CONTACT:
NW3C Research Section
12 Roush Drive
Morgantown, WV 26501
Ph: 877-693-2874 Fax: 304-291-2282

WCC Issue
Identity Theft

Definition
The Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act) was passed to address the problem of Identity Theft. This act (codified at 18 U.S.C. § 1028) makes it a federal crime when anyone.

Knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law.[1]

How It Happens
Identity theft primarily takes two forms: "true name" and "account takeover" fraud.[2] True name fraud occurs when someone uses a consumer's personal information to open new accounts in his/her name. The second type of identity theft, account takeover, occurs when criminals gain access to a person's existing account(s) and make fraudulent charges. An even more insidious aspect of identity theft, however, is when a criminal provides a victim's personal information to law enforcement when the criminal gets arrested. The victim can have a criminal record or outstanding warrants attached to their name and personal information without even realizing it.

There are several common techniques used in conducting identity theft. Some criminals conduct "dumpster diving" expeditions where they go through trash cans or dumpsters to get copies of checks, credit card and bank statements, credit card applications, or other records that typically bear identifying information. These records make it easier for criminals to gain control over accounts in the victim's name and assume their identity.[3] Another technique is "shoulder surfing", looking over the victim's shoulder as he/she enters personal information.[4] Eavesdropping is another simple, yet effective technique that criminals often use. Eavesdropping can occur when the victim is at an ATM machine, when they give credit card information over the phone, or when they dial in the number for their telephone calling card.

Recently the Internet has become an inviting place for criminals to obtain identifying information, such as social security numbers or even banking information. When exploring the many exciting features of the Internet, many individuals respond to "spam"—unsolicited e-mail—that promises them some benefit but requests identifying data, without realizing that in many cases, the requester has no intention of keeping his promise. In some cases, criminals reportedly have used computer technology to obtain large amounts of personal data.[5]

Cost/Statistics
- Despite the difficulty in tracking this type of crime, over a three year period the United States Secret Service has noticed an increase in the number of cases considered directly associated with identity theft. In 1995, 8,806 financial crimes investigation cases were related to identity theft. In 1996 there were 8,686 cases, and in 1997 there were 9,455 cases.[6] In 2000, an estimated 500,000 to 700,000 people were victimized by identity theft.[7]

1 United States Congress, "Identity Theft and Assumption Deterrence Act," United States Congress, October 30, 1998, <http://www.ftc.gov/os/statutes/itada/itadact.htm> (September 10, 2001)

2 Janine Benner, Beth Givens, and Ed Mierzwinski, "Nowhere to Turn: Victims Speak Out on Identity Theft," A CALPIRG/ Privacy Rights Clearinghouse Report, May 2000, <www.privacyrights.org/ar/idtheft2000.htm> (September 10, 2001)

3 Department of Justice "Identity theft and fraud," <www.usdoj.gov/criminal/fraud/idtheft.html> (September 10, 2001)

4 Ibid

5 Ibid

6 "Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited," (briefing report. 05/01/98, GAO/GGD-98-100BR). <http://www.glr.com/govt/privacy/identityfraud.html> (September 10, 2001)

7 Janine Benner, Beth Givens, and Ed Mierzwinski, <www.privacyrights.org/ar/wcr.htm> (September 10, 2001)

- In 1998, The General Accounting Office (GAO) released a report to Congressional requesters entitled, "Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited." The report noted that the Secret Service quantified identity theft losses to individuals and financial institutions at $442 million in fiscal year 1995, $450 million in fiscal year 1996, and $745 million in fiscal year 1997. This involved only those cases of financial crime that the Secret Service itself had tracked. MasterCard has previously stated that dollar losses related to identity theft fraud represent 96% of member banks' overall fraud losses of $407 million in 1997. Also in 1997, U.S. fraud losses of VISA member banks totaled $490 million or about 0.1% of billing transactions.

High Profile Examples/Case Studies

Criminals engage in identity theft to further facilitate many other types of criminal offenses, including fraud. Victims can include all types of citizens including celebrities such as Tiger Woods and Oprah Winfrey. Below are examples taken from recent federal prosecutions that show some of the many ways in which people can commit identity theft:

- Several people obtained names and Social Security numbers of several hundred high-ranking active-duty and retired U.S. military officers from a public Internet Web site. They used the officer's names and numbers to apply for credit cards and bank and corporate credit in the officers' names.[8]

- A man stole the identities of more than 100 people by working with a woman who had worked in the payroll department of a cellular telephone company. In that position, the woman had access to confidential employee information such as Social Security numbers, with which the man was able to access their stock trading accounts at an online brokerage and transfer money to another account that he had set up. One victim had more than $287,000 taken from his brokerage account without his knowledge.[9]

- When various people who picked up their mail at a U.S. post office threw away merchandise catalogs, which contained identifying information such as their names and account numbers, a woman went through the trash, removed the catalogs, and used the identifying information to order merchandise in other people's names.[10]

"For More Information" Links

Identity Theft Resource Center
http://www.idtheftcenter.org/

Federal Trade Commission
http://www.consumer.gov/idtheft/

Federal Bureau of Investigation (FBI)
http://www.fbi.gov/contact/fo/norfolk/1999/ident.htm

Privacy rights clearinghouse: Identity theft resources
http://www.privacyrights.org/identity.htm

---

8 Jonathan J. Rusch "Making a Federal Case Of Identity Theft" *U.S. Department of Justice*, <www.usdoj.gov/criminal/fraud/fedcase_idtheft.hml> (September 10, 2001)

9 Ibid

10 Ibid