DATA BREACHES: WHAT THE UNDERGROUND WORLD OF "CARDING" REVEALS

Kimberly Kiefer Peretti
U.S. Department of Justice
Computer Crime and Intellectual Property Section

Forthcoming in Volume 25 of the
Santa Clara Computer and High Technology Journal

Data Breaches: What the Underground World of "Carding" Reveals

Kimberly Kiefer Peretti[1]

> "Cyber-crime has evolved significantly over the last two years, from dumpster diving and credit card skimming to full-fledged online bazaars full of stolen personal and financial information."[2] Brian Nagel, Assistant Director, U.S. Secret Service

Individuals have been at risk of having their personal information stolen and used to commit identity-related crimes long before the emergence of the Internet. What the Information Age has changed, however, is the method by which identity thieves can access and exploit the personal information of others. One method in particular leaves hundreds of thousands, and in some cases tens of millions, of individuals at risk for identity theft: large scale data breaches by skilled hackers. In this method, criminals remotely access the computer systems of government agencies, universities, merchants, financial institutions, credit card companies, and data processors, and steal large volumes of personal information on individuals. Such large scale data breaches have revolutionized the identity theft landscape, in particular as it relates to fraud on existing accounts by use of compromised credit and debit card account information.

Large scale data breaches would be of no more concern than small scale identity thefts if criminals were unable to quickly and widely distribute the stolen information for subsequent fraudulent use (assuming, of course, that the breach would be quickly detected). Such wide-scale global distribution of stolen information has been made possible for criminals with the advent of criminal websites, known as "carding forums," dedicated to the sale of stolen personal and financial information. These websites allow criminals to quickly sell the fruits of their ill-gotten gains to thousands of eager fraudsters worldwide, thereby creating a black market for stolen personal information.

This article first provides a brief background on large scale data breaches and the criminal "carding" organizations that are responsible for exploiting the stolen data. Second, the article provides an in-depth examination of the process by which large volumes of data are stolen, resold, and ultimately used by criminals to commit financial fraud in the underground carding world. Third, this article discusses how carding activity is linked to other crimes, including terrorism and potentially drug trafficking. Fourth, this article outlines several recent investigations and prosecutions of carding organizations

---

[1] The author is a Senior Counsel with the United States Department of Justice's Computer Crime & Intellectual Property Section (CCIPS). Her duties with the Department of Justice include prosecuting a variety of computer crime cases, focusing on those involving large scale data breaches, identity theft, and online payment systems. In particular, she co-led the prosecution of the Shadowcrew criminal organization, featured in this article. She also serves as a Council Member and Officer of the American Bar Association's Section of Science and Technology Law. The author would like to recognize Richard Downing, Assistant Deputy Chief for CCIPS, for his contributions to this article and Glenn Gordon, for his editing assistance.

[2] Press Release, U.S. Secret Service, United States Secret Service's Operation Rolling Stone Nets Multiple Arrests (Mar. 28, 2006), http://www.secretservice.gov/press/pub0906.pdf.

and the individual carders themselves. Fifth, this article examines the responses by the credit card industry and state legislatures to the recent increase in reported data breaches. Finally, this article outlines several recommendations to enhance the government's ability to continue to successfully prosecute carders and carding organizations.

I. Introduction

A. Large Scale Data Breaches

The term "data breach" is generally and broadly defined to include "an organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers, or financial information such as credit card numbers."[3] Since 2005, there has been a rash of reported high-profile data breaches involving the compromise of large volumes of personal information.[4] This rash began with the reported compromise of 163,000 financial records of consumers from the computer systems of a large consumer data broker, Choicepoint Inc., in February 2005.[5] Choicepoint's security breach became public after it notified approximately 35,000 California consumers pursuant to California law that it may have disclosed their personal records.[6]

The California law at issue had been passed in 2003, making it the first state to enact legislation requiring consumer notification in the event of a security breach involving the unauthorized acquisition of personal information.[7] In response to the increased fears of identity theft resulting from these publicized breaches, a majority of states have since followed California's lead and passed security breach notification laws.[8]

Often, large scale data breaches involve the compromise of personal financial information, such as credit or debit card account information, rather than other types of personally identifiable information, such as Social Security numbers.[9] Three of the larger, more highly publicized data breaches in recent years, including DSW, Inc.,[10]

---

[3] U.S. GOV'T ACCOUNTABILITY OFFICE, Report to Congressional Requesters, GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 2 (2007), available at http://www.gao.gov/new.items/d07737.pdf [hereinafter GAO Report]

[4] According to one estimate, more than 217 million records have been compromised since early 2005. Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm#Total (last visited Mar. 6, 2008).

[5] Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief, United States v. Choicepoint, Inc., No. 1:06-cv-00198-JTC (N.D. Ga. 2006), available at http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf.

[6] *Id*. at 4.

[7] Cal. Civ. Code §§ 1798.29 and 1798.82 (effective July 1, 2003) (the data breach notification legislation is known as "S.B. 1386").

[8] For a comparison of these laws, *see* ANNE P. CAIOLA ET AL,, U.S. DATA BREACH NOTIFICATION LAW: STATE BY STATE (John P. Hutchins ed., ABA Publishing 2007).

[9] GAO Report, *supra* note 3, at 30.

[10] DSW, Inc., FTC File No. 053-3096 (Mar. 14, 2006). DSW is a retail shoe warehouse. The FTC alleged that DSW stored personal information from the magnetic stripes of credit and debit cards on its computer

CardSystems Solutions, Inc.,[11] and TJX Companies, Inc.,[12] have involved the compromise of millions of credit and debit card account information. In these cases, hackers targeted the credit and debit card account information held by merchants or third party data processors as the result of credit and debit card retail transactions.

The compromise of credit and debit card account information most often results in the type of identity theft referred to as "account takeover," which involves fraud on existing financial accounts.[13] Account takeovers occur, for example, when a criminal uses a stolen credit card number to make fraudulent purchases on an existing credit line. Account takeovers are the more common type of identity theft, in contrast to a second type of identity theft referred to as "new account creation."[14] New account creations involve the fraudulent creation of new accounts, for example, when a criminal uses stolen data to open a bank or credit card account in someone else's name.[15] Often, in order to engage in this type of identity theft, the criminal must steal more personal information than merely credit and debit account information.[16]

---

networks, and failed to take reasonable security measures to protect this sensitive customer data. *Id*. DSW responded by issuing press releases that transaction information involving 1.4 million credit cards was stolen from DSW customers who shopped at certain stores between November 2004 and February 2005. Press Release, DSW, DSW Releases Findings from Fraud Investigation into Credit Card and Other Purchase Information Theft (Apr. 18, 2005), http://www.dswshoe.com/ccpressrelease/pr/CCAprilUpdate.html.

[11] CardSystems Solutions, Inc., FTC File No. 052-3148 (Feb. 23, 2006), available at http://www.ftc.gov/os/caselist/0523148/0523148CardSystemscomplaint.pdf. CardSystems is a payment card processor that provides merchants with authorization services for approving credit and debit card purchases. The FTC alleged that CardSystems stored magnetic stripe data on its computer systems and failed to take reasonable security measures to protect this data. *Id*. The complaint specifically alleged that, in September 2004, hackers exploited a vulnerability in CardSystem's security system and stole the magnetic stripe data for tens of millions of credit and debit cards. *Id*. at 2. According to CardSystem's CEO, however, the forensic analysis revealed only that 239,000 discrete account numbers had been exported from the system. Statement of John M. Perry, President and CEO, CardSystems Solutions, Inc., Before the U.S. House of Rep. Subcom. On Oversight and Investigations of the Com. on Financial Services, Hearing on "Credit Card Data Processing: How Secure Is It?, Wash. D.C., July 21, 2005, at 10 [hereinafter Statement of Perry].

[12] On January 17, 2007, TJX, the parent company of T.J. Maxx, Marshalls, HomeGoods, and other retail stores, reported an unauthorized intrusion into its computer systems potentially exposing credit and debit card account information on customers. News Release, TJX Companies, Inc., The TJX Companies, Inc. Victimized by Computer Systems Intrusion (Jan. 17, 2007), https://www.home-savings.com/files/tjxalert.pdf. TJX initially identified 45.7 million credit and debit cards that had been compromised. Amended Consolidated Class Action Complaint at 3, *In Re:* TJX Companies Retail Security Breach Litigation, No. 1:07-cv-10162-WGY (D. Mass. Jan. 9, 2008). That number, however, grew to over 94 million affected accounts. Ross Kerber, *Details Emerge on TJX Breach*, BOSTON GLOBE, Oct. 25, 2007, at E1, available at http://www.boston.com/business/globe/articles/2007/10/25/details_emerge_on_tjx_breach/. TJX is currently subject to several class action lawsuits on behalf of both customers and financial institutions who suffered fraud losses as a result of the breach. *In Re:* TJX Companies Retail Security Breach Litigation, No. 1:07-cv-10162-WGY (D. Mass. notice of appeal filed Jan. 17, 2008).

[13] GAO Report, *supra* note 3, at 9 and 30.

[14] *Id*. at 9.

[15] *Id*. at 2.

[16] *Id*. at 6. According to federal law enforcement, "identity theft involving the creation of new accounts often results not from data breaches, but from other sources, such as retrieving personal information by sifting through a family's household trash." *Id*. at 22.

Accordingly, if individuals suffer any harm as a result of a large scale data breach, that harm is most likely to be in the form of unauthorized use of a debit or credit card on an existing account.[17] This harm often results in little or no economic loss for the individual because consumer liability for unauthorized credit and debit card use is limited by law (in most cases to $50).[18] Nonetheless, the individual may suffer significant non-monetary losses such as invasion of privacy, inconvenience, and reputational damage.

Moreover, the economic loss for both the financial institutions issuing payment cards and the corporate entities from which cardholder account information is stolen is significant. Issuing financial institutions may experience three types of losses, including "(1) costs associated with reissuing new payment cards, (2) costs associated with monitoring open accounts for fraud (with or without reissue), and (3) fraud losses."[19] Merchants, data processors and other companies suffering from the breach, in turn, face significant losses in the form of lawsuits,[20] credit card association fines, customer notification costs, stock price decline, lost business, and loss of existing customer confidence.[21] In the TJX data breach, for example, such costs amounted to $256 million for the victim company.[22]

The process by which large volumes of data are stolen, resold, and ultimately used by criminals to commit fraud is revealed in an underground world known as "carding," discussed below.

B. Background on Carding

---

[17] *See id*. at 26, t. 1. Indeed, evidence suggests that most recent data "breaches have not resulted in detected incidents of identity theft." *Id*. at 5.

[18] Federal law limits consumer liability for unauthorized credit card charges to a maximum of $50 per account. 15 U.S.C. § 1643 (2007). However, credit card companies and most credit card issuers have a "zero liability" policy that waives these limits. *See, e.*g., MasterCard, Guide to MasterCard Card Benefits, http://www.mastercard.com/us/personal/en/cardholderservices/guidetobenefits/index.html (last visited Mar. 6, 2008) (A cardholder whose account is in good standing, who exercises reasonable care in safeguarding the card, and who has not reported two or more unauthorized events in the past twelve months, is not responsible for unauthorized charged made to the account).

With respect to ATM and debit card transactions, under the Electronic Funds Transfer Act, 15 U.S.C. § 1693 *et seq.*, and its implementing Regulation E, 12 C.F.R. Part 205, consumer liability for unauthorized use of a lost or stolen card is generally limited to between $50 and $500. 15 U.S.C. § 1693g (2007); 12 C.F.R. §205.6 (2007).

[19] Declaration of Joel S. Lisker at 11, *In Re:* TJX Companies Retail Security Breach Litigation, No. 1:07-cv-10162-WGY (D. Mass. .Oct. 26, 2007) [hereinafter Declaration of Lisker].

[20] Merchants and processors face class action lawsuits from both consumers and issuing financial institutions. *See* Erin Fonte, *Who Should Pay the Price for Identity Theft?*, 54 FED. LAWYER, 24 (2007).

[21] A recent study suggests that the total average cost to the victim of a data breach in 2007 was $197 per record (or, in the case of financial services companies, $239 per record). PONEMON INSTITUTE, 2007 ANNUAL STUDY: U.S. COST OF A DATA BREACH, at 8 and 15 (2007). The total cost includes costs associated with detecting the breach, reporting the breach, notifying customers, and lost business. *Id.* at 7.

[22] Ross Kerber, *Cost of Data Breach at TJX Soars to $256m*, BOSTON GLOBE, Aug. 15, 2007, at A1, available at http://www.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/.

In its narrow sense, the term "**carding**" refers to the unauthorized use of credit and debit card account information to fraudulently purchase goods and services.[23] The term has evolved in recent years, however, to include an assortment of activities surrounding the theft and fraudulent use of credit and debit card account numbers including computer hacking, phishing, cashing-out stolen account numbers, re-shipping schemes, and Internet auction fraud.[24] Individuals engaged in criminal carding activities are referred to as "**carders**."[25]

In contrast to other types of identity theft, carding involves the large scale theft of credit card account numbers and other financial information.[26] Other types of common methods that criminals use to steal personal information include dumpster diving,[27] skimming,[28] phishing,[29] change of address, and "old-fashioned stealing."[30] In each of these methods, the number of victims rarely exceeds several hundred or, in rare cases, a few thousand. Carding, on the other hand, often involves thousands of victims, and in some cases, millions.

Carders are often members of one or more websites known as "**carding forums**" that facilitate the sale of, among other contraband, stolen credit and debit card numbers,

---

[23] *See, e.g.*, Affidavit in Support of Application for Criminal Complaint and Arrest Warrant at 11, United States v. Jacobsen, No. 2:04-cr-01619-GHK-ALL (C.D. Cal. 2006), available at http://www.infosecinstitute.com/blog/jacob2.pdf (describing "carding" as "purchasing retail items with counterfeit credit cards or stolen credit card information") [hereinafter Jacobsen Affidavit].

[24] Indictment at 2, United States v. Warren, No. 3:06-cr-00372-HEH-1 (E.D. Va. 2007) [hereinafter Warren Indictment], available at http://blog.washingtonpost.com/securityfix/Filed%20Indictment%20%28Dana%20Warren%29.pdf

[25] Warren Indictment, *supra* note 24, at 2.

[26] Affidavit in Support of Arrest Warrant at 6, United States v. Vega, No. 1:07-mj-00942-KAM-1 (E.D.N.Y. Aug. 24, 2007) (referring to "carders" as "thieves who steal large volumes of credit card information and sell it") [hereinafter Vega Affidavit].

[27] Dumpster diving involves rummaging through garbage cans or trash bins to obtain copies of checks, credit card or bank statements, or other records that contain personally identifiable information such as name, address, and telephone number, and using this information to assume a person's identity. U.S. Dep't of Justice, Identity Theft and Identity Fraud, http://www.usdoj.gov/criminal/fraud/websites/idtheft.html. (last visited Mar. 6, 2008).

[28] Skimming involves the use of an electronic storage device by criminals to read and record the encoded data on the magnetic stripe on the back of a credit or debit card. Typical examples of such use involve rogue employees at restaurants that swipe a patron's card in the skimming device prior to swiping it through the restaurant's own card reader or attaching the skimming device to an ATM. THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN 18 (2007), available at http://www.idtheft.gov/reports/StrategicPlan.pdf [hereinafter Combating Identity Theft].

[29] Phishing attacks involve the use of 'spoofed' emails to "lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond." Anti-Phishing Working Group, APWG Home Page, http://www.apwg.org/. (last visited Mar. 6, 2008). Phishing attacks can also involve the use of technical subterfuge schemes that plant malicious code, such as Trojan keylogger spyware, onto an individual's computer without the individual's awareness and steal personal information directly. *Id.*

[30] Such traditional methods include, for example, stealing wallets and purses, bank and credit card statements and pre-approved credit offers from mail, and personnel records from employers. Federal Trade Commission, Fighting Back Against Identity Theft, http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.shtm. (last visited Mar. 6, 2008).

compromised identities, and false identifications.[31] Examples of such sites, described in detail below, are www.shadowcrew.com, www.carderplanet.com, www.CCpowerForums.com, www.theftservices.com, and www.cardersmarket.com. These forums generally provide some or all of the same services, including:

- Tutorials on different types of carding-related activities;
- Private and public message posting enabling members to buy and sell blocks of stolen account information and other goods and services;
- Hyperlinks for hacking tools and downloadable computer code to assist in network intrusions;
- Other exploits such as source code for phishing webpages;
- Lists of proxies;[32]
- Areas designated for naming and banning individuals who steal from other members.[33]

Carding forums also often share a common pattern of organization, as discussed in detail below.

i. Shadowcrew

The Shadowcrew criminal organization was a global organization of thousands of members that was dedicated to promoting and facilitating the electronic theft of personal identifying information, credit card and debit card fraud, and the production and sale of false identification documents.[34] The organization operated and maintained the Internet website www.shadowcrew.com from 2002 until October 2004, when it was taken down by the U.S. Secret Service ("USSS") as the result of a year-long undercover investigation known as "Operation Firewall."[35]

Shadowcrew was operated as a members-only communications medium to facilitate the commission of their criminal activities.[36] Shadowcrew members gained

[31] Vega Affidavit, *supra* note 26, at 6.
[32] The term "proxies" refers to a proxy server, which is a computer that allows other computers to make indirect network connections through it to other networked computers. A proxy server provides criminals with a launch pad from which the criminal can electronically navigate on the Internet without revealing the true IP address of the criminal's computer, thereby significantly complicating an investigator's ability to identify the criminal. Indictment at 6, United States v. Hale, No. 3:06-cr-00360-HEH-1 (E.D. Va. 2007), available at http://blog.washingtonpost.com/securityfix/Filed%20Indictment%20%28Dana%20Warren%29.pdf [hereinafter Hale Indictment].
[33] Warren Indictment, *supra* note 24, at 7.
[34] Indictment at 2, United States v. Mantovani, No. 2:04-cr-00786-WJM-1 (D.N.J. 2006) [hereinafter Shadowcrew Indictment]. Although statements in indictments are only allegations, because all of the domestic targets of the Shadowcrew Indictment pled guilty, as discussed below, the factual bases for their pleas necessarily supports the truth of the statements alleged.
[35] Shadowcrew Indictment, *supra* note 34, at 2, 6; Press Release, U.S. Dep't of Justice, Shadowcrew Organization Called 'One-Stop Online Marketplace for Identity Theft' (Oct. 28, 2004), http://www.usdoj.gov/criminal/cybercrime/mantovaniIndict.htm [hereinafter Shadowcrew Press Release].
[36] Shadowcrew Indictment, *supra* note 34, at 2.

access to the website by typing in their chosen online screen name and password at the login screen for the web site.[37] Individuals often were known by, and conducted their criminal business under, more than one online name.[38]

Once they had logged into the website, Shadowcrew members were able to anonymously conduct their criminal activity through their chosen nicknames by posting messages to various forums within the website and sending and receiving secure private messages to each other via the website.[39] The messages posted to various forums, among other things, provided guidance to Shadowcrew members on producing, selling and using stolen credit card and debit card information and false identification documents.[40] The sole purpose of the Shadowcrew website was to promote and facilitate the commission of criminal activity.[41]

The Shadowcrew criminal organization oversaw the activities of its membership through a hierarchical framework that included the following roles:

- a small group of "**administrators**" who served as a governing council of the criminal organization;
- "**moderators**" who oversaw and administered one or more subject-matter-specific forums on the website that either fell within an area of their expertise or covered their geographic location;
- "**reviewers**" who examined and/or tested products and services that members of the criminal organizations desired to advertise and sell;
- "**vendors**" who advertised and sold products and services to members of the criminal organizations via the website after the product or service had received a favorable written review from a reviewer; and
- "**general members**" who used the web sites to gather and provide information about perpetrating criminal activity and facilitate their purchases of credit card numbers, false identification documents and other contraband.[42]

Shadowcrew members collectively trafficked in at least 1.5 million stolen credit card numbers that resulted in over $4 million in actual losses to credit card companies and financial institutions.[43] The prosecution of the top-tier members of the Shadowcrew criminal organization as the result of Operation Firewall is discussed in more detail below in Section III.A.

ii. Other carding organizations.

[37] Shadowcrew Indictment, *supra* note 34, at 3.
[38] Shadowcrew member Andrew Mantovani, for example, was known to other members in the organization as "Deck," "d3ck," "BlahBlahBlhSTFU," "DeckerdIsMissin," and "ThnkYouPleaseDie." *Id*. at 1.
[39] *Id*. at 3.
[40] *Id*. at 3.
[41] *Id*. at 3.
[42] *Id*. at 4-6.
[43] *Id*. at 3.

Other carding forums supporting separate criminal organizations have been in operation in the past several years. Prior to October 2004, the primary carding forums included Shadowcrew and Carderplanet. After the October 2004 takedown of the Shadowcrew website, several new forums were created, including for example, the International Association for the Advancement of Criminal Activity (IAACA), which later became the Theft Services, CardersMarket, and CCpowersForum.[44] By 2006, there were approximately a dozen other criminal organizations similar to Shadowcrew.[45] Often, the forums attracted thousands of members. In 2007, two of the largest carding forums together had nearly 20,000 member accounts.[46] Several such carding organizations that resemble the (now defunct) Shadowcrew criminal organization in nature, form, and purpose include:

- *Carderplanet*: The Carderplanet organization operated and maintained the website www.carderplanet.com for its criminal activities and was founded in May 2001.[47] By August 2004, the site had attracted more than 7,000 members.[48] The site provided its members with a marketplace for millions of stolen accounts.[49] Although most of the postings on the forum were in Russian, and most of Carderplanet members were from Eastern Europe and Russia, the forum had a significant English-speaking component.[50] The Carderplanet criminal organization was organized similar to the mafia with the highest ranking members, or "the family," having titles such as the Godfather and "capo di capi" (or boss of all bosses).[51] Senior members of the organization shut the website down in the summer of 2004 following some arrests of high-ranking members and law enforcement scrutiny.[52]

- *IAACA and Theft Services*: The International Association for the Advancement of Criminal Activity (IAACA) operated and maintained the website www.iaaca.com

[44] Shadowcrew "established the standard for cybercrime forums – set up on well-designed, interactive Web pages and run much like a well-organized coop … Shadowcrew's takedown became the catalyst for the emergence of forums as they operate today." Byron Acohido and Jon Swartz, *Cybercrime Flourishes in Online Hacker Forums*, USA TODAY.COM, Oct. 11, 2006, http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-10-11-cybercrime-hacker-forums_x.htm [hereinafter Cybercrime Flourishes in Hacker Forums].
[45] Michael Crawford, *Card Fraudsters: A World unto Themselves*, COMPUTERWORLD, May 30, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9000808&source=rss_topic82 [hereinafter Card Fraudsters].
[46] Combating Identity Theft, *supra* note 28, at 20.
[47] Jacobsen Affidavit, *supra* note 23, at 3, 6; Card Fraudsters, *supra* note 45.
[48] Card Fraudsters, *supra* note 45.
[49] Cassell Bryan-Low, *As Identity Theft Moves Online, Crime Rings Mimic Big Business*, WALL ST. J., July 13, 2005, at A1, available at http://online.wsj.com/article/SB112121800278184116.html?mod=article-outset-box [hereinafter As Identity Theft Moves Online].
[50] Cassell Bryan-Low, *Ukraine Captures Key Suspect Tied to Identity Theft*, WALL ST. J., July 19, 2005, at B9 [hereinafter Ukraine Captures Key Suspect].
[51] *Meet the Hackers*, BUS. WK., May 29, 2006, at 58, available at http://www.businessweek.com/magazine/content/06_22/b3986093.htm [hereinafter Meet the Hackers]; As Identity Theft Moves Online, *supra* note 49.
[52] *Id*.

for its criminal activities and was founded after the takedown of the Shadowcrew website. [53] The forum was loosely-knit and brought together hackers, identity thieves, and financial fraudsters, all dedicated to trafficking in stolen financial and personal data.[54] In the fall of 2005, the site was reorganized and began to operate under the name The Theft Services.[55] One of the forum's administrators, allegedly a former technology student in Russia, was known online as "Zo0mer."[56]

- *Cardersmarket*: The Cardersmarket organization allegedly operated and maintained the website www.cardersmarket.com for its criminal activities and was founded in June 2005.[57] Similar to other carding forums, Cardersmarket was allegedly dedicated to the unlawful acquisition, use and/or sale of unauthorized credit card account information, and other personal identification and financial information.[58] As of September 5, 2007, Cardersmarket allegedly had thousands of members worldwide.[59] In August 2006, the forum's administrator, known by the nickname "Iceman," allegedly took over four rival carding forums and thereby increased the Cardersmarket membership to 6,000.[60]

- *CCpowerForums*. The CCpowerForums organization operated and maintained the website CCpowerForums.com and allegedly had thousands of users dedicated to facilitating criminal carding activity.[61] Similar to other carding forums, the CCpowerForums website allegedly offered "multiple forums in which users [could] discuss and engage in criminal carding activity" including forums entitled "hacking, exploits, proxies, Trojans/keyloggers/bots, [and] credit cards."[62]

c. Types of information for sale on carding sites.

To engage in carding on these websites, members advertise their products and services by posting messages to various informational and discussion forums. Such products and services advertised on the Shadowcrew website, for example, included "stolen credit card and bank account information, and other stolen individual identifying

---

[53] Tom Zeller Jr., *Black Market in Stolen Credit Card Data Thrives on Internet*, N.Y. TIMES, June 21, 2005, at A1, available at http://www.nytimes.com/2005/06/21/technology/21data.html [hereinafter Black Market in Stolen Data].
[54] Meet the Hackers, *supra* note 51.
[55] Meet the Hackers, *supra* note 51; INFOWATCH, INFOWATCH: IDENTITY THEFT CLOSER THAN YOU THINK, http://www.infowatch.com/threats?chapter=162971949&id=183934175 (last visited Mar. 6, 2008) [hereinafter InfoWatch].
[56] Meet the Hackers, *supra* note 51; InfoWatch; Tom Zeller Jr., *Countless Dens of Uncatchable Thieves*, N.Y. TIMES, Apr. 3, 2006, at C3, available at http://www.nytimes.com/2006/04/03/business/03link.html?pagewanted=print [hereinafter Countless Dens].
[57] Indictment at 2-3, United States v. Butler, No. 2:07-cr-00332-MBC-1 (W.D. Pa. Sept. 17, 2007) [hereinafter Butler Indictment].
[58] *Id*. at 1.
[59] *Id*. at 2-3.
[60] Cybercrime Flourishes in Hacker Forums, *supra* note 44.
[61] Hale Indictment, *supra* note 32, at 6.
[62] Hale Indictment, *supra* note 32, at 6-7.

information, counterfeit passports, drivers' licenses, Social Security cards, credit cards, debit cards, birth certificates, college student identification card, health insurance cards and other false identification documents."[63] To conceal their activity, carders have adopted a set of vernaculars when advertising their products and services in various posts on the carding websites.

One of the products frequently for sale is the "**dump,"** which generally refers to information electronically copied from the magnetic stripe on the back of credit and debit cards.[64] In the credit card industry, this information is referred to as "full-track data," referencing the two tracks of data (Track 1 and Track 2) on the magnetic stripe.[65] Track 1 is alpha-numeric and contains the customer's name and account number.[66] Track 2 is numeric and contains the account number, expiration date, the secure code (known as the **CVV**),[67] and discretionary institution data.[68] Dumps, which appeared for sale on carding forums in 2002,[69] typically contain at least Track 2 data, but often contain both Track 1 and 2.[70] Carders also refer to **BINs**[71] and **PINs**[72] in the course of selling dumps.

---

[63] Shadowcrew Indictment, *supra* note 34, at 9.
[64] Warren Indictment, *supra* note 24, at 3.
[65] VISA INC., VISA FRAUD INVESTIGATIONS AND INCIDENT MANAGEMENT PROCEDURES: WHAT TO DO IF COMPROMISED 16 (2007), available at http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf?it=r|/merchants/risk_management/cisp_if_compromised.html [hereinafter Visa Procedures].
[66] *Id*. at 17.
[67] Warren Indictment, *supra* note 24, at 3. The term CVV is an acronym used the credit card industry to refer "card verification value." Visa Procedures, *supra* note 65, at 15. (To add to the confusion, Mastercard's term is CVC, or "card validation code.") There are two different types of CVV, each of which provides an additional fraud protection layer for different types of transactions: CVV (or CVV1), which is a unique three-digit value encoded on the magnetic stripe of the card, and CVV2, which is the three-digit value that is printed on the back of all payment cards. Visa Procedures, *supra* note 65, at 15.

CVV (or CVV1) assists in fraud detection for face-to-face retail transactions (known in the credit card industry as "card present" transactions) in that it must be verified online by the credit card issuer at the same time a transaction is authorized. Visa Procedures, *supra* note 65, at 15. Vega Affidavit, *supra* note 26, at 4-5. From the carder's perspective, therefore, in order to engage in card present transactions, he/she must possess not only the card number on the face of the card, but also the CVV encoded on the stripe. Vega Affidavit, *supra* note 26, at 4-5.

CVV2 assists in fraud detection for "card not present" transactions (*i.e.*, sales transactions that take place over the Internet or by telephone) by ensuring that the customer actually has the physical card (because the CVV2 is printed on the back) when making a purchase. Card not present merchants are required to ask the customer for the CVV2 value and submit it as part of their authorization request. Visa Procedures, *supra* note 65, at 15.
[68] Visa Procedures, *supra* note 65, at 17.
[69] U.S. Secret Service, Presentation, https://www.apparelandfootwear.org/UserFiles/File/Presentations/USSS_Data_Security_Presentation.ppt. Prior to dumps, in the late 1990s, the stolen financial information available on carding forums was simply the card number, expiration date, and cardholder name and address. *Id*. In the early 2000s, CVV data was added to the mix. *Id*.
[70] Warren Indictment, *supra* note 24, at 3.
[71] The term "BIN" is an acronym used in the credit card industry to refer to "bank identification number." Each bank that issues credit cards is issued a unique BIN. The first six digits of any valid credit card number is this unique BIN of the bank that issued the card number. Visa Procedures, *supra* note 65, at 15. Carders are interested in BINs because they allow them to identify and target more vulnerable financial

In more recent years, carders have introduced a new product known as "full-infos" that contain more personally identifiable information on individuals than dumps.[73] "**Full Info**" or "**Fulls**" is a carding term that refers to a package of data about a victim, including for example address, phone number, social security number, credit or debit account numbers and PINs, credit history report, mother's maiden name, and other personal identifying information.[74]

In addition to providing a forum for the online trading of stolen account information, carding forums also provide a forum for trading in a variety of counterfeit identification documents. In fact, many of the early carders belonged to, and met each other through, a (now defunct) forum called "Counterfeit Library," which was an informational and discussion bulletin board dedicated to the sale of fraudulent identification documents.[75] Examples of the types of counterfeit documents for sale on the carding forums include counterfeit passports, drivers' licenses, Social Security cards, credit cards, debit cards, birth certificates, college student identification cards, health insurance cards, bills, diplomas, or anything that can be used as an identity document.[76] Carders often refer to these fraudulent identification documents simply as "**IDs**"[77] or "**novs**." The term "nov" (short for novelty) was originally adopted by carders in an attempt to appear to be engaged in the legitimate activity of producing documents for novelty purposes.[78]

As indicated above, the types of information for sale on carding forums has evolved from the sale of a few pieces of sensitive information, such as credit card numbers and expiration dates, to full blown identity packages containing multiple types of sensitive personal information. Indeed, the pricing reflects the evolving nature of information available on the forums, with more readily available information priced lower than information that is harder to obtain. In the first half of 2007, for example, credit card information ranged from $0.50 to $5.00 per card, bank account information ranged from $30.00 to $400.00, and full identity information ranged from $10 to $150.[79]

---

institutions, and spread thefts across a wide range of institutions. Vega Affidavit, supra note 26, at 4, n. 2. Often, carders will advertise "BIN lists" for sale.

[72] The term "PIN" refers to "personal identification numbers" and is used in the credit card industry as a means of cardholder identification. Visa Procedures, *supra* note 65, at 17. PIN is also a carding term of art indicating a credit card or debit card for which the personal identification number has also been obtained, allowing for direct cash withdrawals. Warren Indictment, *supra* note 24, at 6. For a detailed discussion of PIN cashing, *see* Section II.B.iii below. Often, carders will advertise "dumps with PINs" for sale.

[73] *Id*.

[74] Warren Indictment, *supra* note 24, at 4. Unlike purchasers of dumps, purchasers of fulls use the information to either take over or sell the identity of another person. *Id*.

[75] Kim Zetter, *Tightening the Net on Cybercrime*, WIRED MAGAZINE, Jan. 31, 2007, http://www.wired.com/politics/onlinerights/news/2007/01/72581.

[76] Shadowcrew Indictment, *supra* note 34, at 9; Warren Indictment, *supra* note 24, at 5.

[77] Warren Indictment, *supra* note 24, at 5.

[78] Jacobsen Affidavit, *supra* note 23, at 12.

[79] SYMANTEC CORPORATION, Volume XII, SYMANTEC INTERNET THREAT REPORT, TRENDS FOR JANUARY – JUNE 2007 13 (2007), available at http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf . Carders typically advertise in bulk

II. Credit and Debit Card Fraud

A. Obtaining the Information to Sell

There are several methods by which carders obtain the stolen financial account information to resell on the carding forums. Most often, carders purchase the information in bulk from hackers, [80] who steal it from entities that hold large amounts of financial account information, including credit card service providers and data processors,[81] financial institutions,[82] merchants,[83] restaurants and government agencies.[84] The compromise of such computer systems allows hackers to obtain large quantities of financial account information, often on millions of potential victims.

A second method by which carders obtain the financial account information on large numbers of individuals is phishing.[85] Indeed, the carding forums often provide assistance to carders on phishing in the form of "how to" tutorials and selling pre-built kits that allow carders to set up fraudulent web sites within minutes.[86] Carders with hacking skills also engage in phishing that targets vulnerable computers of individual cardholders.[87] This occurs, for example, by infecting the computers with data-mining viruses or other types of malicious code.[88]

B. Types of Carding

Once the stolen information is obtained, vendors advertise their product or service by posting a message on the carding forum. The vendor then arranges for the particular

---

rates. In the first six months of 2007, common bulk amounts included: 10 credit card numbers for $20; 50 credit card numbers for $70; and 100 credit card numbers for $100. *Id.* at 13.

[80] Jacobsen Affidavit, *supra* note 23, at 10; Vega Affidavit, *supra* note 26, at 5, n.4.

[81] *See* Vega Affidavit, *supra* note 26, at 5; Butler Indictment, *supra* note 57, at 2. *See also* John J. Brady, Vice President, Merchant Fraud Control, MasterCard International, Fighting Fraud: Improving Information Security, Testimony Before the Subcommittee on Financial Institutions and Consumer Credit and the Subcommittee on Oversight and Investigations of the House Financial Services Committee 5 (Apr. 3, 2003,) (transcript available at http://www.iwar.org.uk/ecoespionage/resources/fraud/040303jb.pdf) (discussing the unauthorized access to computer systems at Data Processing International which potentially exposed approximately 10 or 11 million credit card account numbers and expiration dates). In this regard, one of the well known carders, Roman Vega, bragged to another carder about being responsible for the hack of DPI. *See* Vega Affidavit, *supra* note 26, at 21.

[82] *See* Butler Indictment, *supra* note 57, at 2.

[83] *See, e.g.*, the TJX data breach, discussed in note 12, *supra*.

[84] For example, on the Carderplanet website, discussed in Section I.B.ii *supra*, many of the stolen accounts originated from compromised systems of banks, e-commerce sites and government agencies. As Identity Theft Moves Online, *supra* note 49. *See also* GAO Report, *supra* note 3.

[85] *See* note 29, *supra*, for an explanation of phishing. Phishing is also referred to as "spamming" by carders. Hale Indictment, *supra* note 32, at 5.

[86] Brian Krebs, *14 Arrested for Credit Card, Phishing Scams*, WASHINGTONPOST.COM, Nov. 3, 2006, http://blog.washingtonpost.com/securityfix/2006/11/14_arrested_for_credit_card_ph_1.html. [*See also* Hale or Warren indictment]

[87] Vega Affidavit, *supra* note 26, at 5.

[88] Vega Affidavit, *supra* note 26, at 5, n. 4.

sale with the purchaser through instant messaging or private email.[89] The carder purchasing the stolen information, in turn, typically uses the information to engage in one of four types of credit or debit card fraud, referred to in the criminal underworld as "carding online," "in-store carding," "cashing," and/or "gift card vending."

i. Carding online

"**Carding online**" simply refers to using stolen credit card information to make purchases of goods and services online from merchants.[90] As stated above, in the credit card industry, these types of transactions fall under the umbrella term of "card not present" transactions. In order to deter fraud for card not present transactions, credit card companies have added a second card verification value on the back of the card, known as the CVV2, which online (and telephone) retailers are usually required to submit as part of the authorization process.[91] As a result, the carder must often possess not only the dump, but also the CVV2, in order to engage in online carding. As a result, dumps with CVV2 are more valuable to carders and more difficult to obtain.[92]

To avoid detection, carders that purchase goods online have the goods sent to a physical address other than their own, such as a mail drop.[93] This process is known in the carding world as "**carding to a drop.**"[94] Alternatively, the carder has the merchandise shipped to a third party with whom the carder has a pre-existing relationship to share in the future proceeds from the sale of the merchandise by the third party.[95]

Carders that engage in online carding and carding to a drop may also need the services of someone who provides "**COBs**" or "change of billing" services. COB services involve accessing the victim's credit card account online or via the telephone after obtaining all relevant information related to the victim's account and causing the billing address to be changed to match a new shipping address (*e.g.*, the drop address) or adding an additional shipping address (*e.g.*, the drop address).[96] Because many online retailers will only ship large items if the billing and shipping addresses match,[97] COB services increased the probability that the stolen credit card account will not be rejected

[89] Vega Affidavit, *supra* note 26, at 12.
[90] Jacobsen Affidavit, *supra* note 23, at 11.
[91] Visa Procedures, *supra* note 65, at 15. *See also Hacking for Profit: Credit "Carding" Exposed*, Secure Science Corporation, Mar.16, 2007, at 9 [hereinafter Hacking for Profit].
[92] Hacking for Profit, *supra* note 91, at 9.
[93] In the criminal world, the term "drop" refers to "[a]n intermediary location used to disguise the source or recipient of a transaction (physical address, email address, bank account, *etc.*)" Warren Indictment, *supra* note 24, at 3. Drops are usually opened with false identification documents.
[94] Jacobsen Affidavit, *supra* note 23, at 11.
[95] Jacobsen Affidavit, *supra* note 23, at 11-12.
[96] Jacobsen Affidavit, *supra* note 23, at 12. A carder offering COB services is "offering fresh bank or credit card accounts, along with the ability to change the billing address through a pilfered PIN. In other cases, a vendor selling cobs is offering to change billing addresses himself." Black Market in Stolen Data, *supra* note 53.
[97] Hacking for Profit, *supra* note 91, at 16.

for Internet transactions, thereby ensuring that the carder is able to entirely takeover the compromised account.[98]

ii. In-store carding

A second form of carding is "**in-store carding**," which refers to the process of presenting a counterfeit credit card that had been encoded with stolen account information to a cashier at a physical retail store location.[99] As discussed above, these transactions are generally referred to in the credit card industry as card present transactions.[100] Because in-store carding requires the carder to physically visit the store, it is more risky for the carder than carding online.

In-store carding also requires a higher level of technical sophistication than carding online because the carder must create a counterfeit credit card. In order to make a counterfeit card, a criminal must possess several pieces of equipment, including for example, laminators, embossers, encoders, scanners, and printers, each of which is easily available for purchase on the Internet. First, the carder copies the dump onto the back of a piece of white plastic in the size and shape of a credit card. This process, performed with an encoder, is known as encoding.[101] The criminal could then use the white plastic as a credit card at any merchant store that allows the purchasers to swipe cards without an employee check. Second, in order to make the face of the white plastic identical to a credit card, the criminal uses an embosser to type in a name and number. Third, the criminal uses a printer to create a false Visa or MasterCard front. After these steps, the carder has a usable counterfeit card and can engage in in-store carding.

iii. Cashing

A third form of carding is known in the criminal world as "**cashing**." Broadly speaking, the term cashing refers to the act of obtaining money, rather than retail goods and services, with the unauthorized use of stolen financial information.[102] One particular method of cashing, known as "**PIN cashing,**" requires the carder to obtain dumps with PINs (*i.e.*, credit or debit card account or bank account information with personal identification numbers), encode the dump onto the back of a piece of white plastic as

---

[98] Warren Indictment, *supra* note 24, at 3.

[99] Jacobsen Affidavit, *supra* note 23, at 11. *See also* Warren Indictment, *supra* note 24, at 6.

[100] *See supra* note 67. A large subcategory of card present transactions involve transactions from "point-of-sale" or "**POS**" terminals in merchant store locations. Vega Affidavit, *supra* note 26, at 4. POS is "an acronym for a cash register transaction involving the purchase of merchandise with the use of a credit card." Warren Indictment, *supra* note 24, at 6.

[101] Criminals use the term "**white plastic**" to refer to white plastic in the size and shape of a credit card with credit card account information encoded on the back of the card. The Ninth Circuit has held that a blank white plastic card "is an access device within the meaning of 18 U.S.C. § 1029(e)(1)." United States v. Nguyen, 81 F.3d 912 (9th Cir. 1996). Encoders are used by criminals to encode dumps onto magnetic strips on white plastic cards in conjunction with an algorithm to "properly encode the magnetic strip and produce a usable card." Black Market in Stolen Data, *supra* note 53. The criminal could stop here and engage in "cashing," discussed below, to use this white plastic at an ATM machine and fraudulently obtain a cash advance on the stolen credit card number.

[102] Warren Indictment, *supra* note 24, at 2-3.

discussed above, and use the counterfeit card with the corresponding PIN at an ATM to obtain cash.[103]

iv. Gift card vending

Finally, some carders engage in a practice known as "**gift card vending,**" which involves purchasing gift cards from retail merchants at their physical stores using counterfeit credit cards and reselling such cards for a percentage of their actual value.[104] Such gift cards can be resold in several ways, including on a carding website or in face-to-face transactions to unwitting purchasers. In at least one reported case, the counterfeit credit cards used to purchase legitimate gift cards were encoded with stolen credit card numbers that originated from a large scale data breach.[105]

III. Links to Other Crimes

Of course, criminals may have motives that extend beyond mere financial fraud for belonging to carding forums and engaging in carding activities. Indeed, the connection between identity theft -- in particular as it relates to obtaining fraudulent identification documents -- and terrorism is well established.[106] In addition, links to drug traffickers engaging in identity theft for purposes of funding drug addictions is also well known.[107] Methamphetamine addicts in particular have been known to use the Internet to

---

[103] Warren Indictment, *supra* note 24, at 2-3; Jacobsen Affidavit, *supra* note 23, at 11. Other methods of cashing include: "cashing-out Western Union wires, postal money orders, and/or other financial instruments that were funded using transfers from stolen accounts … withdrawals from PayPal accounts that received funds via stolen credit and debit accounts, or setting up a bank account with a fake ID to withdraw cash on a credit card account." Warren Indictment, *supra* note 24, at 2-3.

[104] *See*, *e.g.*, Press Release, U.S. Dep't of Justice, Houston Man Pleads Guilty to Federal Identity Theft Charges (Nov. 1, 2005), available at http://www.usdoj.gov/criminal/cybercrime/hattenPlea.htm (member of the Shadowcrew criminal organization used the Shadowcrew website to engage in credit card fraud and gift card vending); Criminal Complaint at 3-6, United States v. Bruguera, No. 6:07-mj-01133-JGG, (M.D. Fla. Apr. 18, 2007) (individual supplied counterfeit credit cards encoded with stolen credit card numbers in conjunction with counterfeit official state driver's licenses' to purchase gift cards at Wal-Mart stores in Florida).

[105] *See* News Release, Fla. Dep't of Law Enforcement, Arrests made in gift card fraud case totaling more than $8 million in losses (Mar. 19, 2007), http://www.fdle.state.fl.us/press_releases/20070319_fraud_case.html (six individuals, including Irving Escobar, arrested in $8 million gift card fraud ring in which stolen credit cards were used to purchase large quantities of Wal-Mart and Sam's Club gift cards). The stolen credit card data used by Mr. Escobar and his codefendants to create counterfeit credit cards for ultimate purchase of the gift cards originated by the mass data breach at TJX, discussed above. Press Release, Office of the Att'y Gen., Ringleader of ID Theft Operation Sentenced to 5 Years in Prison (Sept. 13, 2007), http://myfloridalegal.com/newsrel.nsf/newsreleases/3D930E6715D0935D85257355005143E9 .

[106] BOB SULLIVAN, YOUR EVIL TWIN: BEHIND THE IDENTITY THEFT EPIDEMIC 122-140 (John Wiley & Sons 2004).

[107] Your Evil Twin, *supra* note 106, at 150-152. *See also* Press Release, U.S. Atty's Office for the Southern Dist. of Fla., Twenty-Nine Defendants Charged in Drug Importation and Credit Card Scheme (Apr. 19, 2007), available at http://www.usdoj.gov/usao/fls/PressReleases/070419-01.html (defendants in narcotics trafficking case stole legitimate credit card numbers, encoded the numbers onto blank card, and used the cards at various retail stores, including Wal-Mart, Winn Dixie, and area gas stations, to make unauthorized purchases).

commit identity theft.[108] In some reported cases, such addicts have engaged in phishing schemes and committed network intrusions to obtain stolen credit card numbers.[109] It would only be a small step for such criminals – if they have not already -- to turn to the online carding world rather than the physical world to obtain either fraudulent identification documents or stolen financial information.

Indeed, it appears that terrorists may be well aware of the carding underground. A convicted terrorist in Indonesia, Imam Samudra, specifically referred to credit card fraud and carding as a means to fund terrorist activities in his 280-page autobiography.[110] Samudra allegedly sought to fund the 2002 Bali nightclub bombings, of which he was convicted, in part through online credit card fraud.[111]

In a second case connecting terrorism and credit card fraud, three British men were convicted of inciting terrorist murder via the Internet under the United Kingdom's Terrorism Act of 2000.[112] In this case, Younes Tsouli, Waseem Mughal, and Tariq Al-Daour allegedly ran a network of extremist websites and communication forums through which al-Qaeda statements were issued and videos of beheadings and suicide bombings in Iraq and other jihadi propaganda were disseminated.[113] In a second component of the case, the three men pleaded guilty to conspiracy to defraud banks and credit card companies.[114] In relation to these charges, Al-Daour and his associates allegedly used stolen credit card numbers obtained through phishing scams and Trojan horses to make more than $3.5 million in fraudulent charges.[115] In particular, Al-Daour and his coconspirators used the numbers at hundreds of online stores to purchase equipment and other items, including prepaid cell phones and airline tickets, to aid jihadi groups in the field.[116] In addition, Tsouli and Mughal allegedly used stolen credit card numbers to set

---

[108] Jon Swartz, *Meth addicts hack into identity theft*, USATODAY.COM, Sept. 29, 2005, http://www.usatoday.com/tech/news/computersecurity/2005-9-29-meth-id-theft_x.htm [hereinafter Meth addicts]. *See also* John Leland, Meth Users, Attuned to Detail, Add Another Habit: ID Theft, N.Y. TIMES, July 11, 2006, at A1, available at http://www.nytimes.com/2006/07/11/us/11meth.html?ex=1310270400&en=6df49385bf828429&ei=5088&partner=rssnyt&emc=rss.

[109] Meth addicts, *supra* note 108.

[110] Alan Sipress, *An Indonesian's Prison Memoir Takes Holy War into Cyberspace*, WASH. POST, Dec. 14, 2004, A19.

[111] *Id*.

[112] *Three Admit to Inciting Terror Acts*, BBC NEWS, July 4, 2007, http://news.bbc.co.uk/1/hi/uk/6268934.stm.

[113] *A World Wide Web of Terror*, ECONOMIST, July 14, 2007, at 28; Craig Whitlock and Spencer S. Hsu, *Terror Webmaster Sentenced in Britain*, WASH. POST, July 6, 2007, at A10; Brian Krebs, *Three Worked the Web to Help Terrorists*, WASH. POST, July 6, 2007, at D1. Tsouli, Mughal, and Al-Daour were sentenced to ten years, seven and a half years, and six and a half years, respectively. *Three Jailed for Inciting Terror*, BBC NEWS, July 5, 2007, http://news.bbc.co.uk/2/hi/uk_news/6273732.stm

[114] *Three Jailed for Inciting Terror*, BBC NEWS, July 5, 2007, http://news.bbc.co.uk/2/hi/uk_news/6273732.stm.

[115] Brian Krebs, *Three Worked the Web to Help Terrorists*, WASH. POST, July 6, 2007, at D1.

[116] Brian Krebs, *Three Worked the Web to Help Terrorists*, WASH. POST, July 6, 2007, at D1. *A World Wide Web of Terror*, ECONOMIST, July 14, 2007, at 28.

up and host jihadi websites.[117] Significantly, the investigation revealed that these individuals were members of one or more carding organizations, including the now-defunct Shadowcrew criminal organization.[118]

IV. Federal Prosecutions of Carders and Carding Organizations

In the past several years, federal law enforcement has targeted the top-tier organizers, administrators, and vendors of various carding organizations. These investigations have resulted in several prosecutions, outlined below, shedding light on the global nature of carding organizations. In particular, criminals worldwide belong to, and actively participate in, these carding organizations. In addition, specific criminal carding activity, such as PIN cashing discussed above, often involves, and in some cases requires, the active participation of carders from more than one country. Finally, these investigations have also revealed that stolen information can be immediately and widely distributed across the globe.[119] In the TJX breach, for example, stolen account information was used to make purchases in the States of Florida, Georgia, and Louisiana, and Hong Kong, and Sweden.[120]

A. Prosecution of Shadowcrew Criminal Organization

The Shadowcrew criminal organization, comprised of thousands of members worldwide, operated and maintained the Internet web site www.shadowcrew.com from 2002 until October 2004, when it was taken down by the USSS as the result of a year-long undercover investigation known as Operation Firewall.[121]

In particular, on October 25, 2004, the USSS and the U.S. Department of Justice coordinated the search and arrest of more than 28 members of the Shadowcrew criminal organization, located in eight States in the United States and six foreign countries.[122] As

---

[117] *A World Wide Web of Terror*, ECONOMIST, July 14, 2007, at 28. "According to data gathered by U.S. officials, Tsouli and his two associates used at least 72 stolen credit card accounts to register more than 180 domains at 95 different Web hosting companies in the United States and Europe." Brian Krebs, *Three Worked the Web to Help Terrorists*, WASH. POST, July 6, 2007, D1.

[118] According to a New Scotland Yard investigator, evidence at trial revealed that the defendant Al-Daour was a member of the Shadowcrew criminal organization. Email from Shaun McLeary, Counter Terrorism Command, National Terrorist Financial Investigative Unit, United Kingdom New Scotland Yard, to Kimberly Peretti, U.S. Dep't of Justice (Sept. 24, 2007, 5:28 EDT) (on file with author). In addition, Al-Daour was also purportedly a member of the Carderplanet criminal organization. *See* Bob Sullivan, *Cyberterror and ID Theft Converge in London*, THE RED TAPE CHRONICLES, July 5, 2007, http://redtape.msnbc.com/2007/07/cyber-terror-an.html.

[119] According to one U.S. Dep't of Justice official discussing the Shadowcrew investigation, there is now a "black market for stolen information on a global level where information can be very quickly resold … Cards stolen in one country can, at the snap of your fingers, be used all over the world." *Smashing the Criminals' e-Bazaar*, BBC NEWS, Dec. 20, 2007, http://news.bbc.co.uk/1/hi/uk/7084592.stm.

[120] *45.7m Card Details Stolen in TJX Security Breach*, COMPUTERWEEKLY.COM, Mar. 30, 2007, http://www.computerweekly.com/Articles/2007/03/30/222778/45.7m-card-details-stolen-in-tjx-security-breach.htm.

[121] Shadowcrew Indictment, *supra* note 34, at 2 and 6; Shadowcrew Press Release, *supra* note 35.

[122] Press Release, U.S. Secret Service, U.S. Secret Service's Operation Firewall Nets 28 Arrests (Oct. 28, 2004), http://www.secretservice.gov/press/pub2304.pdf [hereinafter Secret Service Firewall Press Release].

part of this "takedown," the USSS disabled the Shadowcrew website. On October 28, 2004, a federal grand jury in Newark, New Jersey, returned a 62-count indictment of 19 members of the Shadowcrew criminal organization for, among other things, conspiracy to provide stolen credit and bank card numbers and identity documents through the Shadowcrew website.[123] The conspiracy was held responsible for trafficking in at least 1.7 million stolen credit and bank card numbers that resulted in losses in excess of $4 million.[124] However, it is estimated by law enforcement authorities that, had the organization not been interrupted, the credit card industry could have faced hundreds of millions of dollars in losses.[125] To date, and with the exception of two fugitives, all of the domestic Shadowcrew defendants have pleaded guilty and received sentences from probation to 90 months in prison.[126]

The indictment targeted the top-tier members of the organization, including two administrators, and several moderators and vendors.[127] Significantly, the indictment charged these individuals with conspiracy based on their activities and membership in a criminal organization that operated solely online. In doing so, the prosecution of the top-tier Shadowcrew members was the first-of-its-kind in holding individuals responsible not only for the criminal offenses facilitated through the carding forum but for participation in the criminal forum itself.[128]

The prosecution of the Shadowcrew criminal organization also revealed the extent to which criminal carding organizations are truly global in nature. In coordinating the searches and arrests in six foreign countries and investigating other foreign members of Shadowcrew, the USSS received support from law enforcement in the United Kingdom, Canada, Bulgaria, Belarus, Poland, Sweden, the Netherlands and Ukraine.[129] In addition, at least two foreign individuals were indicted in the Shadowcrew conspiracy, including one administrator of the forum from Russia and one vendor from Argentina.[130] Finally, at least one country – the United Kingdom – pursued a separate prosecution of Shadowcrew members in their homeland.[131] In December 2007, several of the United

---

[123] Shadowcrew Indictment, *supra* note 34, at 2 and 6. In addition to the single conspiracy count, the 19 indicted Shadowcrew members were charged with 61 other counts, "including unlawful trafficking in stolen credit card numbers and other access devices, unlawful transfer of identification documents to facilitate unlawful conduct, transferring false identification documents and unauthorized solicitation to offer access devices. Shadowcrew Press Release, *supra* note 35.

[124] Shadowcrew Indictment, *supra* note 34, at __.

[125] Secret Service Firewall Press Release, *supra* note 122.

[126] *See, e.g.*, Press Release, U.S. Dep't of Justice, Houston Man Sentenced to 90 Months for Identity Theft (July 11, 2006), http://www.usdoj.gov/opa/pr/2006/July/06_crm_424.html; Press Release, U.S. Atty's Office, District of New Jersey, "Shadowcrew" Identity Theft Ringleader Gets 32 Months in Prison (June 29, 2006), http://www.usdoj.gov/usao/nj/press/files/mant0629_r.htm.

[127] Shadowcrew Press Release, *supra* note 35.

[128] Computer Crime Research Center, Computer Crime: The Most Significant Case, http://www.crime-research.org/articles/computer-crime-most-significant-case/2. (last visited Mar. 12, 2008).

[129] Secret Service Firewall Press Release, *supra* note 122.

[130] Shadowcrew Press Release, *supra* note 35.

[131] *Smashing the Criminals' e-Bazaar*, BBC News, Dec. 20, 2007, http://news.bbc.co.uk/1/hi/uk/7084592.stm.

Kingdom defendants pled guilty and were sentenced to terms of imprisonment ranging from nine months to six years.[132]

In addition, the activities of the Shadowcrew defendants revealed that members from one country would conspire with members from another country to commit specific carding crimes. In one case, a carder in the United States, Kenneth Flurry, received stolen CitiBank debit card account numbers and PINs from individuals in Europe and Asia.[133] After obtaining the numbers, Flurry encoded them on to blank white plastic cards in order to withdraw cash from ATMs.[134] He then transferred a portion of the proceeds abroad to the individuals supplying the information.[135] In October 2005, Flurry, who was also indicted in New Jersey as part of the Shadowcrew conspiracy, was indicted for bank fraud in connection with his scheme to defraud CitiBank.[136]

Since the takedown of the Shadowcrew criminal organization, the USSS and other federal law enforcement agencies have successfully arrested several other well known carders, gaining further insight into the secret world of carding.

B. Prosecution of Members of Carderplanet Criminal Organization.

In addition to targeting the Shadowcrew criminal forum, Operation Firewall targeted the Carderplanet criminal organization, discussed in Section I.B.ii above,[137] which was disbanded in the months prior to the Shadowcrew takedown. Roman Vega, known online as "Boa," was an administrator of Carderplanet, and allegedly one of the most significant high-level carders from Eastern Europe.[138] Vega, a Ukrainian national, was arrested in Cyprus in July 2005.[139] He was subsequently extradited to the United States where he initially faced a 40-count indictment for access device fraud and wire fraud in the Northern District of California.[140] The indictment charged him with trafficking in credit card information of thousands of individuals that had been illegally obtained from entities around the world, including credit card processors and merchants.[141] Two years later he was again indicted in New York for access device fraud and money laundering.[142]

---

[132] *Id.*

[133] Press Release, U.S. Atty's Office for the Northern Dist. of Ohio, Cleveland, Ohio Man Sentenced to Prison for Bank Fraud and Conspiracy (Feb. 28, 2006), http://www.usdoj.gov/criminal/cybercrime/flurySent.htm.

[134] *Id.*

[135] *Id.*

[136] *Id.* He subsequently pled guilty, and was sentenced to 32 months imprisonment. Plea Agreement, United States v. Flurry, No. 1:05-cr-00567-DCN (N.D. Ohio, 2006); Press Release, U.S. Atty's Office for the Northern Distr. of Ohio, Cleveland, Ohio Man Sentenced to Prison for Bank Fraud and Conspiracy (Feb. 28, 2006), http://www.usdoj.gov/criminal/cybercrime/flurySent.htm.

[137] Secret Service Firewall Press Release, *supra* note 122; Jacobsen Affidavit, *supra* note 23, at 2.

[138] Ukraine Captures Key Suspect, *supra* note 50.

[139] Press Release, U.S. Dep't of Justice, Background on Operation Web Snare – Examples of Prosecutions (Aug. 27, 2004), http://www.usdoj.gov/criminal/fraud//docs/reports/2004/websnare.pdf.

[140] *Id.*

[141] *Id.*

[142] Indictment, United States v. Vega, No.1:07-cr-00707-ARR-1 (E.D.N.Y. Sept. 18, 2007).

Several high-ranking members of the Carderplanet criminal organization have also been targets of investigations in the Ukraine and the United Kingdom, including a founder and administrator known online as "Script," and a senior member and reviewer known online as "Fargo." Dmitro Ivanovich Golubov ("Script") was known as the Godfather of the Carderplanet organization and a notorious hacker.[143] He was allegedly responsible for facilitating the theft and trading of millions of credit and debit card numbers.[144] In July 2005, he was arrested by Ukrainian law enforcement authorities for financial fraud, but was subsequently released.[145]

Douglas Havard ("Fargo") was a senior member and reviewer of the Carderplanet criminal organization who was active in PIN cashing for high-level Russian carders.[146] After fleeing the United States in 2002 from pending drug charges, he was ultimately arrested in the United Kingdom in June 2004.[147] He pled guilty to "charges of fraud and money laundering in connection with his role in the Carderplanet network"[148] and was sentenced in June 2005 to six years in prison.[149]

C. Operation CardKeeper

In 2005 and 2006, another significant federal investigation targeted carders operating on various forums that sprung up in the aftermath of Operation Firewall, including among others CCpowerForums and Theft Services.[150] Operation CardKeeper, which was led by the FBI in conjunction with the U.S. Attorney's Office for the Eastern District of Virginia, originated from complaints of phishing attacks against a major financial institution in late 2004.[151] As a result of this investigation, thirteen individuals

---

[143] Meet the Hackers, *supra* note 51; As Identity Theft Moves Online, *supra* note 49.
[144] Kim Zetter, *Tracking the Russian Scammers*, WIRED MAGAZINE, Jan. 31, 2007, http://www.wired.com/politics/onlinerights/news/2007/01/72605.
[145] "Mr. Golubov was quietly released from prison in December [2005] while awaiting trial." Countless Dens, *supra* note 56. Two Ukrainian politicians evidently "vouched for Golubov's character in court" and the judge released in on a personal recognizance bond. Meet the Hackers, *supra* note 51. Golubov is also subject to federal charges in the United States. *See* Complaint, United States v. Golubov, No. 8:06-mj-00010-1 (C.D. Cal. Jan. 10, 2006) (alleging violations of conspiracy and access device fraud).
[146] Havard and his associate would receive ATM account numbers and PINs from Russians, encode the information on to the magnetic stripes of blank cards, frequent ATMs to withdraw cash, and send 60% of the proceeds to Russia. As Identity Theft Moves Online, *supra* note 49.
[147] As Identity Theft Moves Online, *supra* note 49. Havard was later indicted for a false statement made in application of a passport in violation of Title 18, United States Code, Section 1542. Indictment, United States v. Havard, No. 3:04-cr-00295-1 (N.D. Tex. Sept. 8, 2004).
[148] Ukraine Captures Key Suspect, *supra* note 50.
[149] As Identity Theft Moves Online, *supra* note 49.
[150] Hale Indictment, *supra* note 32, at 6-7; Warren Indictment, *supra* note 24, at 6; *see also* http://blog.washingtonpost.com/securityfix/2006/11/14_arrested_for_credit_card_ph_1.html. For a discussion of the CCpowerForums and Theft Services organizations, *see* Section I.B.ii above.
[151] Robert Lemos, *FBI Nabs Suspected Identity-Theft Ring*, SECURITY FOCUS, Nov. 13, 2006, http://www.securityfocus.com/brief/347.

in Poland and eight in the United Stated were arrested,[152] and search warrants were executed in both Romania and the United States.[153]

One of the significant individuals prosecuted in the United States as a result of Operation CardKeeper was Steven Lance Roberts, known online as "John Dillinger," who pled guilty to conspiracy to commit bank fraud, access device fraud, and aggravated identity theft in November 2006.[154] Roberts was known as a notorious cashier of stolen credit and debit card numbers that he purchased from hackers and phishers in Russia and Romania.[155] Similar to Flurry and Havard, discussed above, after obtaining the stolen numbers, Roberts would encode them "to plastic bank cards, make ATM withdrawals, and return an agreed-upon portion to the vendors."[156]

In addition to stolen account information originating from Romanian phishers and Russian hackers, the investigation also revealed that account information originated from a group of Polish phishers responsible for a series of phishing attacks against United States' financial institutions.[157] The leader of the Polish group was also allegedly responsible for supplying access to compromised computers to the Romanians to assist in their phishing schemes.[158]

Similar to Operation Firewall, Operation CardKeeper demonstrates the extent to which criminal carding organizations are global in nature, and often rely on criminals

---

[152] As part of the initial arrests and charges, Dana Carlotta Warren, Frederick Hale, and Zanadu Lyons were indicted for conspiracy to commit bank fraud, access device fraud, aggravated identity theft and identity fraud. Warren Indictment, *supra* note 24; Hale Indictment, *supra* note 32. In December 2006, Warren plead guilty to conspiracy to commit bank fraud, access device fraud, and aggravated identity theft, and was later sentenced to 45 months in prison. United States v. Warren, No. 3:06-cr-00372-HEH-1 (E.D. Va. 2007).

[153] Press Release, U.S. Atty's Office for the Eastern Dist. of Va., "Operation Cardkeeper" Defendant Sentenced to 94 Months in Prison (Feb. 9, 2007), http://www.usdoj.gov/usao/vae/Pressreleases/02-FebruaryPDFArchive/07/20070209robertsnr.pdf.

[154] Plea Agreement, United States v. Roberts, No. 3:06-cr-00314-HEH-1 (E.D. Va. 2007). Roberts was later sentenced to 94 months in federal prison. Press Release, U.S. Atty's Office for the Eastern Dist. of Va., "Operation Cardkeeper" Defendant Sentenced to 94 Months in Prison, Feb. 9, 2007, http://www.usdoj.gov/usao/vae/Pressreleases/02-FebruaryPDFArchive/07/20070209robertsnr.pdf.

[155] *Id*. In an interview with Wired Magazine prior to his federal indictment, Roberts confirmed that he was a regular cashier of debit account and PIN numbers, and that he obtained stolen numbers from Romanian phishers and Russian hackers. Kim Zetter, *Confessions of a Cybermule*, WIRED MAGAZINE, July 28, 2006, http://www.wired.com/politics/onlinerights/news/2006/07/71479; Kim Zetter, *FBI Busts Credit Card Cybergang*, WIRED MAGAZINE, Nov. 3, 2006, http://www.wired.com/science/discoveries/news/2006/11/72064.

[156] Press Release, U.S. Atty's Office for the Eastern Dist. of Va., "Operation Cardkeeper" Defendant Sentenced to 94 Months in Prison (Feb. 9, 2007), http://www.usdoj.gov/usao/vae/Pressreleases/02-FebruaryPDFArchive/07/20070209robertsnr.pdf. As discussed above, such activity is known as "PIN cashing" in the carding world.

[157] Brian Krebs, *FBI Tightens Net Around Identity Theft Operations*, WASH. POST, Nov. 3, 2006, at D5.

[158] Brian Krebs, *14 Arrested for Credit Card, Phishing Scams*, WASHINGTONPOST.COM, Nov. 3, 2006, http://blog.washingtonpost.com/securityfix/2006/11/14_arrested_for_credit_card_ph_1.html; Kim Zetter, *FBI Busts Credit Card Cybergang*, WIRED MAGAZINE, Nov. 3, 2006, http://www.wired.com/science/discoveries/news/2006/11/72064.

from more than one country sharing expertise in order to carry out particular carding activities.

D. Carders "Maksik" and "Lord Kaisersose"

A second Ukrainian carder, Maksym Yastremskiy, known online as "Maksik" and to be one of the top traffickers in stolen account information, was arrested for his carding activity in Turkey on July 26, 2007.[159] Maksik allegedly sold hundreds of thousands of credit and debit card numbers.[160] One of his customers, an infamous carder known online as "Lord Kaisersose,"[161] was previously searched and arrested in France on June 12, 2007 as the result of a joint investigation conducted by the Secret Service and the French National Police.[162] The arrests of both these well-known carders illustrate the importance of international law enforcement cooperation and partnerships.

E. Carder "Iceman"

Max Ray Butler, known online as "Iceman," was the co-founder and administrator of the carding forum Cardersmarket, discussed in Section I.B.ii above.[163] He was arrested on September 5, 2007,[164] and subsequently indicted for wire fraud and identity fraud.[165] Butler allegedly engaged in a scheme whereby he "hacked into secure computer systems connected to the Internet, including but not limited to computers located at financial institutions and credit card processing centers, in order to acquire credit card account information and other personal identification information that he could sell to others."[166] Butler operated the Cardersmarket website in order to sell this stolen information to others.[167] Butler sold tens of thousands of credit card account information, including credit card numbers, credit card holder names, credit card types and expiration dates, issuing bank names, CVVs, and related financial information, to others "who, in turn, converted the information to cash proceeds by making fraudulent purchases of merchandise that they re-sold, and shared the proceeds of such sales with [Mr. Butler.]"[168]

---

[159] Cassell Bryan-Low, *Turkish Police Hold Data-Theft Suspect*, WALL ST. J., Aug. 10, 2007, at A6. When the Secret Service became aware that Yastremskiy was planning to be in Turkey, they coordinated with local law enforcement for his arrest. U.S. authorities are currently seeking his extradition. *Id.*
[160] *Id.*
[161] *Id.*
[162] Press Release, U.S. Secret Service, United States Secret Service Targets Cyber Criminals (June 25, 2007), http://www.secretservice.gov/press/GPA07-07_investigations.pdf. The fraud loss associated with the investigation exceeded $14 million. *Id.*
[163] Press Release, U.S. Secret Service, Secret Service Investigation Disrupts Identity Theft (Sept. 13, 2007), http://www.secretservice.gov/press/GPA11-07_PITIndictment.pdf.
[164] *Id.*
[165] Butler Indictment, *supra* note 57.
[166] Press Release, U.S. Atty's Office for the Western Dist. of Pa., "Iceman," Founder of Online Credit Card Theft Ring, Indicted On Wire Fraud and Identity Theft Charges (Sept. 11, 2007), http://www.usdoj.gov/usao/paw/pr/2007_september/2007_09_11_02.html.
[167] Butler Indictment, *supra* note 57, at 1.
[168] Butler Indictment, *supra* note 57, at 3.

This prosecution is significant in that the target was both active in stealing the credit and debit card account information – the network intrusion side - and reselling the stolen information through carding forums – the credit card fraud side. One of the methods used by Butler to compromise computer systems in order to steal the information was to exploit wireless systems.[169] In particular, Butler would rent hotel rooms and apartments using false identities, and use an expensive, high-powered antenna to intercept communications through wireless Internet access points, thereby capturing credit card numbers and other personally identifiable information.[170] Butler used this technique, for example, to hack into financial institutions and data processing centers.[171]

A variation of this method used by other hackers to compromise computer systems is "wardriving." Wardriving is the act of driving around in a vehicle with a laptop and a high-powered antenna to locate, and potentially exploit, wireless computer systems of vulnerable targets.[172] Once inside the system, a criminal is able to intercept wireless communications and capture credit card numbers and other personal identification information. In 2003, for example, hackers gained unauthorized access into the computer systems of Lowe's Corporation using the wardriving method.[173] In this case, the hackers compromised the wireless network at a Lowe's retail store in Southfield, Michigan and thereby gained access to the company's central computer systems in North Carolina.[174] After accessing the system, the intruders installed a malicious computer program on the computer systems at several retail stores that was designed to capture the credit card information of customer transactions.[175]

V. Other Responses to Large Scale Credit and Debit Card Compromises

While federal law enforcement has targeted the criminals who steal and sell the credit and debit card account information, the credit card industry has attempted to make credit and debit card account information harder to steal by requiring entities that hold such account information to adopt a set of security standards designed to protect cardholder data. These security standards have, in turn, been codified into law in at least one state.

A. Payment Card Industry Data Security Standard (PCI DSS)

[169] Affidavit in Support of Criminal Complaint at 8, 11, 16, and 17, United States v. Butler, No. 2:07-mj-00401-RCM (W.D. Pa. Sept. 4, 2007).
[170] *Id.*
[171] *Id.* at 11 and 16.
[172] SearchMobileComputing.com, What is War Driving?, http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci812927,00.html (last visited Mar. 12, 2008).
[173] Indictment at 2, United States v. Salcedo, No. 5:03-cr-00053-LHT-1 (W.D.N.C. 2006).
[174] *Id.*; Press Release, U.S. Dep't of Justice, Hacker Sentenced to Prison for Breaking into Lowe's Companies' Computers with Intent to Steal Credit Card Information (Dec. 15, 2004), http://www.usdoj.gov/criminal/cybercrime/salcedoSent.htm.
[175] *Id.*

As noted above, several of the recent high-profile security breaches have involved the compromise of millions of credit and debit card account information from merchants and credit card processors. Because merchants and processors hold this sensitive information, they are a frequent target of hackers, looking for vulnerabilities in their computer systems.[176] Recognizing the risk posed by weak security, the credit card associations developed a set of security standards, known as the Payment Card Industry Data Security Standards (PCI DSS), for merchants and third party processors.[177] The PCI DSS, organized as a set of twelve requirements under six core principles, are designed to protect consumer payment account information. These core principles include: (1) building and maintaining a secure network; (2) protecting cardholder data; (3) maintaining a vulnerability management program; (4) implementing strong access control measures; (5) regularly monitoring and testing networks; and (6) maintaining an information security policy.[178]

All merchants and service providers that store, process, or transmit cardholder data are required to comply with the PCI DSS. [179] In addition, compliance applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce.[180] Deadlines for compliance depend on the size of the organization. The largest merchants, which are referred to as Level 1 merchants and process six million of more Visa transactions annually, were required to comply with the standards by September 30, 2007. Medium-sized merchants, which are referred to as Level 2 merchants and process one to six million transactions annually, were required to comply by December 31, 2007. Noncompliant entities can receive monthly fines of up to $25,000.[181] In January 2008, Visa reported that more than three-fourths of Level 1 merchants and nearly two-thirds of Level 2 merchants (accounting for two-thirds of Visa's U.S. transaction volume) were PCI compliant.[182]

---

[176] Stephen S. Wu, *Update on Information Security Compliance: Selected Information Security Laws, Proposals, and Requirements*, *in* 1 EIGHTH ANNUAL INSTITUTE ON PRIVACY AND SECURITY LAW: PATHWAYS TO COMPLIANCE IN A GLOBAL REGULATORY MAZE COURSE HANDBOOK 105, 114 (Practicing Law Institute 2007).

[177] THE PCI SECURITY STANDARDS COUNCIL , PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD Ver. 1.1 (2006), https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf. The PCI Security Standards Council, founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International, was organized by the major credit card companies to develop, maintain, and disseminate the DSS. https://www.pcisecuritystandards.org/about/index.htm. Prior to the DSS Ver. 1.1, in 2001, Visa had developed a Cardholder Information Security Program (CISP) to protect Visa cardholder data. In 2004, the CISP requirements were incorporated into a PCI DSS developed by Visa and MasterCard, which later became the PCI DSS Ver. 1.1 released in 2006. Visa, Inc., Card Holder Information Security Program, http://usa.visa.com/merchants/risk_management/cisp_overview.html.

[178] THE PCI SECURITY STANDARDS COUNCIL , PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD Ver. 1.1 (2006), https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

[179] Visa, Inc., ,Card Holder Information Security Program, http://usa.visa.com/merchants/risk_management/cisp_overview.html.

[180] *Id.*

[181] Press Release, Visa Inc., PCI Compliance Continued to Grow in 2007 (Jan. 22, 2008), available at http://corporate.visa.com/md/nr/press753.jsp.

[182] Press Release, Visa Inc., PCI Compliance Continued to Grow in 2007 (Jan. 22, 2008), available at http://corporate.visa.com/md/nr/press753.jsp.

Requirement 3 of the PCI DSS, which falls under the principle of protecting cardholder data, is particularly relevant to the recent occurrences of data breaches. This requirement prohibits the retention of:

- The full contents of any track from the magnetic stripe;
- The card-validation code or value (three-digit or four-digit number printed on the front or back of the payment card) used to verify card-not-present transactions; and
- The personal identification number (PIN) or the encrypted PIN block.[183]

At least some of the reported recent breaches have involved the unauthorized storage of sensitive data, such as track data.[184] As a result, particular emphasis has been placed on merchants and processors in regards to whether such entities are improperly storing track data and other sensitive information. Certainly, ensuring that merchants and processors comply with Requirement 3 and do not retain sensitive data is a critical step in closing one avenue through which criminals obtain large volumes of customer information.

Even if data is not retained, however, hackers can break into vulnerable systems and obtain the data by other methods. For example, once inside a system, a hacker could install a piece of malicious code – called a sniffer -- that allows for the capture of data in real-time as it transverses the network. This would allow the hacker to capture cardholder data in transit as opposed to data in storage. As a result, it is important that entities comply with all requirements of the PCI DSS in order to ensure that their computer systems are secure and cardholder data is thereby protected from different methods of compromise.[185]

b. State Legislation

In May 2007, Minnesota became the first state to enact legislation codifying Requirement 3 of the PCI DSS.[186] The legislation was proposed in response to the data breach at TJX, discussed above, and several other retailers.[187] Effective August 1, 2007, the Plastic Card Security Act prohibits any person or entity conducting business in

[183] THE PCI SECURITY STANDARDS COUNCIL , PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD Ver. 1.1 (2006), https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.
[184] For example, Cardsystems acknowledged that it stored magnetic stripe data for research purposes in violation of Visa and MasterCard security standards. Statement of Perry, *supra* note 11, at 9.
[185] In the TJX data breach, a forensics report concluded that TJX only met three of the twelve requirements under the PCI DSS. Declaration of Joel Lisker, *supra* note 19, at 6.
[186] 2007 Minn. Sess. Law Serv. Ch. 108 (H.F. 1758) (West).
[187] News Release, State Senator Mary A. Olson, Senate approves Minnesota Plastic Card Security Act (May 15, 2007), http://www.senate.mn/members/member_pr_display.php?ls=&id=925. In the TJX data breach, a Marshall's store in Minnesota was reported to be the initial entry point for the hackers to enter TJX's central database. *Id*.

Minnesota "that accepts an access device in connection with a transaction"[188] from retaining:

> "the card security code, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.[189]

The legislation also shifts the financial liability of security breaches from the financial institution issuing the card to the merchant or entity from which the cardholder data was stolen.[190] Furthermore, the legislation creates a private right of action for any individual cardholder injured by the breach.[191]

To date, it remains uncertain whether other states will follow Minnesota in codifying this requirement of the PCI DSS.[192] Given the financial incentives for entities to comply with the PCI DSS, however, it is unclear whether these types of statutes are necessary. In addition, as discussed above, the improper storage of data is only one avenue by which hackers can obtain consumer data. As a result, state statutes that are broader in scope – perhaps by codifying other requirements of the PCI DSS in addition to requirement 3 -- may better protect consumer data from compromise.

VI. Challenges and Solutions

Keeping credit and debit card account and other financial information out of the hands of criminals is an essential first step in both reducing the frequency, and lessening the impact, of large scale data compromises. As entities that store, process, or transmit cardholder data work toward complying with industry security standards, significant progress can be made in this area.

Prosecuting and punishing criminals is a second key element of addressing data breaches involving compromised cardholder data.[193] As security experts frequently recite: total security is impossible. Therefore, despite compliance with industry security standards, it is likely that hackers will continue to develop techniques to exploit the computer systems of entities holding cardholder data. Prosecutions of carders and

---

[188] The term "access device" is defined as "a card issued by a financial institution that contains a magnetic stripe, microprocessor chip, or other means for storage of information which includes, but is not limited to, a credit card, debit card, or stored value card." Id. at subdiv. 1(b).
[189] 2007 Minn. Sess. Law Serv. Ch. 108 (H.F. 1758) (West), subdiv. 2.
[190] *Id.*, at subdiv. 3.
[191] *Id.*, at subdiv. 4.
[192] In April 2007, the Texas House of Representatives passed a bill that would have required a business that collects sensitive information in connection with a credit, debit, or stored value card to "comply with payment card industry data security standards." H.B. 3222, 80th Leg., Reg. Sess., § 1 (Tex. 2007). The Texas legislature, however, failed to enact this bill before the end of the legislative session. California and New Jersey still have pending bills that would codify the PCI DSS. See A.B. 779, 2007-2008, Reg. Sess. (Cal. 2007) (as amended May 14, 2007), sec. 1; A2270, 213th Leg., Assemb. No. 2270 (N.J. 2008).
[193] A third essential step in the data breach problem is making it more difficult to misuse the stolen financial information. This step, however, is beyond the scope of the article.

carding organizations provide law enforcement and private industry with valuable insight into the nature of large scale data breaches and resulting identity theft, in particular with respect to the evolving nature of the targets and methods and types of attacks. Such prosecutions also fulfill the goal of punishing and deterring those responsible for this form of identity theft.

Successful prosecutions of carders (including hackers) depend in large part on: (1) victims reporting the cases to law enforcement; (2) the availability of statutes criminalizing the underlying conduct; (3) sentences reflecting the seriousness of the crime; and (4) increased cooperation with foreign law enforcement. The following section discusses each of these aspects in turn.

A. Reporting Breaches to Law Enforcement.

Over 36 states have laws that require consumer notification in the event of a security breach.[194] Many of these state laws allow victim entities to delay notification if a law enforcement entity informs the entity that notification may impede a criminal investigation.[195] Some even also require that the compromised entity notify affected parties, including law enforcement and/or consumer reporting agencies.[196] In addition, Visa requires all entities that have experienced a suspected or confirmed security breach to contact their local U.S. Secret Service office.[197]

These reporting requirements are vital to the ability of law enforcement to investigate the types of crimes involving large scale data breaches. Without such reporting, law enforcement may never hear of the incident or may be notified after it is too late to preserve critical evidence. In other circumstances, law enforcement may be generally aware of the incident through undercover channels, but not know the name of the victim, and thus not be able to confirm the particular details needed to further investigate and/or prosecute the case.

In its Strategic Plan, the President's Identity Theft Task Force recommends the establishment of a national standard which would require entities that maintain sensitive data to provide timely notice to law enforcement in the event of a breach.[198] The standard would also allow law enforcement to authorize a delay in the required notice for law enforcement or national security reasons.[199] Because only a handful of state laws currently require reporting to law enforcement and because private sector requirements

[194] Combating Identity Theft, *supra* note 28, at 34.
[195] *See*, *e.g.*, Florida (Fla. Stat. § 817.5681 (2005) and New York (N.Y. Gen. Bus. Law § 899-aa (Consol. 2006).
[196] *See*, e.g., Colorado (Colo. Rev. Stat. § 6-1-716 (2006)) and Ohio (Ohio Rev. Code Ann. § 1349.19 (West 2006).
[197] Visa Procedures, *supra* note 65, at 4.
[198] Combating Identity Theft, *supra* note 28. On May 10, 2006, President George W. Bush signed an executive order addressing identity theft that, among other things, established an intergovernmental Identity Theft Task Force. Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 15, 2007). In April 2007, the Task Force released a strategic plan for combating identity theft. Combating Identity Theft.
[199] Combating Identity Theft, *supra* note 28, at 36.

are not enforced, such a national standard that requires reporting of breaches to law enforcement is a critical precursor to successful prosecutions of these crimes.

Several bills now before Congress include a national notification standard. In addition to merely requiring notice of a security breach to law enforcement,[200] it is also helpful if such laws require victim companies to notify law enforcement prior to mandatory customer notification. This provides law enforcement with the opportunity to delay customer notification if there is an ongoing criminal investigation and such notification would impede the investigation.[201] Finally, it is also helpful if such laws do not include thresholds for reporting to law enforcement even if certain thresholds – such as the number of customers affected or the likelihood of customer harm -- are contained within customer notification requirements. Such thresholds are often premised on the large expense of notifications for the victim entity, the fear of desensitizing customers to breaches, and causing undue alarm in circumstances where customers are unlikely to suffer harm. These reasons have little applicability in the law enforcement setting, however, where notification (to law enforcement) is inexpensive, does not result in reporting fatigue, and allows for criminal investigations even where particular customers were not apparently harmed.

B. Statutes Criminalizing Hacking and Carding.

As indicated by the federal prosecutions discussed above, the government has successfully prosecuted a variety of carders and carding organizations. These prosecutions utilized a range of federal statutes, including the identity theft statute (18 U.S.C. § 1028(a)(7)), access device fraud (18 U.S.C. § 1029), wire fraud (18 U.S.C. § 1343), bank fraud (18 U.S.C. § 1344), conspiracy (18 U.S.C. § 371), and aggravated identity theft (18 U.S.C. § 1028A), reflecting the fact that a number of existing statutes are available to punish criminals who engage in carding-related activities. In addition, if the carder is also engaged in the stealing of the information, he/she may be prosecuted under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

One of the newer offenses available to federal prosecutors is aggravated identity theft.[202] The aggravated identity theft offense provides for an additional mandatory two-year imprisonment term in cases where a defendant "knowingly transfers, possesses, or uses, without lawful authority a means of identification of another person" during and in relation to one of several enumerated felony offenses, including, among other offenses, access device fraud, wire fraud, bank fraud, and computer fraud.[203] The term "means of identification" is broadly defined and includes, for example, a credit or debit card account

[200] *See* Privacy and Cybercrime Enforcement Act of 2007, H.R. 4175, 110th Cong. § 102 (2007) (providing prompt notice of a major security breach to the U.S. Secret Service or the Federal Bureau of Investigation).
[201] *See* Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. § 311 (2007) (allowing a reasonable delay in notice to customers in order to provide notice to law enforcement and allowing law enforcement to authorize a further delay if customer notification would impede a criminal investigation).
[202] This offense was created by The Identity Theft Penalty Enhancement Act, which took effect July 15, 2004.
[203] 18 U.S.C. § 1028A (2007).

number.[204] In carding-related prosecutions, the aggravated identity theft offense often enables prosecutors to obtain an additional two-year imprisonment term for each underlying carding-related offense for which the defendant is convicted and thereby acts as a significant deterrent. These additional imprisonment terms provided by the aggravated identity theft offense also counteract potential lenient sentences, which are often received by identity thieves and hackers.

C. Appropriate Sentences

Hackers and identity thieves receive light sentences in many cases either because of their young age or because the sentencing judge may not view these non-violent crimes as serious. Indeed, a recent identity theft bill passed by the Senate directs the Sentencing Commission to review its guidelines to reflect the intent of Congress that penalties for identity theft-related offenses should be increased.[205] Many of the factors listed in the bill for consideration by the Sentencing Commission could potentially support changes to the Guidelines that enhance the sentences of carders and hackers involved in data breaches, including: (1) the level of sophistication and planning involved in the offense; (2) whether such offense was committed for private financial benefit; (3) the extent to which the offense violated the privacy rights of individuals; (4) whether the defendant disclosed personal information obtained during the commission of the offense; and (5) whether the term "victim" should include individuals who suffer non-monetary harm.[206] This last consideration warrants further elaboration.

One particular sentencing issue that surfaces in carding cases is the uncertainty surrounding the "multiple victim enhancement." Under the U.S. Sentencing Guidelines, criminals who victimize more than one person may receive a sentencing enhancement of up to six levels.[207] The Guidelines currently define "victim" to include persons who suffer monetary loss and exclude persons who suffer only non-monetary harm.[208] It is unclear, however, whether the definition of "victim" includes an individual who initially suffers monetary loss but who is later indemnified or reimbursed, such as in the case of unauthorized credit card charges. Some jurisdictions, for example, do not consider victims to include individuals who have been indemnified for unauthorized credit card charges.[209] Because of this uncertainty, the President's Identity Theft Task Force recommends that the Sentencing Commission amend the definition of "victim" to "state clearly that a victim need not have sustained an actual monetary loss."[210]

Given that victims are usually indemnified by their financial institutions for any unauthorized credit or debit card purchases, this amendment would be particularly helpful in prosecutions of carders and carding organizations.

---

[204] *See* 18 U.S.C. §§ 1028(d)(7)(D) & 1029(e) (2007).
[205] Identity Theft Enforcement and Restitution Act of 2007, S. 2168, 110th Cong. § 10(a) (2007).
[206] S. 2168 § 10(b).
[207] U.S. Sentencing Guidelines Manual § 2B1.1(b)(2) (2007).
[208] U.S. Sentencing Guidelines Manual § 2B1.1 cmt. n.1, 3(A)(i), & 3(A)(iii) (2007).
[209] Combating Identity Theft, *supra* note 28, at 67.
[210] Combating Identity Theft, *supra* note 28, at 68 and Appendix 1.

D. Coordination and Cooperation from Foreign Law Enforcement

As described in detail above, carding forums provide a means for criminals worldwide to congregate, exchange information and buy and sell contraband. In addition, once carders have met through forums, they often join together in carrying out a particular financial fraud or criminal activity. As a result, coordination and cooperation from foreign law enforcement is vital to the success of carding investigations and prosecutions. In this regard, the President's Identity Theft Task Force specifically recognizes the need to:

- "Encourage other countries to enact suitable domestic legislation criminalizing identity theft;
- Facilitate investigation and prosecution of international identity theft by encouraging other nations to accede to the convention on cybercrime
- Identify the nations that provide safe havens for identity thieves and use all measures available to encourage those countries to change their policies
- Enhance the United States Government's ability to respond to appropriate foreign requests for evidence in criminal cases involving identity theft
- Assist, train, and support foreign law enforcement."[211]

Two of these items merit special attention: the problem of countries acting as save-havens, and the need to have countries accede to the Council of Europe's Convention on Cybercrime.[212] The global fight against identity theft and criminal carding activity is only as good as the weakest link. Countries that either do not have the legal framework to prosecute such activity or that turn a blind eye through law enforcement inaction, in effect, become breeding grounds for organized criminal carding operations. One important tool to changing the practices in these safe-haven countries is the promotion of the comprehensive legal framework embedded in the Convention on Cybercrime. By providing standards for substantive and procedural laws, the Convention provides an important benchmark for countries evaluating their cybercrime laws, and demonstrates a commitment of the acceding country to provide assistance in international cybercrime investigations.[213]

As companies increasingly rely on computer systems and the Internet in the Information Age, it has become increasingly clear that criminals have the tools to access and exploit for financial gain large volumes of personal information, thereby revolutionizing the identity theft landscape. In order to protect such information from thieves, it is also clear that both the private and public sectors have a significant role to

---

[211] *Id*. at 8.

[212] For background on the Convention on Cybercrime, including the text of the Convention, *see* Department of Justice's Computer Crime and Intellectual Property Section's website, at http://www.cybercrime.gov/intl.html#Vb.

[213] *See* Richard W. Downing, *Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime*, 43 COLUM. J. OF TRANSNAT'L L. 705 (2005).

play. For example, by complying with industry security standards, companies holding personal data can better protect their systems from exploitation. In addition, by providing the government with better tools to continue successfully prosecuting criminal carding organizations, we can ensure that individuals committing these crimes can be adequately and appropriately punished and deterred.

I. Introduction
   A. Large Scale Data Breaches
   B. Background on Carding
      i. Shadowcrew
      ii. Other carding organizations
      iii. Types of information for sale on carding sites.
II. Credit and Debit Card Fraud
   A. Obtaining the Information to Sell
   B. Types of Carding
      i. Carding Online
      ii. In-Store Carding
      iii. Cashing
      iv. Gift Card Vending
III. Links to Other Crimes
IV. Federal Prosecutions of Carders and Carding Organizations
   A. Shadowcrew
   B. Carderplanet
   C. Operation Cardkeeper
   D. Maksik and Lord Kaisersose
   E. Iceman
V. Other Responses to Large Scale Credit and Debit Card Compromises
   A. PCI DSS
   B. State Legislation
VI. Challenges and Solutions
   A. Reporting Breaches to Law Enforcement
   B. Statutes Criminalizing Hacking and Carding
   C. Appropriate Sentences
   D. Coordination and Cooperation with Foreign Law Enforcement