

# Identity Theft

## Thieves Steal 30,000 Identities<sup>1</sup>

Following a year-long investigation, Federal authorities arrest three men they say systematically stole and resold the identities of more than 30,000 Americans. The three men, all believed to be of Nigerian decent, operated from a base in New York. According to sources, the three were assisted by a help-desk employee working for a New York telecommunications company who provided them credit reports and passwords. The same sources said that the victims, from as many as 48 states, so far have lost more than \$2.7 million, but that the losses could eventually be much greater. The thieves drained bank accounts and ruined the credit of tens of thousands. Prosecutors said the three men were part of a ring that sold credit reports to street criminals for as little as \$60.00 each. If convicted, each face penalties of up to 30 years in prison.

### How to Protect Your Identify:

- ◆ Keep credit cards, personal identification and passwords in a safe place
- ◆ Never carry more credit cards or cash with you than you need
- ◆ Report the theft of credit cards or personal identification immediately
- ◆ Carefully examine your credit card bills and look for charges that may not be yours
- ◆ If you must give your credit card number over the telephone, ensure no one is eavesdropping
- ◆ Destroy or safely store all credit card offers, receipts and bills when finished with them

---

<sup>1</sup> The following articles have been compiled from issues of the Security Headlines newsletter. Security Headlines is a monthly newsletter published by [Business Controls, Inc.](#), exclusively prepared for its clients and those in the security industry. For more information about Business Controls, Inc. or its newsletter services, call 800.650.7005.

## Thieves Steal the Identity of 500,000 Military Members

In what may be the largest case of ID theft yet, patient records, Social Security numbers and even some credit card numbers from over 500,000 military users of the TriCare health system were recently stolen. The theft occurred at the Phoenix offices of TriWest Healthcare Alliance. The news sent shivers through the military community who feared a possible terrorist link. Not likely say experts. Like many of the big ID thefts of the recent past, this one was most probably the handy-work of insiders. The damage could still be enormous. The typical ID theft victim spends over \$1,100 and 200 hours repairing their good name and credit.

The Federal Trade Commission's annual report detailing consumer complaints showed identity theft topped the list. The number of fraud complaints jumped from 220,000 in 2001 to 380,000 in 2002 and the dollar loss consumers attributed to the fraud they reported grew from \$160 million in 2001 to \$343 million in 2002.

Identity thieves may work in the following ways:

- ◆ They open a new credit card account, using your name, date of birth and Social Security number. When they use the credit card and don't pay the bills, the delinquent account is reported on *your* credit report.
- ◆ They call your credit card issuer and, pretending to be you, change the mailing address on your credit card account. Then your imposter runs up charges on your account. Because your bills are being sent to the new address, you may not immediately realize there's a problem.
- ◆ They establish cellular phone service in your name.
- ◆ They open a bank account in your name and write bad checks on that account.

## Identity Theft Continues to be a Growing Problem

Incidents of identity theft in the United States have steadily increased over the last several years much to the dismay of lawmakers and law enforcement. FBI bank-fraud expert, Agent Ben Berry, says that the Internet and all the information it makes available is the principal reason for the increase. The Internet provides a cloak of anonymity so businesses and governments have stepped up their efforts to protect the credentials of consumers and identify fraud more quickly. Phillip Cummings was arrested in November for his alleged involvement in the biggest case of ID theft yet. According to authorities, Cummings netted \$2.7 million selling information stolen from his employer, Teledata Communications. The matter is still under investigation.

**Fact:** *Spam costs employers roughly \$1000 per year, per Internet connected employee. Every day, the average U.S. email account receives one spam message for every legitimate message. (Source MailWatch, 2003)*

## **Net Fraud: A Growing Problem**

The FBI and National White Collar Crime Center report that online auction fraud was by far the most reported Internet offense last year, and that the average loss for those who filed complaints was \$395. According to the FBI study nearly 10,000 people reported losing \$17.8 million through Internet scams. Of those reported, 43 percent involved online auctions. Law enforcement says prosecution and recovery are difficult, at best. The problem stems from weak laws, jurisdictional conflicts and scarce resources. However, to help overcome buyer concerns, on-line auction house, eBay now offers the “*Power Seller*” designation to its best vendors. To obtain the moniker, the eBay vendor must have at least a six-month track record on the site and do about \$2000 a month while maintaining a high, 98% positive feedback rating.

Nigerian letter fraud, one of the fastest growing scams on the Net, accounted for 16 percent of complaints. But those duped by the Nigerian letter fraud scam lost an average of \$5,575, the most of any scam. According to Susan Grant of the Internet Fraud Watch, a division of National Consumers League, “It used to not be in the top 10 of Internet frauds, and now its No. 3!” And although, Nigerian money offers have been around for decades, the number of victims has exploded because of the fraudsters use of the Internet.

The potentially dangerous scam involves a person who claims to have millions of dollars locked in a bank account controlled by an oppressive foreign government and wants to transfer it to a U.S. account. The perpetrator requests a fee from the victim in exchange for a percentage of the transfer, often topping 50 percent. Of course the only money exchanged is that which belongs to the victim. In some cases the victim is even lured to some remote and lawless corner of the world, kidnapped and then ransomed. For more information go to [www.fraud.org](http://www.fraud.org) or call your local FBI office.

## **Theft-proof Credit Cards**

Need to make a large purchase online, but are afraid to use your credit card? While online security is better than ever, the theft of credit card numbers and account information is still a problem. In response, [American Express](#), [Discover Card](#) and some MasterCard issuers now offer single use credit card numbers. The number expires after one purchase. To sign up, log on to your card company’s Web site and obtain a username and password and a disposable card number will be instantly issued. To get another number, log back on again and repeat the process. The service is free and comes with several perks, including award points and fraud insurance. Issuers report these one-time use card numbers are popular and protect everyone, including *them*.

## **Pass Me the Password Please**

Combine a readily available cracking application with a simple dictionary file and chances are any hacker could crack most of the passwords protecting your systems.

As simple as it sounds, this type of “brute force” attack is one of the most common among hackers.

Password cracking doesn't always have to take a high tech approach to be successful. Finding a sticky note on a computer or under a keyboard is fairly simple. Because most passwords are so simplistic, crackers often use tools that literally try every word in the dictionary. Add a hybrid module and this same program starts adding numbers and symbols to these words. According to security experts at Carnegie Mellon University, well over a million passwords have been stolen on the Internet.

Ineffective passwords include common words, the same words spelled backwards, or words with numbers added at the end. Users who are comfortable with a password will often start off with the word, and when prompted monthly to change their password, will simply add a digit. So what starts in January as “Snoopy” ends up in December as “Snoopy 11.” Avoid family member's names, pet's names, and Social Security numbers.

An effective strategy is to use a combination of upper and lower case letters in conjunction with symbols and numbers. Some examples might be:

- ◆ Time+Effort=\$
- ◆ IThinkThere4Im
- ◆ \$howMeThe\$

For more information, go to [www.106.ibm.com/developerworks/security/](http://www.106.ibm.com/developerworks/security/).

## **Check Washing**

Although the public's concern about identity theft and the information they share while online is well placed, security experts say consumers should also be concerned about what they put in the mail. Check washing has become a popular new crime. The process, which uses chemicals to wash away the written ink from a stolen check, allows criminals to rewrite a check in any amount they please. The washer obtains signed checks by stealing them from residential mailboxes. He photocopies and washes them in a chemical solution to remove all handwritten ink. The washer then rewrites the check and forges the original signature. Some enterprising washers set up washing stations in their vehicles. It is possible that some stolen checks are washed, dried, forged and cashed in less than 45 minutes. Here's what to do to protect yourself and your checks:

- ◆ Pay your bills electronically. Most major banks offer electronic payment services. The convenience is safe and saves time and money.
- ◆ Take your mail containing checks directly to the Post Office. Do not leave them in your mailbox for pickup.
- ◆ Sign checks with indelible black ink. Do not use felt-tip pens or pencil.
- ◆ Keep unused checks in a safe place. Destroy all unused checks from closed accounts.
- ◆ Review your bank statements carefully. Notify your bank immediately if you suspect someone has altered or forged one of your checks.

## Gone Phishing

Spam and malicious code in the form of viruses and worms are the modern evils of our electronic world. According to security specialist MessageLabs, last May, spam accounted for 50% of all business email traffic in the U.S. for the first time. In November, in response to the SoBig and Blaster viruses, which exploited vulnerabilities in its software, Microsoft offered a \$250,000 reward to anyone who could lead it to those who created the viruses. Experts believe that criminals will next combine spam with viruses. Hackers have already given the scheme a name, dubbing the mass distribution of spoofed email messages with return links that appear to come from reputable businesses, *phishing*. Some customers of eBay, PayPal and other online vendors have already been victims. Says one IT security manager, "It will only get worse. The Internet will remain wild and dangerous well into the 21<sup>st</sup> Century."

### Top 10 Viruses / Worms of 2003

Name	Number of Interceptions	Description
SoBig.F	32,000,000	"Re: Your wicked screensaver
Swen.A	4,000,000	Masquerades as a Microsoft security update
Klez.H	4,000,000	Comes disguised as free inoculation tool
Yaha.E	2,000,000	Free screensaver
Dumaru.A	1,100,000	Bogus Microsoft security patch
Mimail.A	1,000,000	Bogus PayPal email and URL to capture credit card info
Yaha.M	900,000	Delivers DOS attack against remote machines
SoBig.A	800,000	Harvests email addresses
BugBear.B	800,000	Captures victim's key strokes and disrupts network printers
SirCam.A	500,000	Deletes files and consumes disk space

Source: CFO Magazine, 2004

## Your E-mail Isn't Safe Either

Most cyber-users know e-mail messages are neither secure nor private. But privacy advocates have recently issued new a warning that e-mail may be less confidential than people thought. A recent First Circuit Court of Appeals decision suggests that e-mail's mode of transmission—hopping from computer to computer—does not fit the definitions of "electronic communications" in federal

wiretap laws says the advocates. If so, the privacy protections that once thought to exist when using e-mail may not exist at all. In response, security and legal experts have issued their own warning:

- ◆ Do not send messages, which if compromised, would embarrass you or your organization.
- ◆ Read your e-mail service provider's privacy statement. Ensure it promises that your messages will not be read by the provider or shared with others without your permission.
- ◆ Consider using encryption software. A Google search while writing this article for the term, *encryption software* yielded approximately 3,030,000 results.
- ◆ Do not use instant messaging (IM) for confidential communications.
- ◆ Before giving away that old computer, remove the hard drive and destroy it.

*Best advice: When in doubt, use the telephone for personal communications. For the exchange of sensitive business information use an Application Service Provider (ASP). ASPs store confidential information like employee records and reports on remote, secure servers. The information is not transmitted over the Internet, instead users simply "view" the information.*

### **Ingredients for Identity Theft Soup Found in Politicians' Cupboards**

Provisions of U.S. Rep. E. Clay Shaw's Social Security Number and Identity Theft Prevention Act of 2004 and S 2801, its companion bill introduced by Senator Dianne Feinstein, would shut businesses off from the use of personal identifying information for legitimate purposes. In the name of identity theft protection, these privacy measures would eliminate civilian crime fighters' abilities to perform their professional duties, disrupt judicial processes and restrict other important business activities in the banking and insurance industries. However, Congress may not be aware that lurking within politicians' offices are all the ingredients needed for criminal abuse of their constituents' personal identifying information.

Political candidates frequently rely on voter registration data to advance and financially fortify their campaign efforts. For example, in the Commonwealth of Virginia (and other states), political candidates are allowed to obtain the following voter data: full name, residence/mailling address or both, gender, date of birth, date of registration, and voting history. In and of itself this information, while personal, is rather benign, with name and address information readily available from telephone directories, commercial mailing lists, or other public record resources. However, once indexed and matched to the signatures of voters collected on a petition during a political campaign, one has nearly all the ingredients necessary to perpetrate the crime of identity theft.

"Further add to the mix telephone or door-to-door campaign [soliciting] during which volunteers speak with voters gaining their trust and confidence, and one

unscrupulous campaign worker who requests a social security number and mother's maiden name 'for the record.' A criminal now has the finishing ingredients for identity theft soup," says Deborah Aylward, a prominent private investigator in Virginia. Based on her professional experience with actual cases of identity theft, Aylward claims it is reasonable to think that this type of scenario could occur. According to Aylward, "There is no statutory requirement mandating the protection of voter registration information [including] donor financial information and signatures, or that persons working for political candidates be subject to criminal background [checks]." Aylward reminds voters, "Let's not forget the fact that anyone touting a voter registration form may obtain personal identifying information [from a citizen]. Voter registration information can be solicited and collected by anyone using a Web site, collected at places of employment, [or] by members of religious and civic organizations, just to name a few. The potential for criminal abuse of these records is enormous."

"It is abundantly clear that political candidates are the most voracious consumers of personal identifying data contained in voter registration information," says Aylward. She summarizes, "However, current privacy proposals [such as HR 2971 and S 2801] do not impose identity theft safeguards upon politicians [and their campaign activities]. It would seem that what's good for the goose is good for the gander. [We] suggest that Congress slow the rush to pass identity theft legislation until all adverse consequences are thoroughly understood, explored, debated and resolved."

*Contributed by [Deborah Aylward](#), 703-205-9692. Edited with permission.*

## **The Check is in the Mail**

Paper check processing and the afternoon bank run are about to become history. Using a new technology, retailers and other businesses can now swipe a check and instantly transfer money from a customer's account into their own. Effective October 28, 2004 America's banks are allowed to exchange checks electronically instead of using paper versions. Signed into law last year, the Check Clearing for the 21<sup>st</sup> Century Act, better known as "Check 21," is expected help checks clear faster and eventually eliminate the need for paper checks all together. For the first time, last year, the number of electronic payments made by Americans topped the number of check and cash payments. The decline is expected to continue. The Federal Reserve, which processed some 16 billion checks last year, has begun to shutter some of its check-processing facilities around the country. For years, the check-clearing process involved the handling of paper checks and passing them from institution to institution. The labor-intensive process was expensive and time consuming, often allowing checks to "float" and check writers days to cover a check written against accounts with insufficient funds. With Check 21, banks now have the option of sending digital images of the check instead of the actual check. Businesses are keen on the idea, hoping they will no longer get stuck with bounced checks and items returned NSF (non-sufficient funds).

## Best Check Fraud Self-Defense

Security experts agree that it is only a matter of time before criminals figure out ways to find and exploit security holes in Check 21's new check processing technology. In the meantime, consumers can do more to protect themselves. Here's what we recommend:

- ◆ Never make checks payable to *Cash*.
- ◆ Order your checks from your bank. Mail-order checks are often less expensive but typically are easier to alter than bank checks.
- ◆ Protect deposit slips. A common scam is to deposit worthless checks into your account and get some of the deposit back as cash.
- ◆ Review all deposited checks and ensure they are still made out to and endorsed by the original intended party.
- ◆ Protect your signature. Use your real signature for checks and important documents; use another for forms, questionnaires and other routine documents.
- ◆ Report suspicious transactions to your bank immediately. The sooner the bank is aware of problem, the sooner it can investigate it and take corrective action.

**Fact:** *More than 1.3 million worthless checks are written every day.*

*Source: Boardroom Inc., 2004*