Investigative Protocols for Credit-Card Fraud on the Internet

Cmdr. Dave Pettinari
Pueblo County Sheriff's Office
Pueblo High-Tech Crime Unit
davepet@cops.org

Investigative Steps

1. Have the victim provide you with a copy of their credit-card statement listing the suspicious charges. They should have already reported the fraud to the credit-card company, which usually assigns a fraud investigator. You could call the company for the statement. Some of them are cooperative, while others are stinkers about releasing any info other than to the actual credit-card holder. However, if you have a few well-cultivated contacts over time, you might be able to get it more quickly from the credit-card company.
2. When the victim gets a letter from the credit-card company, get the name of the fraud investigator for coordination and information-sharing.
3. Once you get the statement, identify which charges are suspect (which Internet company accepted the card). Often, there is an 800 phone number for the company. Ask the company that took the charge if you can get a physical shipping address, which usually provides a lead. Again, they may or may not give out any information to law enforcement without a subpoena or search warrant.
4. Once you identify the suspect charges, check under whose name the purchase was made, and where it was shipped. From here, you can start by interviewing the person who delivered the goods ordered -- UPS, Post Office, FedEx, etc. You'd be surprised whom these delivery people remember.
5. In addition, check with the merchant. Sometimes they call to verify orders or suspicious addresses, and they can tell you the number they called. They usually keep a record of these conversations. They are often more helpful than the credit card companies because the liability for the charge is on them (the merchant). The credit-card company (bank) requires three things for them to assume liability for the purchase: 1) a signature, 2) authorization from them to the merchant that the account is active, has the available funds/credit, and 3) an imprint of the card (which can be the electronic swipe of a card, not just the manual method).
6. Check other online retailers of a similar type to what you are investigating. For example, if your case involves purchases of electronics, query other sites that sell electronics. This can be a big task, but that is what many investigators of this type of fraud do. Many times, a suspect will get hold of a credit card or number, go to all the clothes sales sites on the Internet (LL Bean, Lands End, Levis, etc.) and order stuff. Each case is different, so adjust accordingly.
7. If the charge involves downloading of software, or required entry of an e-mail address for completion of the transaction, get the e-mail address of the person ordering or downloading. That can be traced back to the Internet Service Provider, where, with a subpoena or search warrant, you could get the subscriber information. If the person was using, say, America Online, a subpoena will generally get you some good subscriber information. If one of the more anonymous services such as Hotmail or Yahoo, a subpoena will get you only raw data logs or IP (Internet Protocol) numbers. The IP number can be traced back to the Internet Service Provider of the suspect through customary backtracking based on the IP/date/time. The suspect can be using a number of ways to stay anonymous on the Internet, which means you will never find out who he is. But, if less stealthy, you might get a good lead.
8. If they Internet Service Provider's records still exist (we have to move very quickly because these are not maintained very long), they will show the IP address for a given date and time. These might be matchable with the merchant's logs even if the merchant can't tie a specific purchase to an incoming IP address. If you have 1) goods shipped to an address and 2) an account owned by someone at that address, which account just HAPPENED to be accessing the merchant's site at the time the fraudulent order was placed, THEN you should have probable cause for a search and/or arrest warrant.

9. If you are feeling really aggressive, you could also attack from the other end. Tangible goods have to be shipped somewhere, meaning you should be able to identify the person or household. Once you have the household, historical phone detail will tell you what Internet Service Provider that person is dialing into repeatedly. For example, if it is Internet Express from the Pueblo area, the number repeatedly seen in the phone records would be 544-9994. This assumes, of course, that the suspect uses a "vanilla" dial-up service. If they have a cable modem, which is online all the time, you won't see these repeat dial-ups.
10. If you need help with the process or more information on how to work these scams, the U.S. Postal Inspectors and U.S. Secret Service work a bunch of them.

Crime Prevention Tips to Give the Cardholder

Credit-card fraud is affecting people who have never used their credit card numbers on the Internet. We suspect it involves both the theft of credit card numbers from other sources (e.g., kid who took your credit-card at a gas station as you traveled cross country, some low-paid employee at your doctor's office selling your private information to thieves, mail/credit bureau theft, airline baggage handlers, etc.) and the use of software that generates "well formed" credit card numbers.

Even so, the following tips will help consumers learn what they have to do to prevent a recurrence and target-harden for future safeguarding of their credit.

1. The quicker you dispute the better. Waiting a week or two will leave you liable only for the first $50, but report the fraud within 24 hours, and both MasterCard and Visa will instruct the bank that issued your card to waive all fraudulent charges. Be forewarned, however: claiming a case of credit fraud where there isn't one is considered fraud in itself and is a federal offense. Discover will respond similarly to claims of online fraud, investigating the disputed charges and then refunding them when they prove to be fraudulent.
2. Credit card companies are working on some new technology called SET that should be operational in the near future. The principle behind SET is public key cryptography. SET software will "reside" in your computer and in the merchant's and the bank's network computers. Your computer's SET software will have a coded sequence or a "key" unique to you, that will be recognized by the SET-equipped computer on the other end.
3. Until SET is in place, knowing it is possible but unlikely someone will steal your credit information over the Internet, you should stick to some simple rules:

- Find out where -- in real space, not cyberspace -- the merchant is located. If the only address on their Web site is a post office box, be wary. It is very easy for such companies to disappear, making it nearly impossible to track them down for redress.
- Don't give out your credit card number via e-mail (it is too easy for someone to forward your number to someone else to someone else to an unscrupulous someone else).
- Shop with a merchant who uses a secure server (solid key, or locked lock at the lower right hand corner of the web page). On your end, you should be using the latest encrypting version of one of the major browsers, such as Netscape Navigator or Microsoft's Internet Explorer.
    - It is easy to figure out whether your credit-card data is secure as it travels from your PC to your web merchant's server. Just check your browser in the URL address block. The URL of a secure (encrypted) page begins with https rather than just http. If you have an updated version of Netscape or Internet Explorer, you will also see the closed-lock symbol in the status bar at the bottom of your browser screen.
    - Locate or request a security or privacy statement that spells out how the merchant handles sensitive data. If possible, find out who has access to credit card data within the company.

Other tips:

- Report lost or stolen cards and any suspect charges on your account to your issuing bank immediately (There should be a hotline number on the back of your card). It's the single most important maneuver to prevent fraud and dodge liability for fraudulent charges. You should follow up with a written report as well.
- In the case of stolen wallets, having a police report on file is advantageous for verifying your claims if a liability conflict arises between you and the credit card company.
- The American Bankers Association suggests acquiring a copy of your credit report from each of the three major credit bureaus (see below) annually to ensure their accuracy. Verify that all accounts in your name are legitimate and that any accounts you've closed are officially closed. Bureau reports generally cost around $8 each, but you can obtain them free of charge if you've been denied credit.
- In many instances, a swindler can open charge accounts in your name with just a license and major credit card. If your wallet is lost or stolen, contact the fraud departments of the three bureaus and ask them to place a "fraud alert" on your file so that any future credit applications will have to be confirmed with you over the phone.

    - Trans Union Credit Services: (800) 888-4213
        - Fraud Assistance Dept.: (800) 680-7289
    - Equifax Credit Services: (800) 685-1111
        - Fraud Assistance Dept.: (800) 525-6285
    - Experian Credit Services: (888)397-3742
        - Fraud Assistance Dept.: (888) 397-3742

In most cases, you'll only be liable for $50 if fraudulent usage occurs. When you get the report, look for new addresses and signs of new cards being issued. If you have conflicts with your issuing bank or the credit card company itself, there are consumer advocacy groups which may be able to help:

- National Consumers League (202) 835-3323

- Federal Trade Commission (When enacted, recently passed legislation will make the FTC a clearinghouse for all types of identity fraud.)

Tips For Foiling Credit Card Criminals

- Keep a record of your cards, issuing bank phone numbers, account numbers and expiration dates in a
- safe place (not your wallet) in case your wallet is lost or stolen to ensure that you have the proper
- information to cancel everything.

- Sign new cards as soon as they arrive.

- Destroy credit card offers that come in the mail, especially pre-approved offers

- When making transactions, keep cards in view whenever possible. If the sales clerk is giving you the willies, call a manager.

- Don't sign blank receipts. Draw a big fat line or N/A through blank spaces like the tip section of a restaurant receipt.

- Save receipts to reconcile with your monthly statement. And never toss receipts without mutilating them first.

- Notify card companies in advance of address changes.

- Hide your cards and account numbers from everyone, including friends and family. Disgustingly enough, a significant amount of fraud is committed by people the cardholder is related to, knows or works with.

- Never give out your account number over the phone unless you have initiated the call to place an order with a reputable company.

- Don't volunteer any personal information when making a credit card transaction. ID may be requested, otherwise, the sales clerk doesn't need to know. If it becomes an issue, ask for the manager.

- If you're using a debit card or other service which involves a PIN, never disclose it. No one, not even the police, needs to know your PIN.

- Don't carry all your cards around in your wallet. Store them in a secure place and only carry the ones you need.

- Don't leave cards in your car; a staggering number of card thefts are from glove compartments.

- All of the above applies doubly when you're traveling.

- With increased Internet commerce, the credit industry has been making a valiant effort to tighten online credit card security as well. For more information on web safety, improved technology, policy and lists of reputable online businesses, visit the major credit card companies' websites:

-
    - www.mastercard.com
    - www.visa.com
    - www.discovercard.com
    - www.americanexpress.com

Other Advice for Victims (Credit-card holders)

- Be sure to obtain a mailing address and telephone number for any online business you purchase from. The contact information will come in very handy should any problems arise with an order, of if you have to track back to see where you purchased online where a credit card number could have been stolen from.
- If you have any questions about a merchant, call the Better Business Bureau where the merchant is located. You'll find that number at www.bbb.org/bureaus. Also contact Internet Fraud Watch, 800-876-7060, www.fraud.org and ask if it has received any complaints about the merchant.
- Phone the FTC Hotline that has been setup to deal with this fraud: 202-326-3144 for updated information (messages only). Fill out the online form at http://www.ftc.gov/ftc/complaint.htm so you are eligible for reimbursement.
- Look for a bank that has a good service and anti-fraud record.
- Use as few credit cards as possible. Eliminate any debit or other cards that you don't really use. Minimize transactions so you can detect irregularities.
- Report the fraud to www.fraud.org and other anti-fraud sites (see links).

- Send a complaint to the Consumer Affairs Division for the state where the fraud occurred. Be sure to include a copy of the billing, your name and address as well as the business name and address.

For more information on credit-card fraud and its prevention, or to report…

- Better Business Bureau
  - http://www.bbbonline.org
  - http://www.bbb.org/alerts/scamtel.html
- Blacklist of Internet Advertisers
  - http://cco.caltech.edu/~cbrown/BL/
- Consumer World
  - http://www.consumerworld.org
- Fraudnet
  - http://www.acfe.org/ -- Association of Certified Fraud Examiners
- Internet Scambusters
  - http://www.scambusters.com
- National Fraud Investigations Center
  - http://www.tunfc.com
- U.S. Postal Service
  - http://usps.gov/websites/depart/insept/consmenu.htm
- FBI Computer Crime Center
  - http://www.fbi.gov/compcrim.htm
- Scams on the Internet
  - http://www.ftc.gov/bcp/scams01.htm
- To read about how crooks disguise who they are with anonymous remailers in doing credit-card fraud on the Internet:
  - http://www.well.com/user/abacard/remail.html
  - http://electron.rutgers.edu/~gambino/anon_servers/anon.html
  - http://www.anomymizer.com

Steps To Minimize Credit Card Fraud For Merchants

- Begin taking a few extra steps to validate each order. Don't accept orders unless complete information is provided (including full address and phone number). Many cards now require Address Verification for all of credit card orders.

- Be wary of orders with different "bill to" and "ship to" addresses. Many companies now require anyone who uses a different "ship to" address to send them a fax with their signature and credit card number authorizing the transaction.

- Be especially careful with orders that come from free email services. There is a much higher incidence of fraud from these services (hotmail.com, juno.com, usa.net, etc.). Many businesses won't even accept orders that come through these free email accounts anymore. That's because it's so easy for a fraud artist to open a free, anonymous email account in another person's name and then send you, the merchant, an order using the fake email account and a fraudulent credit card number.

- Since there are so many free email services, how do you know if the order you receive is from one of these free email services? You can check a list of 700+ of these free email services.

- You can also find an excellent article published at this same site, which provides a good (although not foolproof) suggestion for verifying email addresses: check every Email address by typing "www" in front of the domain name of the email address into your browser.

- For example, if you got an order addressed from audri@scambusters.org and you typed www.scambusters.org, you'd get to the ScamBusters Web site, which is a legitimate Web site. Or, if you got an order from sallysmith@netcom.com, you'd type in www.netcom.com and you'd be at a legitimate ISP. On the other hand, the article suggests that if you got an order from joesmith@cyberdude.com and typed in www.cyberdude.com, you'd find yourself at a site which offers 150+ free email domains. (I'm not saying cyberdudes, juno, hotmail, etc. are not legitimate. Rather, I'm suggesting that orders that come from these free email services warrant additional care and attention.)

    - What precautions should you take with orders from free email accounts? How about sending an email requesting additional information before you process the order. More specifically, ask for: a non-free mail address, the name and phone number of the bank that issued the credit card, the exact name on credit card, and the exact billing address. Often, you won't get a reply. If you do, you can easily verify the information (which you should take the time to do).

- Be especially wary of orders that are larger than your typical order amount, and orders with next day delivery. Crooks don't care what it costs, since they aren't planning on paying for it anyway.

- Pay extra attention to international orders. Do everything you can to validate the order before you ship your product to a different country. Some merchants won't ship international orders which have different "bill to" and "ship to" addresses.

- If you're suspicious, pick up the phone and call the customer to confirm the order. It will save you a lot of time and money in the long run.

- Consider using software or services to fight credit card fraud online -- sources such as Cybersource or Clear Commerce Corp.

- If you (as a merchant) do have the misfortune of being scammed by a credit card thief, you should contact your merchant processor immediately and inform them of the situation. You should also contact your bank and the authorities as well.

Additional Law Enforcement Resources

Federal Trade Commission (FTC)

The FTC is very interested in this type of crime. They will review reports from foreign victims when the operation is US-based. Complete the online form at http://www.ftc.gov/ftc/complaint.htm so you are eligible for reimbursement. They usually act when they receive many complaints.

Secret Service

The U.S. Secret Service has jurisdiction over credit card and access-device crimes if the credit card is underwritten by a U.S. bank. However, they consider the bank to be the injured party, and not the card holder (who is theoretically reimbursed by the bank). They are also not set up to deal with many small losses. They generally don't have the manpower to go after anything less than $100,000. Many local law enforcement agencies, likewise, are reluctant to get involved due to manpower constraints and the detailed, lengthy investigations involved when the loss is not great. Additionally, since the merchant generally is the loser, not the cardholder (the merchant takes the loss 99+ percent of the time) there is frequently a jurisdictional issue.