A F F I D A V I T

I, Matthew D. Ferrante, being duly sworn, hereby depose and state as follows:

1. I am a Special Agent ("SA") of the United States Secret Service (“USSS”), and have been so employed since April 2000.

a. I am currently assigned to the Newark, New Jersey field office, to the “Operation Firewall” squad. In that capacity, I am responsible for investigating, among other things, electronic crimes including computer hacking and computer fraud.

b. During my career as a Special Agent of the USSS, I have participated in numerous investigations involving computer-related offenses, and assisted in the service of search warrants involving searches and seizures of computers, computer equipment, software, electronically stored information, and instrumentalities of fraud.

c. I have also been certified as an “Electronic Crimes Special Agent,” which I obtained through extensive training in computer forensics and network analysis.

2. The facts set forth in this affidavit are based primarily on information I have obtained from my work on the “Operation Firewall” squad. The affidavit is also based on knowledge obtained from other individuals, including other law enforcement officers; my review of documents and computer records

related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

3. This affidavit is submitted in support of an application for a criminal complaint and arrest warrant charging NICOLAS LEE JACOBSEN, of 1655 East 1st Street, Apartment 291, Santa Ana, California, with violating 18 U.S.C. § 1030(a)(2)(C) (intentionally accessing a computer without authorization and thereby obtaining information from a protected computer).

4. This affidavit is intended to show merely that there is sufficient probable cause to support a criminal complaint and arrest warrant and does not purport to set forth all of my knowledge of, or investigation into, this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

5. Title 18, United States Code, Section 1030(a)(5)(A) states, in pertinent part:

> Whoever . . . intentionally accesses a computer without authorization or exceeds authorization access, and thereby obtain . . . information from any protected computer if the conduct involved an interstate or

foreign communication.

6. This Application is being made to further an investigation into Shadowcrew, Carderplanet, and Darkprofits (collectively, the "criminal organizations"), three organized criminal groups dedicated to promoting malicious computer hacking; Internet fraud schemes; electronic theft of personal financial and identifying information; trafficking in and use of stolen credit card and debit card information ("dumps"), stolen bank account information, and other stolen individual identifying information; and the production of, trafficking in, and use of counterfeit identification documents.

Background

Definition of Relevant Computer and Internet Concepts

7. **The Internet** is a collection of computers and computer networks that are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between Internet computers exist across state and international borders; therefore, information sent between two computers connected to the Internet frequently crosses state and international borders even where the two computers are located in the same state.

8. **Internet Service Providers** ("ISP's"): Most individuals and businesses obtain access to the Internet through ISP's. America Online ("AOL"), Microsoft, and Earthlink are examples of

some of the larger and better-known ISP's. Other ISP's include private entities such as corporations, universities, and government agencies. Among other services, ISP's provide their customers with access to the Internet using telephone, cable, Digital Subscriber Line, or other types of telecommunications lines.

9. **Internet Protocol Address** ("IP address"): An IP address is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots (e.g., 149.101.10.40). Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. ISP's assign IP addresses to their customers' computers. An ISP might assign a different IP address to a customer each time the customer makes an Internet connection ("dynamic IP addressing"), or it might assign an IP address to a customer permanently or for a fixed period of time ("static IP addressing"). Either way, the IP address used by a computer attached to the Internet must be unique for the duration of a particular session; that is, from connection to disconnection. ISP's typically log their customers' connections, which means that the ISP can identify which of its customers was assigned a

specific IP address during a particular Internet session.

10. **Domain Names**: Numerical IP addresses generally have corresponding domain names. For instance, the IP address "149.101.10.40" resolves to the corresponding domain name "www.cybercrime.gov". The Domain Name System ("DNS") is an Internet service that associates each domain name with an IP address. This mapping function is performed by DNS servers located throughout the Internet. DNS allows a user knowing only a domain name to reach a computer without having to know its IP address. In general, a registered domain name should resolve to a numerical IP address.

11. **Log files** are computer-generated files containing information regarding the activities of computer users, processes running on a computer, and the usage of computer resources.

12. **File Transfer Protocol** ("FTP") is a communication protocol for transferring files between computers connected to the Internet.

13. **ICQ** is an online real-time instant messaging service. ICQ sessions between individuals can run for hours or days at a time during which these individuals often will have several discrete conversations separated by breaks in time when there is no communication. Each person participating in ICQ chat is assigned a unique ICQ number eight-digit number that remains assigned to them until such time as they abandon that number; the

number may or may thereafter be recycled and assigned out to another person.

14. **Whois search** is a search of a public records database to learn the identity of the ISP with assignment authority over particular IP addresses. Once the identity of the ISP is determined, that ISP can be compelled to disclose records related to the customer or subscriber assigned that IP address on a specific date and at a specific time.

Background of the Criminal Organizations

15. As noted above, Shadowcrew, Carderplanet, and Darkprofits are three organized criminal groups dedicated to promoting malicious computer hacking; Internet fraud schemes; electronic theft of personal financial and identifying information; trafficking in and use of stolen credit card and debit card information ("dumps"), stolen bank account information, and other stolen individual identifying information; and the production of, trafficking in, and use of counterfeit identification documents. These groups operate, respectively, the Internet web sites **www.shadowcrew.com**, **www.carderplanet.com**, and **www.darkprofits.com** as the public manifestations of the criminal organizations. These web sites serve primarily as communications media to facilitate the commission of the above-referenced criminal activity. These web sites publicly disseminate information regarding the perpetration of such

criminal activity through postings and responses to postings by members to electronic forums on the sites. They also facilitate the transmission and receipt of private electronic messages between members of the respective criminal organizations. Furthermore, the web sites serve as electronic bulletin boards for members of the respective criminal organizations to advertise and promote the sale of credit card and debit card dumps, stolen bank account information, other stolen individual identifying information, and counterfeit identification documents to other members.

16. The criminal organizations operate their associated web sites and oversee the activities of their members through the following hierarchical framework:

a. "Administrators"/"Forum Techs" are a small group of individuals that serve as a governing council of each criminal organization who, collectively, control the destiny of their organization. The administrators handle day-to-day management decisions of the organizations as well as long-term strategic planning for the organizations' continued viability. They determine which individuals are permitted to become and remain members of criminal organizations; the functions, responsibilities and levels of access to information for all members of the organizations; and the rewards accorded members for their loyalty to the organizations as well as the punishments

meted out to members evidencing disloyalty to the organizations. Furthermore, they decide when, how and under what circumstances to attack and/or to retaliate against members of rival criminal organizations and their associated Internet web sites. The administrators are accorded full access to and privileges on the computer servers hosting the corresponding web sites and, thus, have ultimate responsibility for the physical administration, maintenance and security of these computer servers as well as for the content of the web sites.

b. "Moderators" oversee and administer one or more subject-matter-specific forums on the web sites that either fall within an area of their expertise or cover their geographic location, limiting their activities to editing and deleting posts by members on these forums. Moderators also frequently serve as reviewers for particular products or services with which they have an expertise.

c. "Reviewers" examine and/or test products and services that members of the criminal organizations desire to advertise and sell via the corresponding web sites (e.g., counterfeit passports, drivers licenses, Social Security cards, credit cards, birth certificates and other identification documents; credit card dumps; counterfeit checks; and stolen credit card pre-authorization ("dump check") services) and post a written summary of that examination or testing on the appropriate

web site. A favorable written review is a prerequisite to vending on the web sites hosted by the criminal organizations. While most reviewers primarily serve in the capacity of administrator or moderator, any qualified individual can be appointed by an administrator to conduct a review, even a general member.

d. "Vendors" advertise and sell products and services to members of the criminal organizations via the associated web sites after the product or service has received a favorable written review from a reviewer. Once a reviewer is designated, a prospective vendor is required to ship multiple samples of the product or provide access to the service to facilitate completion of the review. This contact between the prospective vendor and the reviewer is usually made through a private e-mail message or through a public post in a forum on the relevant web site.

e. "General members" of the criminal organizations have no role in the operation of the corresponding web sites. Instead, they typically use the web sites to gather and provide information about perpetrating criminal activity through postings on the various forums and through private e-mail messaging to other members. They also use the sites to facilitate their purchases of credit card dumps, false identification documents and other contraband that then serves as instrumentalities of their own criminal conduct. A member of any of these criminal

organizations is known to other members by his/her chosen screen name or nickname ("nic"). Individuals often are known by and conduct their criminal business under more than one nic.

17. The continued viability of the criminal organizations is dependent upon individuals who are skilled hackers. A computer hacker is an individual who accesses computer systems without authorization, often for the purpose of stealing information or causing damage to computer systems. Hackers, whether actual members of the criminal organizations or not, are the primary source of credit card dumps and stolen identity information that are sold on the associated web sites and used to create false identity documents and counterfeit credit cards. Like the members of the criminal organizations that they service, hackers are known by their nic's and predominantly communicate with each other and with others in the online criminal underworld through real-time chat sessions, exchanging information on forums and other electronic bulletin boards, and private e-mail messaging.

18. The hackers and members of the criminal organizations use their own descriptive vernacular when communicating with each other regarding their criminal activity. Several of the most frequently used words and phrases include:

a. "Banging out ATM's" (or "cashing out PIN's") refers to illegally obtaining funds from an automated teller

machine ("ATM") through the unauthorized use of bank account information encoded onto counterfeit plastic cards. These counterfeit plastic cards are often used in conjunction with other personal information acquired from potential victims by various methods, including hacking and phishing scams, to steal money and to engage in financial fraud.

b. "Carding" refers to the general concept of purchasing retail items with counterfeit credit cards or stolen credit card information.

c. "In-store carding" occurs when the carding committed by an individual requires him/her to be physically located inside a retail store when making the fraudulent purchase. In such a scheme, a counterfeit credit card that has been encoded with the legitimate account information of the victim is presented to the cashier by the offender. Often, various false identification documents are used to facilitate this fraud.

d. "Carding on-line" refers to carding via an online Internet transaction.

e. "Carding to a drop" refers to the act of carding goods via online Internet transactions and having the items purchased shipped to an anonymous mail drop. A variation of this scheme occurred when the offender causes the fraudulently obtained merchandise to be shipped to a third party in return for

a previously agreed upon sum of money, thing of value, or service or for a specific percentage of the future proceeds from the sale of the item by the third party.

f. "Change of billing" (or "cob") occurs when an individual, after having acquired all the pertinent information related to victim's credit card account, accesses the account via the Internet or via a telephone call and causes the billing address for the credit card changed, or causes an alternate shipping address to be added, in order to facilitate credit card fraud.

g. "Novelty" (or "nov") refers to a counterfeit identification document (e.g., drivers licenses, birth certificates, and passports). The term is often used on the web sites by vendors of counterfeit identification documents in a misguided effort to afford them plausible deniability of any criminal culpability for producing and selling these items by claiming that they are only for novelty purposes.

h. "Phishing" refers to an Internet fraud scam involving the sending out of large volumes of unsolicited commercial e-mail ("spam") containing a link to a replica of an Internet web page of a well known commercial or financial company in an effort to trick the victim into clicking on this link and entering his/her credit card or personal financial information as requested by the replica web page, which is then sold by the

offender or used by the offender to commit fraud or identity theft.

i. "Printing" is commonly used to refer to the production of counterfeit plastic credit cards.

19. The members of the criminal organizations have employed multiple, real-time Internet chat messaging services to facilitate the commission of criminal conduct. These services include America On-Line Instant Messenger ("AIM"), ICQ (I seek you), mIRC (Internet Relay Chat), Yahoo Messenger, and MSN. Many of these chat messaging services can all be accessed simultaneously using a software program called Trillian which offers, for example, encrypted instant messaging capabilities. These services accommodate discussions among the subjects and aid them in securing their communications with each other. Specifically, Trillian offers a secure method by which online criminals can communicate and facilitates their ability to engage in criminal activity without being monitored by law enforcement.

20. To further facilitate their illegal activity, members of these criminal organizations utilize Digital Currency Businesses ("DCB's") to pay for illegal purchases and launder money gained from criminal conduct. These DCB's are based on the concept of stored value, and do not act in a manner consistent with traditional banking methods. In other words, the electronic currency is backed by and translated into an unencumbered

physical commodity, most often a quantity of gold or another precious metal. DCB's are popular within these criminal organizations because they quickly and easily facilitate the conversion of national hard currencies when dealing with co-conspirators in foreign countries. Moreover, because of DCB internal policies and their location beyond the reach of U.S. law enforcement authorities, they provide unprecedented levels of privacy for those engaging in illegal monetary transactions.

21. The members of the criminal organizations use proxies to surf the Internet and access web sites. A "proxy" is an intermediate computer that sits between the user's computer and the destination computer. It accepts requests from the user's computer, transmits those requests on to the destination computer, and then returns the response from the destination computer back to the user's computer via the proxy. These proxies are used to conceal the identity of the user from law enforcement by hiding the user's true originating IP address. When an individual uses a proxy to access a web site for illegal activity, the logs from the web site show the IP address of the proxy, not the IP address of the user's computer. It is not uncommon for hackers and other online criminals to conceal their identities by using more than one proxy when accessing the Internet for the purpose of engaging in criminal conduct. The USSS has learned that there are currently over 100,000

compromised computers being used as proxies in the United States. These proxies are part of hotel computer networks, university computer networks, and corporate computer networks, as well as compromised privately owned computers throughout the country.

22. Members of the criminal organizations often establish, maintain and make use of proxies augmented by high quality encryption standards specifically to conceal their true identities when accessing the Internet ("anonymizers"). A common example of an anonymizer is a virtual private network ("VPN"). A VPN affords many computers the ability to simultaneously connect to it via a single shared IP address, commonly referred to as the "gateway IP address." Privacy is achieved by providing each user a separate encrypted tunnel to secure his/her electronic communications. The content of the data packets sent from each individual's computer to the VPN is then encrypted.

Probable Cause to Believe A Person Using the Nickname "Ethics" Violated 18 U.S.C. § 1030(a)(2)(C)

23. On March 15, 2004, a person using the online nickname "Ethics" posted the following information on a website designated as www.muzzfuzz.com:

> am offering reverse lookup of information for a t-mobile cell phone, by phone number at the very least, you get name, ssn, and DOB at the upper end of the information returned, you get web username/password,

voicemail password, secret question/answer, sim#, IMEI#, and more.

24. I know that www.muzzfuzz.com is an Internet bulletin board for buying, posting and sharing hacks and credit card numbers, and for facilitating identity theft and fraud.

25. In my training and experience, I understand this posting to be an offer to sell information contained on T-Mobile's customer database, including "reverse lookup" information that enables a person to enter a phone number and obtain personal information regarding the person using that telephone number.

26. Or or about July 28, 2004, USSS Special Agent Peter Cavicchia spoke with representatives of T-Mobile, who confirmed that a hacker had obtained unauthorized access to their customer database.

27. On July 28, 2004, a confidential informant ("CI") working for the USSS was contacted by a person using the online nickname "Sigep," who the CI knew to be a member of the Shadowcrew criminal organization.

a. In that communication, Sigep permitted the CI to see portions of previous online conversations that Sigep had with another member of the Shadowcrew criminal organization who used the online nickname "Myth."

b. The portions of the conversation between Sigep and Myth contained excerpts of an internal USSS Memorandum Report as well as part of a Mutual Legal Assistance Treaty from the Russian Federation. These documents contained highly sensitive information pertaining to ongoing USSS criminal cases.

28. The CI is a high ranking member of both the Shadowcrew and Carderplanet criminal enterprises having served in the capacity of administrator, moderator and reviewer. The CI has entered into a cooperating plea agreement with the United States pursuant to which the CI will receive consideration in return for his/her assistance. The CI has not yet been formally charged, but has been informed that he/she will be charged as a result of his participation in the criminal enterprises. The CI has been assisting the undercover investigation since in or about August 2003, and has provided extensive information about the activities of the criminal enterprises, their members, and the manner in which computer systems are used by these groups and individuals. In the course of providing assistance, the CI's online activities and communications have been logged, with his/her consent, by monitoring software. In addition, the information provided by the CI has been extensively corroborated through consensual communications with the subjects of the investigation and through the results of search warrants and pen register and

trap and trace orders. The USSS special agents supervising the CI believe him/her to be truthful and reliable.

29. Later on July 28, 2004, the CI was contacted directly by Myth, who stated that:

a. Myth had received the compromised USSS documents from an undisclosed person.

b. Myth knew, based on information from this undisclosed person, that his (Myth's) ICQ number was under surveillance by federal agents.

c. Myth would try to put the CI in contact with the undisclosed person who had provided the USSS documents and who had informed Myth of the surveillance.

30. Later that same day, the CI received an email from Myth that contained prior conversations between Myth and the undisclosed supplier of the data. The conversations between Myth and an unknown person contained references to subpoena requests for information regarding the ICQ numbers pursuant to an ongoing USSS investigation.

31. On July 29, 2004, the CI was again contacted by Myth, who stated that the undisclosed person who had supplied the Secret Service investigation information (as well as the other information outlined above) wanted to speak to the CI. Myth instructed the CI to meet this person in an IRC chat room.

32. Later that day, the CI met Myth and another person who was using the online nickname "anyonman" in an IRC chat room. During that three-way conversation:

a. "Anyonman" stated that he had obtained information from numerous Secret Service documents.

b. "Anyonman" thereafter showed the CI numerous USSS documents (through pasting them into the chat).

c. "Anyonman" then told the CI that the computer at IP address 209.250.116.88 was "interesting," and identified that address as belonging to the United State Secret Service New York field office.

33. After checking online database and Secret Service records, I know that IP address 209.250.116.88 is registered to a Secret Service computer in the New York Field Office Electronics Crimes Task Force. In particular, that IP address is registered to a computer used by USSS Special Agent Peter Cavicchia.

34. From speaking with Peter Cavicchia, I know that he has a T-Mobile account which:

a. He has used to access his work computer at IP address 209.250.116.88.

b. Automatically received email forwarded from his personal "mac" account, at pcavvichia@mail.mac.com.

35. On August 2, 2004, the CI contacted a person using the online nickname "Ethics." Based on the CI's extensive involvement with the Shadowcrew criminal organization, the CI knows that "Ethics" is a "vendor" in the Shadowcrew organization. During their conversation:

a. The CI asked "Ethics" whether he was the person using the nickname "anyonman" earlier that day. When the CI raised that possibility, Ethics proceeded to paste text conversation intercepted from SA Cavicchia's T-Mobile e-mail account, including conversations that explicitly referenced Cavicchia.

36. A few days later, on August 5, 2004, the CI and Ethics again spoke, and Ethics asked if the CI had a proxy server that he/she could use. When the CI asked Ethics why he needed a proxy, Ethics responded, "[t]o browse and log into a site with the credentials of a USSS Agent." Under the direction of USSS agents the CI was instructed to configure a computer that was controlled by agents of the Newark Field Office. The CI then gave Ethics the IP address of the undercover USSS computer and the appropriate port number which would allow Ethics to access the computer. Later that day, USSS observed the following:

a. Ethics used the proxy supplied to him by the CI.

b. We observed Ethics use the undercover proxy computer to log into http://mail.sidekick.dngr.com, which is the

web server computer used by T-Mobile to store its customers' information, and attempt to log into the SA Cavicchia's compromised personal email account with T-Mobile. It was later determined that the sensitive USSS information was stored on the T-Mobile/Danger servers.

c. We also observed Ethics attempt to log into pcavicchia@mail.mac.com, which is the personal email account of SA Cavicchia to which Cavicchia's T-Mobile e-mail account automatically forwards any T-Mobile email.

37. On or about October 19, 2004, Ethics sent a private message to the CI which contained a link that provides unauthorized access to the T-Mobile database. This link allows a user to input a phone number ultimately allowing access to the user's personal information. Ethics also instructed the CI to be extremely careful with this type of information. Furthermore, Ethics provided our CI with the direct access to SA Cavicchia's T-Mobile account.

Probable Cause to Believe "Ethics" Is JACOBSEN

38. On July 30, 2004, analysts at Criminal Investigative Division, USSS Headquarters conducted searches on the Internet to try to determine the true identity of the person using the Ethics nickname.

a. Analysts identified Ethics by his ICQ number of 23292256, which is the only ICQ number Ethics used when communicating with the CI.

b. A resume posted on the Internet from 2001 for Nicolas JACOBSEN, with an address of 120 Winston Section Road, Winston, Oregon 97496, contained ICQ 23292256 as a contact number for JACOBSEN. The e-mail address listed on the resume was "ethics@netzero.net".

39. On August 8, 2004, USSS agents examined the backdoor logs into the Shadowcrew web site (the backdoor had been operated by the USSS as part of the undercover operation) and learned that Ethics logged into www.shadowcrew.com using the IP address 24.75.10.122 on August 8, 2004 at 17:22:29 EDT.

40. On that same day, USSS agents conducted a Whois search and a trace route on the IP address of 24.75.10.122 and determined that this IP address belonged to the Residence Inn Hotel located near Buffalo, New York. USSS agents searched the Internet and located the phone number for the Residence Inn located in Williamsport, New York (just outside of Buffalo.) Agents telephoned the aforementioned hotel and confirmed that Nicolas Jacobsen was residing at that hotel at the date and time at issue.

41. On August 11, 2004, the Residence Inn in Williamsport, New York provided business records relating to the customer

assigned the IP address 24.75.10.122 on August 8, 2004 at 17:22:29 EDT. The Residence Inn's records showed that the IP address in question was assigned to "Nicolas Jacobson" as a guest at the hotel.

42. On or about July 28, 2004, a review of public record databases was conducted for Nicolas JACOBSEN. This review revealed the address 1655 East 1st Street, Apartment 291, Santa Ana, CA. It was also learned that JACOBSEN works for Pfastship Logistics International, 17752 Mitchell Ave., Suite H, Irvine, CA. USSS agents placed a call to Pfastship Logistics International and confirmed that Jacobsen is currently employed by that company.

43. From California Department of Motor Vehicles records, I know that JACOBSEN has a valid California driver's license D6644175, under the name Nicholas Lee Jacobsen, which lists his date of birth as February 24, 1983; his address as 1655 East 1st Street, Apt 291, Santa Ana, CA; and his physical description as 5'10"; 210 lbs; brown hair; brown eyes.

44. On or about October 26, 2004, USSS Special Agent Christopher Henderson conducted physical surveillance on 1655 East 1st Street, Apt 291, Santa Ana, CA. Earlier that morning, Henderson observed JACOBSEN leaving the residence for the Irvine location of Pfastship Logistics. Henderson followed JACOBSEN to that locale and continued surveillance.

45. After speaking with Pfastship Logistics International, I know that JACOBSEN regularly travels on business and was in Buffalo, New York on business when he accessed the T-Mobile service on August 8, 2004. I also have reason to believe that JACOBSEN had continuous access to the T-Mobile database between March 2004 and October 2004 because the Secret Service documents he showed the CI bore different dates and because we witnessed multiple intrusions, as noted above. Because JACOBSEN travels with the computer he uses to access to the T-Mobile database, and because JACOBSEN lives and works in Orange County, California, there is probable cause to believe, in light of his continuous, unauthorized access, that JACOBSEN has illegally accessed the T-Mobile database on at least one occasion from his home or work in the Central District of California.

Sealing Order Requested

46. It is respectfully submitted that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this application, including the application, the affidavit, the criminal complaint, and the arrest warrant. Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Premature disclosure of the contents of this affidavit and related

documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness.

Conclusion

46. For the foregoing reasons, I believe that there is probable cause to believe that NICOLAS LEE JACOBSEN accessed a protected computer without authorization and obtained information, in violation of 18 U.S.C. § 1030(a)(2)(C).

Matthew D. Ferrante
Special Agent
United States Secret Service

Sworn to before me this
26th day of October 2004.

UNITED STATES MAGISTRATE JUDGE
Central District of California