS terminals. It does not reflect, however, the total number of accounts that were successfully used to make unauthorized charges. That number has never been fully ascertained by the myriad issuing banks involved. As noted above, however, this 150,000 number understates the total number of compromised accounts, as they represent only Subway's numbers. There were other merchants who were victimized but who have not provided figures. The investigation identified a total of

800 merchants who were victimized by Oprea's scheme. Subway accounts for 250 of those 800. Multiplying the 150,000 compromised accounts by the $500/account set forth in the sentencing guidelines equates to slightly less than $73 million as noted at paragraph 15 of the PSI. That falls within the $50-$100 million loss range in Section 2B1.1(b)(1)(M) of the guidelines, resulting in 24 levels being added.

Nevertheless, the government believes that the $73 million number may overstate the actual loss that Oprea caused, and consequently may overstate the seriousness of the offense, because not all of the compromised accounts incurred unauthorized charges on them.[1] Extrapolating from data provided by MasterCard, as to the Subway restaurants alone, it is estimated that approximately 25,000 of the 150,000 compromised accounts incurred unauthorized charges on them, totaling approximately $12.5 million in unauthorized charges.[2] In addition, Subway has estimated that it incurred approximately $5 million in responding to the

[1] During the latter stages of the scheme, the Secret Service was able monitor the exploits of Oprea and was therefore able to identify compromised payment card accounts prior to Oprea being able to process and sell them to co-conspirators. Because the Secret Service was able to so notify the issuers of many of the compromised accounts, those accounts were closed prior to them being fraudulently used. Unfortunately, notwithstanding these efforts, millions of dollars were still lost.

[2] Examining data from December 2009-November 2011, of 24,591 MasterCard accounts that were known to have been compromised at Subway restaurant franchises, unauthorized charges were made on 4,112 of those accounts. So approximately 17% of the compromised accounts had actually been used to make unauthorized charges. MasterCard was able to show with particularity that the unauthorized charges made on those 4,112 accounts during that time frame totaled approximately $2.1 million. Accordingly, approximately $510 on average was fraudulently charged to each of those accounts ($2,100,000/4,112=$512) which is interestingly close to the presumed guideline minimum loss amount of $500/card. Extrapolating the MasterCard data to apply to the total number of 150,000 compromised accounts yields an estimate of total unauthorized charges of approximately $12.5 million; 150,000 compromised accounts x 17% charged = approx. 25,000 charged accounts times $500/account = $12.5 million.

hacking scheme.[3] Accordingly, the total actual losses that resulted from Oprea's criminal conduct are approximately $17.5 million.

Although admittedly this does not account for all of the stolen cards, it nevertheless accounts for a significant portion of the stolen cards and the government believes that it is a reasonable estimate of the actual loss.

6. Other Enhancements

The government is also recommending a six-level enhancement for multiple victims, given that over 150,000 cardholders had their accounts compromised at the 250 Subway franchises alone, and there were at least 800 identified hacking victims. See also §2B1.1, Comment 4(e) (defining identity theft "victim" to include those whose means of identification were stolen, irrespective of whether they actually sustained monetary losses). The government is also recommending a two-level enhancement under §2B1.1(b)(10)(B) and (C) for sophisticated means/overseas operations. As the Guidelines note indicates, this enhancement applies if "a substantial part of a fraudulent scheme was committed from outside the United States." Here, the bulk of the scheme took place in Romania. Furthermore, Oprea employed sophisticated means in the hacking scheme---he engaged in port scanning, installing malware remotely over the internet, ex-filtrating data to himself, using proxy computers to hide his identity, using

[3] Specifically, according to Subway, it spent $4.5 million on installing an end-to-end encryption hardware and software system in each of 25,000 Subway restaurant franchises, as well as $500,000 in installing a centralized monitoring console so that it could monitor data breaches from headquarters. The $4.5 million amount seems high, but divided by 25,000 franchises, it equates to only $180 per store. Subway also incurred $100,000 in forensic investigative costs, $500,000 in incident response expenses, and an additional $500,000 in hardware and software to centrally monitor their computer systems.

dozens of disposable e-mail and chat addresses, setting up dump sites, compromising a computer in Pennsylvania, and the like.

The government also recommends a two-level enhancement under § 2B1.1(b)(11) because the offense involved trafficking access devices (here, payment card account numbers and other information). Oprea pleaded guilty to all counts of the indictment, and count three charged him with conspiracy in connection with trafficking in access devices, in violation of 18 U.S.C. § 1029. Likewise, Oprea should receive a four-level enhancements under § 2B1.1(b)(17) for engaging in a hacking crime that involved the installation of malicious software code (e.g., the keystroke loggers) under 18 U.S.C. § 1030(a)(5)(A). Oprea pleaded guilty to count one, which charges him with conspiring to violate 18 U.S.C. § 1030(a)(5)(A), among other crimes. (Indictment ¶9(c)).

The government also recommends a four-level enhancement under § 3B1.1(a) for Oprea's role in the offense as a leader/organizer, as well as for his role in an offense that was otherwise extensive. As to the extensive nature of the scheme, it spanned three years, involved conduct in many different countries (dump sites in Cyprus, hackers in Romania, victims in the U.S., buyers in France), and involved hundreds of hacked computers. Furthermore, it involved dozens of constantly changing dump sites, disposable e-mail and instant message chat accounts, and over 150,000 compromised accounts. Oprea was also a leader/organizer of over 5 people. He not only supervised his co-conspirator Iulian Dolan on the front-end, but he also supervised various re-sellers, including co-conspirator Cezar Butu, on the back-end, who helped him sell the stolen card data on the black market. Other buyers/re-sellers include Radu, and three others known only by their screen names. Furthermore, Butu himself oversaw a team of at least five others who worked with him in a rented house in Lille, France, to encode the stolen payment

card data onto blank plastic cards. By extension, then, Oprea effectively supervised not only Butu but his crew as well. In total Oprea supervised Dolan, Radu, Butu, Butu's group of five, and the three known only by their screen names. Consequently, Oprea was the leader of a criminal activity that involved at least eleven individuals in addition to himself; sufficient, the government submits, to satisfy the requirements of "involve[ing] five or more participants" or "otherwise extensive" to trigger a 4 level enhancement pursuant to Section 2B1.1(a) of the Guidelines.

7. Recommendation for 15-Year Sentence

A sentence of not less than 15-years is fair and appropriate in light of several factors. First, a 15-year sentence is needed to deter Oprea from engaging in future criminal activity. Oprea seems to have been "under deterred" in the past. As noted, he has a criminal history in Romania. His prior arrests in Romania apparently only drove him further underground; they did not stop, let alone slow down, his hacking activities.

Second, a strong sentence is also needed to deter other hackers. If hackers around the world know that they can hide out safely in their home countries, remotely hack into hundreds of U.S. merchants' computers, steal hundreds of thousands of U.S. cardholder's account information out of those computers, cause over $17 million in losses, and do so with minimal punishment, then they will likely continue to engage in these crimes and injure more victims. These predators presumably already realize that it is extremely unlikely that they will be detected and criminally charged by U.S. authorities. They also undoubtedly realize that, if they are detected and charged, it is even less likely that they will then either be lured or extradited to the

U.S.[4] If, on top of that, they realize that the punishment that is ultimately meted out is fairly mild, then there is a serious risk that these predators will do a "cost-benefit" analysis and continue their crimes unabated. They will continue hacking into companies' POS systems, continue stealing cardholders' data, and continue wreaking havoc on businesses and cardholders alike. They will instead chalk up the minimal risk of apprehension and mild punishment to the "cost of doing business," and will continue their criminal conduct, undeterred.

Nevertheless, the government does not believe that a higher sentence is warranted, despite the guideline's calculation and the 35-year statutory maximum. It bears noting that over a three-year period, Oprea only made approximately $40,000. Furthermore, Oprea, virtually as soon as he was arrested, agreed to plead guilty and cooperate immediately. He gave a full confession upon his arrest, and came in for multiple proffer sessions. Oprea tried to provide as much information not only as to the charged co-conspirators but as to others involved overseas as well.

Third, the 15-year sentence is in line with other sentences handed down recently in other, similar hacking/carding prosecutions, particularly in comparison to the number of accounts that were compromised. In 2013, in the Western District of Washington, David Schrooten, 22, was sentenced to 12 years for a carding scheme involving 100,000 compromised cards and only two hacked businesses. In that case, Schrotten was the data broker, and his co-conspirator, Christopher Schroebel, 21, was the hacker. Schroebel was sentenced to seven years. Here, Oprea essentially acted in both capacities—the hacker and the data broker—and his scheme involved almost twice as many compromised cards and over a hundred more hacked businesses.

[4] Romania and other former Eastern Block countries has become a hot bed of hacking, with U.S. credit cards (with their high credit limits) as the primary targets. Oprea was the first Romanian National cyber-criminal ever extradited by Romania to the United States.

In 2012, in the Eastern District of New York, Aleksandr Suvorova was sentenced to seven years for hacking into 11 restaurants and selling 160,000 stolen cards to an undercover agent. In November 2011, also in the Eastern District of New York, Lin Mun Poo was sentenced to 10 years for a hacking and carding scheme involving 120,000 stolen credit cards. In 2012, in the Eastern District of Virginia, Peter Borgia, 22, was sentenced to four years for a carding scheme involving 21,000 stolen cards and $3 million in actual losses.

A 15-year sentence would also be in line with other sentences meted out in this case. One of Oprea's co-conspirator's, Butu, was sentenced to two years, and his other co-conspirator, Iulian Dolan has agreed to be sentenced to 7 years. Butu was merely a buyer and re-seller for Oprea, and accordingly, played a much less significant role. He had no involvement on the front-end of the conspiracy. Dolan, as set forth in his sentencing memorandum, was Oprea's right hand man, who helped primarily on the front-end.

8. Restitution

Actual restitution has not been determined. Each issuing bank whose cards were hacked and then upon which fraudulent charges were made has sustained a loss. As noted in the PSI, at paragraphs 17 & 66, 18 U.S.C. §3663A(c)(3)(A) provides that where the number of identifiable victims is so large as to make restitution impracticable, otherwise mandatory restitution need not be ordered. In this case, identifying each loss of each issuing bank has not been done because it is not as easily ascertainable as the casual observer would think. Nonetheless, Subway, the primary victim in this case, has sustained out-of-pocket losses of approximately $5 million, independent of the losses directly associated with the hacked card data. Those losses were incurred as a result of remediation efforts necessitated by the criminal scheme in which Dolan

was involved. Oprea was directly and personally responsible for hacking approximately 144,000 of the approximately 150,000 cards hacked through Subway franchises and was indirectly responsible for the 6,000 cards hacked by Dolan. Consequently, the government submits that he should be ordered to pay full restitution to Subway for it's out of pocket expenses of approximately $5 million.

8. Conclusion

The government asks the Court to sentence Oprea to the following:

- 15 years in prison;
- 3 years supervised release;
- $5 million in restitution;
- no fine, in light of the defendant's financial state and the restitution order; and,
- a $400 special assessment.

August 27, 2013

Respectfully submitted,

JOHN P. KACAVAS
United States Attorney

By: /s/ Arnold H. Huftalen
Arnold H. Huftalen
Assistant U.S. Attorney
53 Pleasant St., 4th Floor
Concord, NH 03301
(603) 225-1552
NH Bar #1215
arnold.huftalen@usdoj.gov

/s/ Mona Sedky
Mona Sedky, Trial Attorney
U.S. Dept. of Justice, Crim. Div.
950 Pennsylvania Ave. NW
Washington, DC 20530
(202) 353-4304
DC Bar #447968
mona.sedky@usdoj.gov

CERTIFICATION OF SERVICE

I certify that a copy of this Sentencing Memorandum has been served upon counsel for defendants Oprea and Dolan via ecf filing notice, and on the Probation Department via .pdf e-mail attachment.

/s/ Arnold H. Huftalen
Arnold H. Huftalen
Assistant U.S. Attorney