



U.S. Department of Justice

United States Attorney  
Eastern District of New York

JPL:MBM  
F.#2009R01925

271 Cadman Plaza East  
Brooklyn, New York 11201

October 25, 2011

By Hand Delivery

The Honorable Dora L. Irizarry  
United States District court  
Eastern District of New York  
225 Cadman Plaza East  
Brooklyn, New York 11201

Re: United States v. Lin Mun Poo  
Court Docket No. 10-891 (DLI)

Dear Judge Irizarry:

The defendant is scheduled to be sentenced on November 4, 2011. By memorandum dated October 19, 2011, the defendant objects to the applicable advisory United States Sentencing Guidelines ("Guidelines" or "U.S.S.G.") range. The defendant further argues that the Court should impose a below-Guidelines sentence because the Guideline range is calculated based upon "speculation," and based upon the factors set forth in Title 18, United States Code, Section 3553(a). (Defendant's Sentencing Memorandum ("Def. Mem.") at 1.) The government submits this letter in opposition to the defendant's memorandum.

I. Background

On April 13, 2010, the defendant pled guilty before the Court to access device fraud, in violation of 18 U.S.C. § 1029(a)(3) and (c)(1)(A)(i). (Presentence Investigation Report (hereinafter, "PSR") ¶ 1.) At his plea hearing, the defendant stipulated and allocuted that, with the intent to defraud, he knowingly possessed fifteen or more stolen credit or debit card numbers, and that he "compromised computer servers for the purpose of obtaining credit and debit card information of others, and that during this course of conduct, he compromised a computer server belonging to the Federal Reserve Bank, onto which he installed a malicious code." (Plea Agreement ¶ 2.)

The defendant's conviction stems from an investigation by the United States Secret Service into compromises of servers (also known as "hacking") which were maintained by financial

institutions, including a compromise of a server maintained by the United States Federal Reserve Bank ("Federal Reserve"). With respect to the Federal Reserve server, a malicious code had been installed onto it. The malicious code recorded users' keystrokes and stored that information in a location accessible to the defendant. (PSR ¶¶ 3-5.) Subsequently, the defendant traveled to the United States, where he met with an undercover agent, to whom the defendant sold 31 stolen credit and debit card numbers. The defendant believed that the undercover would use the data to make fraudulent withdrawals from the compromised accounts. (*Id.* at ¶¶ 5-6.) The defendant obtained the stolen numbers from his laptop computer. (*Id.* at ¶ 6.)

Upon arrest, the defendant's laptop computer from which he obtained the 31 stolen numbers was searched. (*Id.* at ¶ 9.) Approximately 122,000 additional card numbers for compromised accounts were identified on the computer. (*Id.*) In addition, numerous stored internet chats were recovered from the defendant's computer. (*Id.* at ¶ 10.) Specifically, the defendant's computer contained stored online chats from December 2008 until October 2010 in which the defendant transmitted approximately 250 credit or debit card numbers to other individuals. (Government's Objections to the PSR, dated August 3, 2011 ("Gvt. Aug. Obj.") at 2.) According to another chat, the defendant explained to a potential co-conspirator that he "provide[s] dumps," or stolen credit card information, "to my partners." The defendant then solicited this potential co-conspirator to receive the defendant's stolen debit and credit card numbers. He then asked "How many dumps [credit/debit card numbers] can you work per day? . . . Every day I provide dumps." (PSR ¶ 6; Government's Objections to the PSR, dated September 20, 2011 ("Gvt. Second Obj.") at p. 4.) In post-arrest statements, the defendant admitted that he "hack[ed] computers for money." (PSR ¶ 10.) Investigation also revealed that the defendant was a member of online forums devoted to credit card fraud, such as ShadowCrew and CarderPlanet. (PSR ¶ 10; Gvt. Aug. Obj. at p. 2.) Finally, the defendant told an undercover agent that he had "crews" of people who could make withdrawals from Automated Teller Machines ("ATMs") around the world using stolen debit and credit card information. (Gvt. Aug. Obj. at p. 7.)

## II. Guidelines Calculation

The Department of Probation calculated the defendant's adjusted offense level to be 37 and his Criminal History to be Category I, which carries an advisory Guideline range of 210 to 262 months. (PSR ¶ 34, Addendum to the PSR.) Because the statute carries a maximum penalty of 120 months, however, the

defendant's effective Guidelines range is 120 months. (PSR ¶ 72.) In relevant part, the PSR's Guideline calculation is based upon the following:

(1) pursuant to U.S.S.G. Section 2B1.1(b)(1)(M), a 24-point base offense level enhancement because the defendant possessed 122,000 stolen card numbers, resulting in a \$61,000,000 loss amount;

(2) pursuant to U.S.S.G. Section 2B1.1(b)(9)(B), a two-level enhancement for committing the crime outside the United States;

(3) pursuant to U.S.S.G. Section 2B1.1(b)(15)(B), a two-level enhancement for public dissemination of private information;

(4) pursuant to U.S.S.G. Section 2B1.1(b)(4), a two-level enhancement for receiving stolen property;

(5) pursuant to U.S.S.G. Section 3B1.3, a two-level enhancement for use of a special skill; and,

(6) pursuant to U.S.S.G. Section 2B1.1(b)(10)(B)(i) a two-level enhancement for trafficking in unauthorized access devices.

In letters dated August 3, 2011 and September 20, 2011, the defendant objected to enhancements (1) through (5). In letters dated August 3, 2011 and September 20, 2011, the government concurred that enhancement (4), the two-level enhancement pursuant to U.S.S.G. Section 2B1.1(b)(4) for receiving stolen property, should not be applied because the government is unable to prove that the defendant received stolen information from a third party. The government's calculation of the adjusted offense level is therefore 35, resulting in a Guideline range of 168 to 210 months. The effective Guidelines range is 120 months in light of the statutory maximum - the same effective Guidelines range calculated by the Department of Probation.

A. Base Offense Level

With respect to enhancement (1), the defendant contends that the base offense improperly accounts for approximately 122,000 stolen credit and debit cards numbers obtained from the defendant's computer (hereinafter, "the 122,000 stolen card numbers"). Specifically, the defendant concedes that the loss

amount attributable to the possession of stolen credit cards is \$500 per card, as set forth in U.S.S.G. § 2B1.1, Application Note 3(F)(1). (See Def. Obj. at p. 2.) The defendant argues, however, that he pleaded guilty to possessing 31 stolen card numbers, which he sold to an undercover agent. He further contends that his possession of the 122,000 stolen card numbers was unrelated to that conduct because there is insufficient evidence to establish that he intended to use the 122,000 stolen card numbers to commit fraud. (Def. Mem. at 2-5.) The defendant's argument is without merit.

As an initial matter, the defendant pleaded guilty to possessing fifteen or more stolen credit and debit card numbers in October 2010 with the intent to defraud. The defendant possessed the 122,000 stolen card numbers in October 2010 on his laptop in the Eastern District of New York. As such, the defendant's possession of the 122,000 stolen card numbers constitutes part of the offense conduct. See United States v. Feldman, 637 F.3d 450, 462-63 (2d Cir. 2011) (holding that defendant's two schemes to defraud Medicare using different facilities were "the same offense conduct" pursuant to U.S.S.G. § 1B1.3(a)(2).)

In any event, the defendant's possession of the 122,000 stolen card numbers constitutes relevant conduct pursuant to U.S.S.G. § 1B1.3(a)(2). In fraud cases, the Guidelines provide that "specific offense characteristics," such as loss amount, are based on all acts "that were part of the same course of conduct or common scheme or plan as the offense of conviction." U.S.S.G. § 1B1.3(a)(2). The relevant Application Note provides that two or more offenses are part of a "common scheme or plan" when they are "substantially connected to each other by at least one common factor, such as common victims, common accomplices, common purpose, or similar modus operandi." Id., Application Note 9(A). In addition, "[a]cts may be found to be part of the same course of conduct if the defendant engaged in a repeated pattern of similar criminal acts, even if they were not performed pursuant to a single scheme or plan." United States v. Brennan, 395 F.3d 59, 70 (2d Cir. 2005) (internal quotation marks omitted). In light of the evidence that the defendant stated that the reason he "hacked" computers was to make a profit, and his pattern of attempting to distribute stolen credit and debit card information for profit, the defendant's possession of 122,000 stolen account numbers was part of the same course of conduct to which he pleaded guilty. See Brennan, 395 F.3d at 70; see also United States v. Perdomo, 927 F.2d 111, 115 (2d Cir. 1991) ("The 'same course of conduct' concept . . . looks to whether the defendant repeats the same type of criminal activity over time. It does

not require that acts be 'connected together' by common participants or by an overall scheme." ).

The defendant now insists that Brennan and Perdomo are inapplicable to the instant case. Specifically, the defendant states that the 122,000 stolen card number do not have a sufficient "nexus" to the 31 stolen card numbers he sold to the undercover agent. (Def. Mem. at 4-5.) This is erroneous, because the 122,000 stolen card numbers were part of the defendant's long-standing scheme to steal card numbers and sell them to individuals who would pay for them, a practice also known as "carding." Not surprisingly, he maintained his stash of stolen card numbers on his computer. The defendant then retrieved 31 stolen card numbers from that computer and sold those numbers to the undercover agent.

Nevertheless, the defendant asserts that the 122,000 stolen card numbers should not be included in the Guidelines calculation because many of the numbers "were stale and expired account numbers from five or six years ago." (Def. Mem. at 3.) The defendant's argument is contrary to logic. As detailed above, the defendant obtained and possessed the 122,000 stolen card numbers during his career of hacking and carding. Thus, he possessed the card numbers with the intent to cause fraudulent withdrawals to be made from the compromised accounts. That the numbers expired or were cancelled before they could be exploited has absolutely no bearing on the defendant's intent in obtaining those stolen numbers - to use them fraudulently as part of his scheme to steal and sell stolen card numbers. The government respectfully submits that the defendant's possession of the stolen card numbers, taken together with the stored chats, the defendant's post-arrest statements and the defendant's statements to the undercover agent, rises well above the requisite preponderance of evidence. See United States v. Garcia, 413 F.3d 201, 220 n.15 (2d Cir. 2005). Moreover, the government notes the utter lack of any evidence that the defendant possessed these stolen card number for any purpose other than to commit fraud. Therefore, the PSR correctly accounted for the 122,000 stolen credit and debit card numbers in its loss calculation.

#### B. Crime Committed From Outside the United States

The defendant also claims that the enhancement for committing a substantial part of the fraudulent scheme outside of the United States, pursuant to U.S.S.G. § 2B1.1(b)(9)(B), does not apply, because the enhancement only pertains to schemes in which "the foreign location played a purposeful role," such as allowing the defendant to evade law enforcement by hiding assets

through offshore accounts. (Defendant's Objections to the PSR, dated August 3, 2011 ("Def. Obj.") at p. 2.) The defendant's unsubstantiated claim should be rejected.

The defendant's narrow reading of § 2B1.1(b)(9)(B) runs afoul of the provision's plain text, which states without caveat that the enhancement applies whenever "a substantial part of a fraudulent scheme was committed from outside the United States," making no mention of a requirement that the defendant's purpose be "to evade law enforcement." The drafters' intent to not impose such specific intent in subsection U.S.S.G. § 2B1.1(b)(9)(B) is especially clear in light of the fact that § 2B1.1(b)(9)(A) (pertaining to a relocation of a scheme) specifically does require an intent by the defendant to evade law enforcement officials.<sup>1</sup> Therefore, the defendant's unsupported contention that the foreign location "play[] a purposeful role" in the crime is meritless; the two-point enhancement pursuant to U.S.S.G. § 2B1.1(b)(9)(B) is warranted.

#### C. Dissemination of Personal Information

The defendant objects to the two-level enhancement for the defendant's public dissemination of personal information, to wit: credit and debit card information including Personal Identification Numbers ("PIN" numbers). (Def. Obj. at 2.) The defendant first alleges that there are insufficient facts to support the enhancement. The defendant is incorrect.

The enhancement is supported by the following facts, which demonstrate that the defendant's business involved disseminating personal information to the public:

(1) the defendant explained to a potential co-conspirator that he "provide[s] dumps," or stolen credit card information, "to my partners." The defendant then solicited him/her to receive the defendant's stolen debit and credit card numbers. He then asked "How many dumps [credit/debit card numbers] can you work per day? . . . Every day I provide dumps";

---

<sup>1</sup> Although there do not appear to be any published decisions on point, recent unpublished decisions support such a reading. See, e.g., United States v. Olumuyiwa, 406 Fed. Appx. 243, 244 (9th Cir. 2010) ("Subsection (B) . . . was intended to apply to defendants who are involved in a [fraudulent scheme] . . . operated from outside the United States, regardless of whether they moved overseas to evade detection or to make detection more difficult.").

(2) the defendant's computer contained stored online chats from December 2008 until October 2010 in which the defendant sent approximately 250 credit or debit card numbers to at least nine individuals;

(3) the defendant told an undercover agent that he had "crews" of people who could make withdrawals from Automated Teller Machines ("ATMs") around the world using stolen debit and credit card information;

(4) 122,000 stolen credit and debit card numbers were recovered from the defendant's computer.

The defendant next claims that such facts do not constitute "part of the offense or relevant conduct," and "the discussion of such information in a secure and exclusive chat room is not tantamount to 'public dissemination.'" (Def. Obj. at 2.) This is erroneous. The defendant's livelihood consisted of stealing credit and debit card information. Therefore, the dissemination of the stolen card numbers is "relevant" to the charged offense, since the defendant "repeat[ed] the same type of criminal activity over time." See United States v. Perdomo, 927 F.2d at 115. Moreover, the fact that the defendant made a career of distributing debit and credit card information, including PIN numbers, to individuals who would not ordinarily have had access to such information constitutes "public distribution" by its plain meaning. See United States v. Sloley, 464 F.3d 355, 359 (2d Cir. 2006) ("We follow other circuits in giving the Guidelines language its plain meaning and force.")

### III. The Defendant Should Be Sentenced Within the Applicable Guidelines Range

The defendant claims that the Guideline range is calculated based upon "speculation," and that the Court should impose a below-Guidelines sentence. The Guidelines accurately reflect the severity of the defendant's crime, and he should be sentenced within the Guidelines range.

According to Title 18, United States Code, Section 3553(a), factors to be considered by the court in sentencing the defendant include, inter alia: (1) the nature and circumstances of the offense; (2) the history and characteristics of the defendant; (3) the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law and to provide just punishment for the offense; and, (4) the need for the sentence imposed to protect the public from further crimes of

the defendant. Those factors militate in favor of a sentence within the applicable Guideline range.

A. Nature of the Offense

As detailed herein, the defendant is a skilled hacker who made a career out of compromising servers in order to obtain valuable information - information other members of the hacking and carding community wanted to purchase for exploitation. He successfully obtained more than 100,000 stolen credit card numbers through his activities. The defendant's activities were not theoretical - he participated in online carding forums, and from as early as 2008, he repeatedly sold credit card numbers to co-conspirators. Indeed, the defendant admitted to an undercover agent that he had "crews" of people waiting to exploit stolen credit and debit card data. Moreover, the defendant not only compromised servers to obtain stolen credit and debit card numbers but, by his own admission, he compromised a server for the United States Federal Reserve Bank onto which he installed a malicious code which enabled him to track the keystrokes of Federal Reserve Bank employees. The defendant's intrusion, had it not been intercepted and stopped by law enforcement, could have had devastating ramifications.

B. History of the Defendant

As described herein, the defendant made a career of compromising protected computer servers for the purpose of stealing valuable data to sell. The defendant has engaged in this activity for years - since at least 2008. Indeed, the defendant's criminal activity threatened the integrity of numerous financial institutions around the world.

C. Just Punishment

As demonstrated by the defendant's crimes, hacking and carding pose a grave threat to the integrity and soundness of financial and governmental institutions. Hackers, such as the defendant, commit their crimes in relative anonymity by using nicknames on hacking forums, such as CarderPlanet and ShadowCrew, by committing these crimes from outside the United States, and by employing "crews" of carders to perform the actual ATM transactions on their behalf. As such, the defendant was able to perpetrate his crimes over the course of several years, and he obtained a tremendous amount of stolen data from his victims.



The seriousness of the offense and the need to promote respect for the law and provide just punishment therefore militate in favor of a Guidelines sentence.

D. Protecting the Public

The defendant is a skilled computer hacker who used his training and experience to compromise protected computers. For years, he victimized banks, governmental institutions and other private companies by exploiting vulnerabilities in their systems and stealing information from their servers.

The defendant's activities extended beyond breaking into computer servers to steal protected and private information. The defendant also installed malicious code on at least one server, belonging to the United States Federal Reserve Bank. By doing so, the defendant attempted to gain significant personal data from the Federal Reserve Bank - specifically, keystrokes of its employees.

Moreover, the defendant victimized the thousands of individuals whose bank account information he stole. The defendant targeted bank account information for the purpose of exploiting it. Specifically, the defendant stole individuals' bank account information so that co-conspirators would make fraudulent withdrawals from the victims' private accounts.<sup>2</sup> To date, the defendant is accountable for possessing information for at least 122,000 compromised accounts with the intent to defraud. Consequently, the defendant poses a risk to the security of financial institutions, governmental institutions, private companies, and any individual who has a bank account.

---

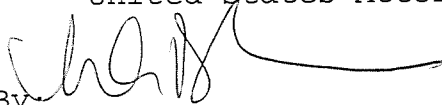
<sup>2</sup> To the extent that these compromises were detected, the banks assumed the financial responsibility for any losses.

IV. Conclusion

Based upon the foregoing, the defendant should be sentenced within the appropriate Guidelines range.

Respectfully submitted,

LORETTA E. LYNCH  
United States Attorney

By:   
\_\_\_\_\_  
Melissa B. Marrus  
Assistant U.S. Attorney  
(718) 254-6790

cc: Clerk of the Court (DLI)  
Kannan Sundaram, Esq.  
Mary Ann Betts, United States Probation Dept.