Illinois Criminal Justice Information Authority

Research Bulletin

Vol. 5, No. 3 October 2006

Technological innovation fuels identity theft fraud epidemic

By Sal Perri, ICJIA research analyst

Stealing a person's identity is a relatively new type of crime, but one that is threatening to become epidemic as technology evolves and provides innovative techniques to capture victim information. Unsuspecting millions of Americans already have been exposed to this crime.

In a recent case, a computer containing personal data of 26.5 million veterans discharged since 1975 was stolen from the home of a U.S. Department of Veterans Affairs analyst.[1] The stolen electronic files also contained personal data for 1.1 million active-duty military personnel, 430,000 National Guard members, and 645,000 reserve members.[2] The employee, who was not authorized to remove the computer from his office, was subsequently fired and the computer with the data, reportedly not accessed, was recovered.

Due to at least 15 major data breaches, millions of Americans in 2005 were also victims of large-scale information fraud. ChoicePoint Company sold private consumer data to con artists posing as legitimate executives, triggering a surge of identity theft disclosures for months. Discount Shoe Warehouse Inc. had data for 1.4 million consumers stolen; CitiFinancial, data for 3.9 million customers stolen; Bank of America, data for 1.2 million government workers stolen; and MasterCard was hit by a data heist that could affect 40 million credit card users.[3]

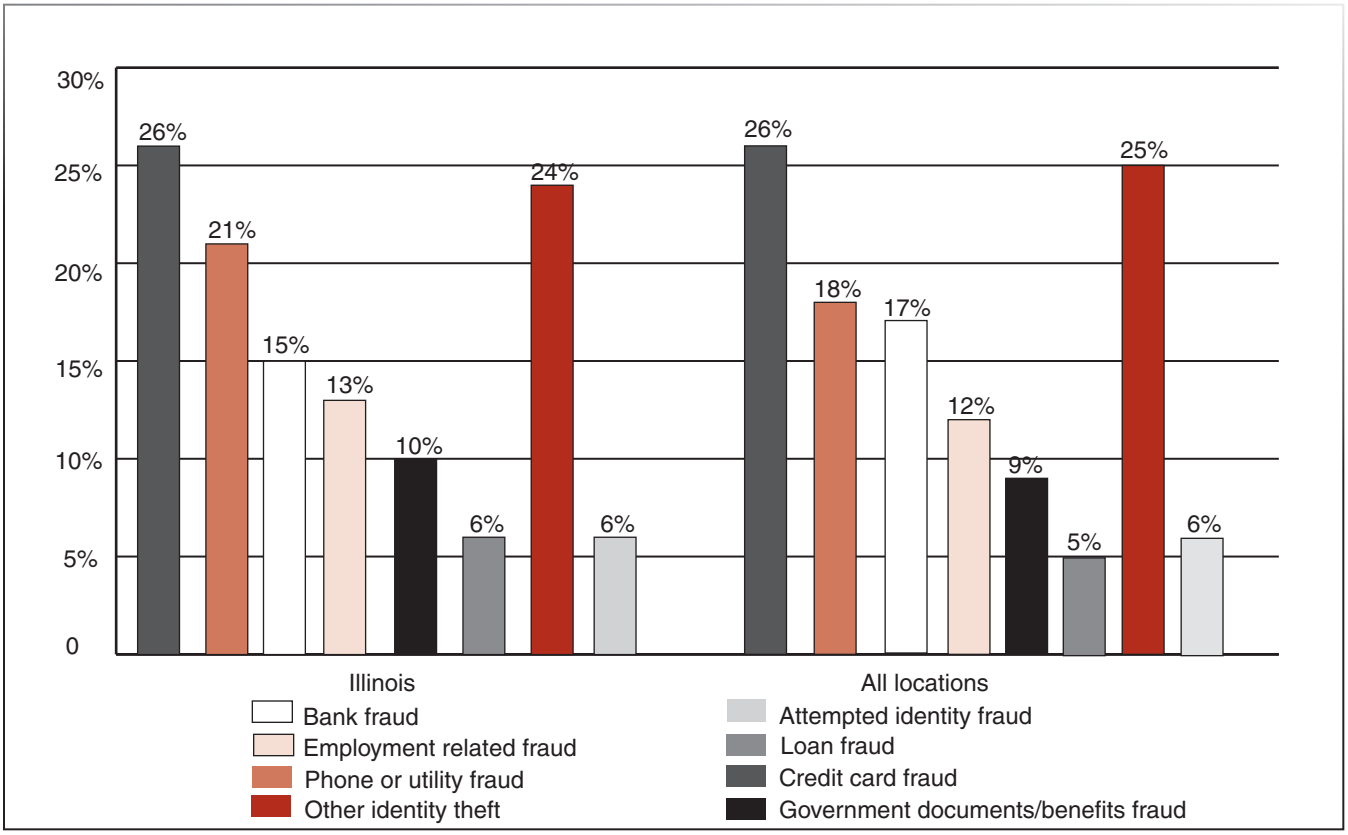
Federal Trade Commission (FTC) Identity Theft Clearinghouse Data statistics indicate 685,000 consumer fraud and identity theft complaints were received in 2005. Of those, 37 percent were identity-theft related, and consumers reported more than $680 million in losses from fraud.[4] In 2003 the FTC estimated identity theft cost businesses, governments, and consumers more than $53 billion a year.[5]

Defining identity theft

The taking of a person's identity for financial gain, to obtain credit or credit cards, steal money from a victim's accounts, apply for loans, establish accounts with utility companies, rent an apartment, or find employment all constitute identity theft or identity fraud. Offenders can steal someone's identity by using their social security number, birth date, address, phone number, or any other personal information. With this

This project was supported by Grant #03-DB-BX-0037, awarded to the Illinois Criminal Justice Information Authority by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. Points of view in this document do not necessarily represent the official position or policies of the U.S. Department of Justice.

Figure 1
How victims' information is misused Jan. 1 to Dec. 31, 2005



Source: Federal Trade Commission Identity Theft Victims Complaints Data released Jan. 25, 2006

information and a fraudulent driver's license, identity theft can be accomplished by applying for credit. To avert detection, identity thieves often use their own address and claim to have moved since credit grantors do not verify personal information or addresses. Once the thief is able to open one account, the account can be used with other identifiers to add credibility.

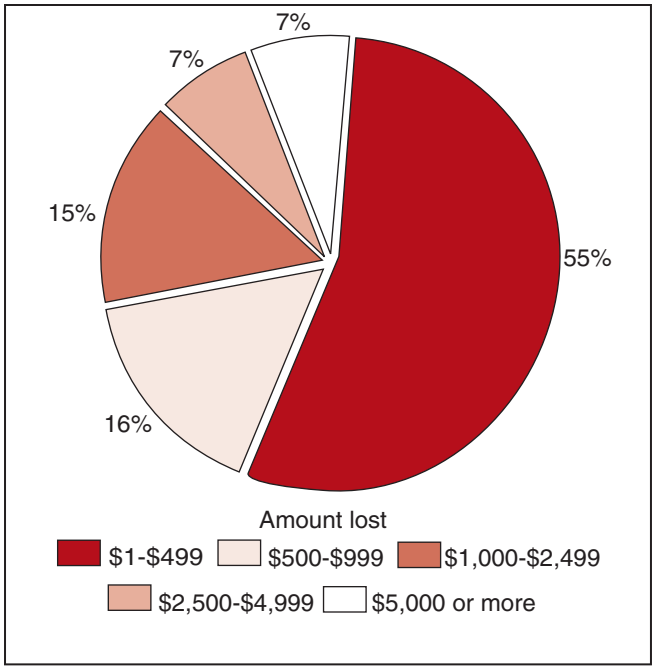
An identity thief can gain access to personal information in several ways. Employees of a victim's doctor, accountant, lawyer, dentist, school, health insurance carrier, and other businesses may access personal information. Confidential information is in unshredded utility bills, credit card slips, and other documents found in garbage. The Internet, mailboxes, the courts, and recorded public documents furnish personal data. If a thief gathers enough information to get someone's credit report, he can steal thousands of dollars without a victim's knowledge, and use a person's identity to commit other crimes.

Skimming credit cards

An emerging threat is the use of a skimmer device to steal credit card information, which can then be used to make fake cards, purchase items, or provide data for identity theft. A skimmer, similar to a credit card reader commonly used in shopping malls, looks like a small pager with a slit for swiping cards to record personal information. Its memory can store data for 500 credit cards for computer downloading. Anyone with access to consumer credit cards during the course of a business transaction can skim, and crime syndicates target low-wage or part-time workers to skim cards.[6]

Credit card skimming is a worldwide problem whose annual losses exceed $1 billion. Skimming and counterfeit credit card fraud is widespread in Europe, Asia, and Latin America, and is a growing problem in the United States.[7] Small-scale skimming operations, already are reported to be common. In a Florida case, two servers skimmed a large number of credit cards from an Orlando restaurant and sold the data to an intermediary, who then sold it to Miami credit card counterfeiters.[8]

Figure 2
Percent of households experiencing identity theft by amount lost in theft ($1 or more)



Source: Identity Theft, 2004, National Crime Victimization Survey, Bureau of Justice Statistics

Phishing

Phishing, pronounced "fishing," is the creation and use of e-mail messages and websites designed to look like e-mails and websites of well-known legitimate businesses, financial institutions, and government agencies. Internet users are deceived into disclosing bank and financial account information or personal data such as user names and passwords, and "phishers" use that information for criminal activities involving identity theft and fraud.

Most phishing e-mails include false statements that create the impression of an immediate threat to a victim's bank, credit card, or financial account. Phishing e-mail messages often claim an unauthorized person has been using the recipient's credit card or that a recent credit card transaction has been declined. Some phishing messages promise a prize or other special benefit, but the objective is the same: to trick victims into disclosing financial and personal data.

Some identity thieves use spamming, or mass e-mailing, to send a computer message to thousands of users. Phishers anticipate that some recipients have an account or customer relationship with the legitimate business or company being misrepresented, and therefore may be more likely to believe the message has come from a trusted source.[9]

Ultimately, people responding to phishing e-mail messages put their accounts and financial status at risk by providing data phishers can use to:

- Access existing accounts of Internet users for withdrawals or purchase of expensive merchandise or services.
- Disseminate phishing e-mail messages to more people via computer viruses and worms.
- Open new bank or credit card accounts in victims' names and use the new accounts to cash bogus checks or buy merchandise. If phishers open new accounts in the victims' names but do not use their addresses, victims may not realize they have become identity theft targets until creditors contact them or they check their credit reports.[10]

Law enforcement authorities, businesses, and Internet users are observing an increase in phishing. According to the IBM Global Business Security Index monthly report, based on the work of 2,700 information security professionals monitoring 500,000 network systems, incidents of phishing attacks jumped more than 226 percent from April to May 2005. MessageLabs Ltd., an e-mail security company that collects phishing statistics in partnership with IBM, tracked 9,139,704 phishing e-mails in May 2005, topping the previous record of 7,724,659 in April 2005.[11]

Pharming

Identity thieves have developed another technological weapon known as "pharming," similar in nature to phishing. Both aim to hijack web-surfers' personal information, but whereas phishing uses direct e-mail, pharming focuses on particular Web domains used on a daily basis by web-surfers accessing their registered accounts. Pharming is much more difficult to prevent and it can affect multiple users per attack due to the high volume of web-surfer visits.

The simplest form of pharming targets a customer after he or she types a Web address into an Internet browser attempting to visit a Web page. The browser locates the Web page using the domain name service, which is translated into a numerical Internet Protocol address, and is then viewed on the web surfer's computer.

Pharming comes into play once the web surfer inputs the Web address and a server begins searching for the correct address. The identity thief quickly hacks into the server and redirects the request to a phony address that looks identical to real Web page. By the time the web-surfer logs onto the apparently legitimate website with a user name and password, the identity thief has already hijacked the surfer's information. Identity thieves are able to deceive everyone who attempts to log onto a compromised website, making detection extremely difficult while permitting access to mass amounts of personal information.

In many cases, a computer virus accomplishes the pharming techniques. Recently, banking and investment companies including Barclays, HSBC, Lloyds TSB, and NatWest were victims of a virus that was discovered more than 40,000 times on the Internet since its first appearance in February 2005. Pharming is rapidly becoming the most advanced and undetectable fraud technique.[12]

Spoofing

Spoofing is the telephone industry's version of phishing. Identity thieves can manipulate the phone number and name displayed on a victim's caller ID, allowing them to pose as officials from a church, bank, or court, with the purpose of getting social security number or other sensitive information from them. Spoofing does not require a large investment, and a number of businesses specialize in it, including SpoofCard.com, which sells cards for as little as $10 for 60 minutes of talk time. SpoofCard users can request that an altered male or female voice substitute for their own, so that although a thief speaks normally, the person called hears an altered voice. Because a legitimate institution's name and phone number display on a victim's caller ID, the spoofer may persuade the consumer to divulge credit card or other personal information, at which point the thief can begin fraudulent use of that information.

The American Association of Retired Persons' alerted members to spoofing in its May 2006 monthly bulletin, coincidentally the same month the Federal Trade Commission filed its first case alleging the transmission of bogus caller ID information against a mortgage loan provider. One of the charges against the mortgage provider was that the company violated telemarketing rules by transmitting a phony caller ID, which made it impossible for consumers to stop its unwanted pitches.[13]

Throughout the country, caller ID users are being subjected to a scam that fakes a phone call from a court official using the official's actual phone number on caller ID display. A phone-scam alert even appears on the website of the U.S. District Court in Washington. St. Thomas Orthodox Church in Fairlawn, Ohio, received hundreds of calls over a five-month period from people reporting that the church phone number appeared on their caller ID when a caller, who claimed he was owed money, asked for their bank account number.[14]

The Truth in Caller ID Act, passed June 6, makes it a crime to transmit misleading caller ID information with the intent to defraud or harm.

Medical identity theft

Medical identity thieves use victims' names or insurance information to get medical treatment, buy prescription drugs, or be reimbursed by insurance companies for services never received. According to the World Privacy Forum, the perpetrators are often professional thieves selling pills and medical supplies online, but sometimes a doctor will file false insurance claims for patients and non-patients. False entries made to health care records could mean patients might be treated based on someone else's medical history.

Discovery of medical identity theft might not occur until long after commission of a crime. Often discovery comes when a bill collector calls a victim, or when an insurer will not pay a bill because a thief's claims put victims over their insurance limit.[15]

The World Privacy Forum recently issued a report estimating that medical identity theft in 2003 ranged from a minimum of about 3,500 victims to a maximum of almost 3.25 million victims. The best estimate is a quarter to a half million people have been victims of this crime.[16]

Methamphetamine and identity theft

Postal inspectors and law enforcement personnel are finding that identity thieves often are meth addicts. Postal inspectors say meth is the perfect companion for identity theft, because the drug enables addicts to stay awake for several days and provides the patience and energy to perform obsessive-compulsive repetitive

Table 1
Consumer awareness tips

Prevent access to your personal information
Do not release Social Security or account numbers in response to e-mail, phone or in-person requests. When responding to e-mail, ignore any Internet links provided and type the full address instead. Do not carry your social security number or give it to anyone unless necessary. For abuse of your social security number, call the Social Security Administration's fraud hotline at (800) 269-0271 or file a Fraud Reporting Form at http://www.ssa.gov/oig/public_fraud_reporting/index.htm.
Be aware of your surroundings whenever you take your credit card or other identifying documents out of your wallet.
Keep all sensitive documents, checkbooks and credit cards securely locked away at home and at work. Or store sensitive documents in a safety deposit box at your local bank.
Carry only those credit cards that you need in your wallet.
Before discarding sensitive documents shred them.
Retrieve paper mail promptly and place outgoing checks or other sensitive documents in a U.S. Postal Service mailbox.
Sign up for automatic payroll deposits.
Replace paper bills, statements and checks with online (paperless) versions.
Keep passwords hidden (even in your own home) and change the hiding place frequently.
Use and regularly update firewall and anti-virus software. Visit http://OnGuardOnline.gov for more information.
Do not respond to suspicious e-mails. Delete them, and if there is any doubt contact the company to determine if the e-mail is real. Never click on links sent in unsolicited emails; instead, type in a Web address you know.
Do not discard a computer without destroying the data on the hard drive.
Detect unauthorized activity
Review bank, credit card and billing statements regularly usually available through online account access. Contact your financial provider if you fail to receive statements in a timely manner.
Review your credit information regularly (free yearly reports are available at http://www.AnnualCreditReport.com or call 1-877-322-8228. You also can write Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281).
Use e-mail-based account "alerts" to monitor transfers, payments, low balances, withdrawals, or detect any out-of-pattern activity.
Visit your bank, credit card issuer or biller's Web site(s) frequently to monitor regular account activity.
Resolve the fraud immediately, minimizing losses and protect your credit record
Ask your financial provider about zero-liability guarantees against fraud and dedicated resources to help you resolve and recover from any potential financial losses.
Victims of identity theft notify your financial providers, begin monitoring your accounts more frequently, and place an "fraud alert" with all three credit bureaus: Experian at (888) 397-3742, Equifax at (800) 525-6285, and TransUnion at (800) 680-7289.
If you suspect or detect identity fraud, alert federal and local law enforcement by filing a police report. Report it to the Illinois Identity Theft Hotline by calling 1-866-999-5630 and review the Identity Theft Resource Guide at http://www.ag.state.il.us/consumers/Identity_Theft_Resource_Guide.pdf.
Check guarantee companies can also help if checks have been stolen or if phony bank accounts are set up in your name. Call Telecheck at (800) 366-2425 or visit their web site at http://www.telecheck.com and contact the National Processing Company at (800) 526-5380.

tasks, such as making counterfeit checks or stitching together shredded documents.[17]

Methamphetamine can be manufactured in small transient laboratories that move around suburban or rural areas, locations where addicts can more easily steal mail from unlocked mailboxes. Small-scale meth manufacturers often use stolen identities to buy drug-making ingredients or to pay rent without arousing suspicion. In 2005 in Phoenix, Ariz., which has the nation's highest rate of identity theft complaints, officials first became aware of the identity theft-meth connection when laboratory raids discovered stolen mail and checks that had been washed with acetone, a chemical used to make methamphetamine. In Minnesota, meth users have developed a barter economy to trade items such as washed checks, stolen checkbooks, drugs, meth ingredients, and equipment.[18]

A recent National Association of Counties survey of 500 law enforcement officials determined meth abuse increased identity theft by 27 percent.[19]

Victims of identity theft

According to a 2006 Identity Fraud Survey Report released by the Council of Better Business Bureaus and Javelin Strategy & Research, in 63 percent of fraud cases a victim's information was obtained from close associates, such as friends, family, and neighbors; from lost or stolen wallets, cards or checkbooks, or stolen mail; from breaching home computers; or from information taken from trash.

In 63 percent of cases, the survey indicated preventing fraud was under the victim's control, and consumer awareness was primary in preventing fraud. Statistics showed identity theft cost U.S. consumers 4 percent more in 2005 than the $54.4 billion identity theft cost in 2004, and that the average fraud theft amount rose to $6,383 in 2005 from $5,885 in 2004. But the number of adult Americans who experienced identity theft and fraud is trending downward, falling from 10.1 million in 2003 to 9.3 million in 2004, to 8.9 million in 2005. Data also indicated that younger people and lower-income groups are more vulnerable to identity theft fraud.

In 2005 almost half the victims themselves discovered their identities had been stolen, and growing consumer awareness has had a positive impact in averting thefts. In 2003 consumers took 101 days to identify identity

Table 2
Households experiencing identity theft

Household characteristics	Number	Percent of all households
Total	3,589,100	3%
Race of head of household		
White	2,930,900	3.1%
Black	481,300	3.3%
American Indian Aleut (Alaska Native)	15,800	3%
Asian, Pacific Islander	124,300	2.8%
More than one race	36,800	4.3%
Hispanic	319,300	2.6%
Non-Hispanic	3,250,600	3.1%
Age of head of household		
18-24	363,600	4.6%
25-34	654,700	3.3%
35-49	1,223,100	3.4%
50-64	938,200	3.3%
65 or older	410,600	1.8%
Household income		
Less than $7,500	115,400	2.2%
$7,500-14,999	222,500	2.6%
$15,000-24,999	235,700	1.9%
$25,000-34,999	367,300	3.2%
$35,000-49,999	472,900	3.3%
$50,000-74,999	513,800	3.4%
$75,000 or more	1,086,700	5.2%
Urbanicity		
Urban	1,221,500	3.6%
Suburban	1,918,200	3.2%
Rural	449,300	2%

Source: Identity Theft, 2004; NCJ 212213 by Katrina Baum, Ph.D., National Crime Victimization Survey, Bureau of Justice Statistics.

theft, but by 2005 that number fell to an average 67 days. The average fraud amount declined from $8,466 in 2003 to $4,431 in 2005, and the cost of identity recovery per consumer came down from $538 in 2003 to $347 in 2005. Checking credit-monitoring reports remains one of the most effective ways of detecting identity theft, as the survey determined monitoring caught about 11 percent of fraud cases.[20]

A 2004 study by U.S. Justice Department's Bureau of Justice Statistics estimated that 3.6 million, or 3 percent, of households have been affected by identity theft at a cost of $6.4 billion a year. According to the study, 48 percent of households experienced unauthorized use of credit cards, 25 percent unauthorized use of banking accounts, and 15 percent unauthorized use of personal information. The remaining 12 percent experienced multiple identity thefts.

The report stated 4.6 percent of households headed by persons age 18 to 24 were more likely to experience identity theft than others, while 1.8 percent headed by persons ages 65 or older were least likely to experience it. Households in the highest income bracket, $75,000 and over, were the most likely (at 5.2 percent) to be identity theft victims, while rural households were less likely targets (2 percent), than urban households (4 percent), or suburban households (3 percent).[21]

Illinois perspective

The FTC ranked Illinois 10th in 2005 of states reporting identity theft with 11,137 complaints and a rate of 87.3 victims per 100,000 population.[22] Similarly, the state ranked 10th in 2004 and 9th in 2003 in identity theft reporting.[24]

Among Illinois cities, Chicago tallied 4,088 identity theft victims in 2005 and Rockford had 180 victims, but Chicago suburbs had much fewer incidents of identity fraud. Victim number have shown little fluctuation since 2003.

The most frequent types of identity theft in Illinois in 2005 included credit card fraud (26 percent), phone or utility fraud (21 percent), and checking/savings/electronic fund transfers fraud (15 percent). In all cases, only slight percentage changes occurred since 2003.

Illinois is one of six states with personal data freeze and security breach notification laws. Personal data freeze laws allow consumers to restrict access to credit reports and block the opening of new accounts in their names. Security breach notification laws require prompt notification when an individual's personal records have been stolen from a company storing them.[25]

In June 2005, Illinois increased penalties for identity theft, making it a Class 4 felony for thefts up to $300; Class 3 felony for offenders previously convicted of identity theft of less than $300, or previously convicted of any type of theft, robbery, armed robbery, burglary, residential burglary, possession of burglary tools, home invasion, home repair fraud, aggravated home repair fraud, or financial exploitation of an elderly or disabled person; and a Class X felony for thefts exceeding $100,000.[26]

Twice in the past year personal information of thousands of Illinois state workers was found in dumpsters, prompting the legislature to make it a felony for state employees to knowingly discard sensitive personal data. The Privacy Rights Clearinghouse reported that more than 200 publicly disclosed cases of sensitive personal data were lost or stolen in 2005 and during the first 6 months of 2006, the majority of which involved federal, state or local agencies. Since the beginning of 2005 the personal data of 88 million people was exposed due to security breaches.[27]

The future

Creation of the Identity Theft Hotline, 1-866-999-5630 (TTY: 1-877-844-5461), by the Illinois Attorney General's Office is intended to assist the criminal justice system in the investigation, arrest, prosecution, and conviction of identity thieves. The hotline provides victims one-on-one assistance in reporting identity theft to local law enforcement and financial institutions, repairing their credit, and helping prevent future problems. Statistics indicate 61 percent of identity theft victims do not notify the police. Illinois requires police departments to take an identity theft report from a victim, but in other states 9 percent of victim reports are not taken by police.[28]

A new threat to consumer information involving gangs recently was uncovered. The first major study of Chicago area gangs by the Chicago Crime Commission found that although gangs generate most of their money from illegal drugs, some are getting into crimes such as mortgage fraud and identity fraud and theft.[29] In response to this growing threat to the public, government officials

seek to enhance detection, public awareness, citizen outreach and education, and criminal justice system training in this area. In the private sector, the response has been for businesses and organizations that process consumer data to focus on upgrading security methods to safeguard consumer information.

Notes

[1] Vanden Brook, Tom. "VA: Data on 26.5M veterans stolen." USA TODAY, May 23, 2006. http://www.usatoday.com/news/washington/2006-05-22-veterans-information_x.htm.

[2] Tyson, Ann Scott and Lee, Christopher. "Data Theft Affected Most in Military National Security Concerns Raised." Washington Post, June 7, 2006, A01.

[3] Patton, Zach. "Stolen Identities." Governing, August 4, 2005. http://www.governing.com.

[4] Federal Trade Commission. "Consumer Fraud and Identity Theft Complaint Data January – December 2005." http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[5] Federal Trade Commission. "2003 FTC Identity Theft Survey Report." http://www.consumer.gov/idtheft/pdf/synovate_report.pdf.

[6] "A Growing Problem Credit Card Skimming: A Growing Problem," August 2003, http://www.identitytheft911.org/articles/article.ext?sp=67.

[7] Op. cit.

[8] Op. cit.

[9] "IBM Reports Phishing Surge," June 30, 2005, by Paul F. Roberts, eWEEK.com, http://www.eweek.com/print_article2/0,1217,a=155172,00.asp.

[10] Op. cit.

[11] Op. cit.

[12] "New Techniques Scam Artists 'Pharm' New Techniques," April 2005. http://www.identitytheft911.org/articles/article.ext?sp=117.

[13] Yerak, Becky. "Scam artists add new arrow to their quiver: Caller ID." Chicago Tribune July 16, 2006. http://www.chicagotribune.com/technology/chi0607160318jul16%2C1%2C2774137.story?coll=chi-news-hed&ctrack=1&cset=true.

[14] Op. cit.

[15] "Watch out for medical identity theft - Report estimates that up to 500,000 consumers have been victimized so far." Sun-Sentinel Co. & South Florida Interactive Inc., May 15, 2006. http://www.sun-sentinel.com/business/local/bal-ambrose0515,0,2331801.column?track=rss.

[16] Dixon, Pam with Gellman, Robert. "Medical Identity Theft: The Information Crime that Can Kill You." Released May 3, 2006, http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf.

[17] Sullivan, Bob. "The meth connection to identity theft - Drug addiction plays a part in many crime rings, cops say," MSNBC, March 10, 2004, http://www.msnbc.msn.com/id/4460349/.

[18] "The Meth Epidemic in America: Two Surveys of U.S. Counties," National Association of Counties, July 5, 2005, http://www.naco.org/Template.cfm?Section=Library&template=/ContentManagement/ContentDisplay.cfm&ContentID=16925.

[19] Leland, John. "Stolen Lives - Meth Users, Attuned to Detail, Add Another Habit: ID Theft," New York Times, July 11, 2006, http://www.nytimes.com/2006/07/11/us/11meth.html.

[20] Council of Better Business Bureaus and Javelin Strategy & Research. "2006 Identity Fraud Survey Report," http://www.bbbonline.org/idtheft/safetyQuiz.asp.

[21] Baum, Katrina, Ph.D. "First Estimates from the National Crime Victimization Survey Identity Theft, 2004." BJS Statistician, April 2006, NCJ 212213, U.S. Department of Justice Office of Justice Programs Bureau of Justice Statistics Bulletin, http://www.ojp.usdoj.gov/bjs/abstract/it04.htm.

[22] "Identity Theft Victim Complaint Data - Figures and Trends in Illinois January 1-December 31, 2005," http://www.consumer.gov/idtheft/pdf/CY2005/Illinois%20CY-2005.pdf.

[23] "Identity Theft Victim Complaint Data - Figures and Trends in Illinois January 1-December 31, 2004," http://www.consumer.gov/idtheft/pdf/CY2004/Illinois%20CY-2004.pdf.

[24] "Identity Theft Victim Complaint Data - Figures and Trends in Illinois January 1-December 31, 2003" http://www.consumer.gov/idtheft/pdf/CY2003/Illinois%20CY-2003.pdf.

[25] U.S. Public Interest Research Group. States with notification laws, as of June 23, 2005.

[26] Identity Theft Law 720 ILCS 5/16G-15, http://www.ilga.gov/legislation/ilcs/documents/072000050K16G-15.htm.

[27] Peterson, Kavan. "States failing to secure personal data," Stateline.org., July 12, 2006, http://www.stateline.org/live/ViewPage.action?siteNodeId=136&languageId=1&contentId=126215

[28] "Identity Theft Victim Complaint Data - Figures and Trends in Illinois January 1 - December 31, 2005," http://www.consumer.gov/idtheft/pdf/CY2005/Illinois%20CY-2005.pdf.

[29] Ponce, Dan. "New report says Chicago street gangsters moving to suburbs," WLS-TV News, June 19, 2006, http://abclocal.go.com/wls/.