10-2008

Identity Theft 101

Robert E. Holtfreter
Central Washington University, holtfret@cwu.edu

Recommended Citation

Holtfreter, R.E. (2008). Taking back the ID. *Fraud, 22*(5), 17-19, 57.

FRAUD
SEPT/OCT 2008
TAKING BACK THE I.D.

Identify Theft Prevention and Analysis

IDENTITY THEFT 101

By Robert E. Holtfreter, Ph.D., Educator Associate Member

This new column will critically analyze identity theft issues to keep readers current about this growing problem that has become a plague to consumers and businesses worldwide.

For about eight days last year, my copy of USA Today wasn't being delivered through the mail. The newspaper told me that I had made a change of address, which I hadn't. After the customer service rep verified my identity, she told me that she would extend the term of my subscription to account for the days missed and delivery would resume.

Evidently the fraudster stole the newspaper from my mailbox and used my name and address to send my subscription his way. This is a rather elementary example of identity theft (and mail fraud, which is a felony). I plan to report this incident to the U.S. Postal Service and the Federal Trade Commission (FTC).

Identity theft, as defined by the FTC, "occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, to commit fraud or other crimes."[1]

In this first column, we'll lay a foundation with identity theft complaint data recently published by the FTC as part of its 2007 "Consumer Fraud and Identity Theft Complaint Data" report. The data in the report was provided by the Consumer Sentinel, which is a complaint database developed and maintained by the FTC since 1997.

The Consumer Sentinel collects information about consumer fraud and identity theft from the FTC and more than 125 other organizations. It shares that info with law enforcement partners across the nation and throughout the world for use in their investigations. The Sentinel database now includes more than 4.3 million complaints. In 2007, the Sentinel received more than 800,000 consumer fraud and identity theft complaints; consumers reported losses from fraud of more than $1.2 billion.[2]

The Sentinel network is composed of three entities: the Identity Theft Data Clearinghouse (**www.consumer.gov/idtheft**), launched in November 1999 as the sole national repository of consumer complaints about identity theft; Econsumer.gov (**www.econsumer.gov**), created in April 2001 to gather and share cross-border e-commerce complaints to respond to the challenges of multinational Internet fraud and enhance consumer confidence in e-commerce, and Military Sentinel (**www.consumer.gov/military**), established in September 2002 as a project of the FTC and the U.S. Department of Defense to identity and target consumer protection issues that affect members of the U.S. Armed forces and their families.[3]

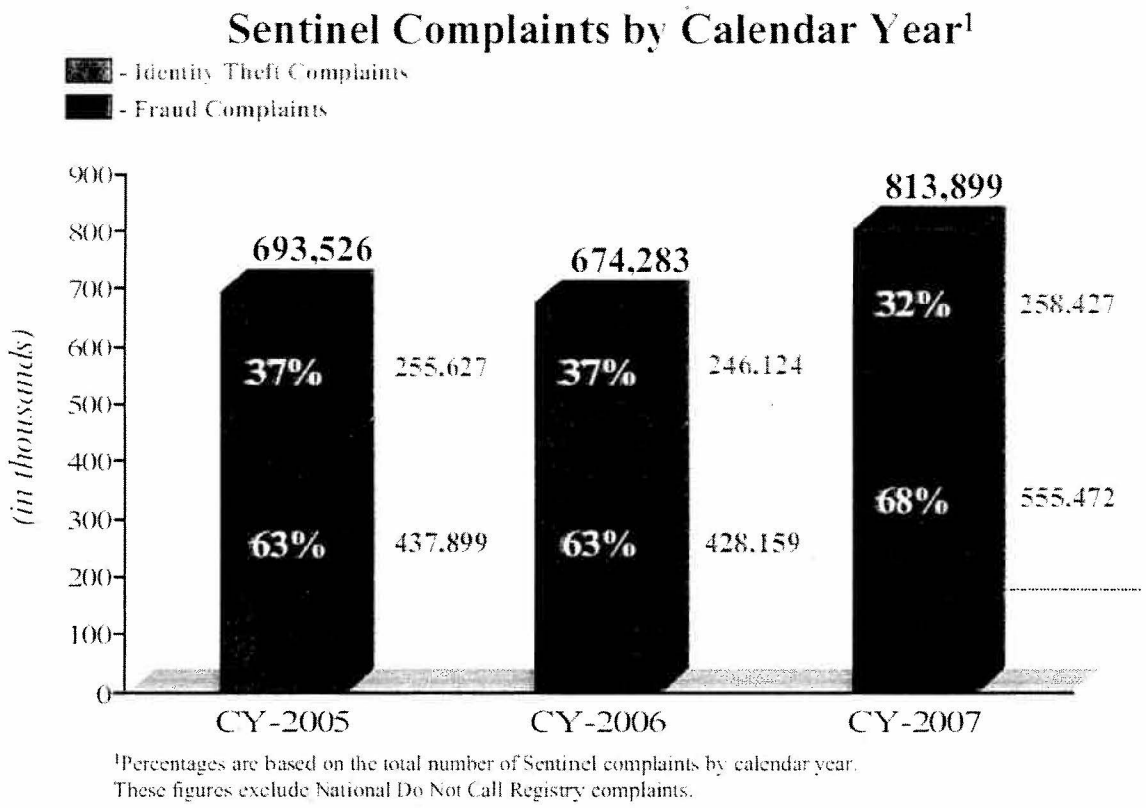


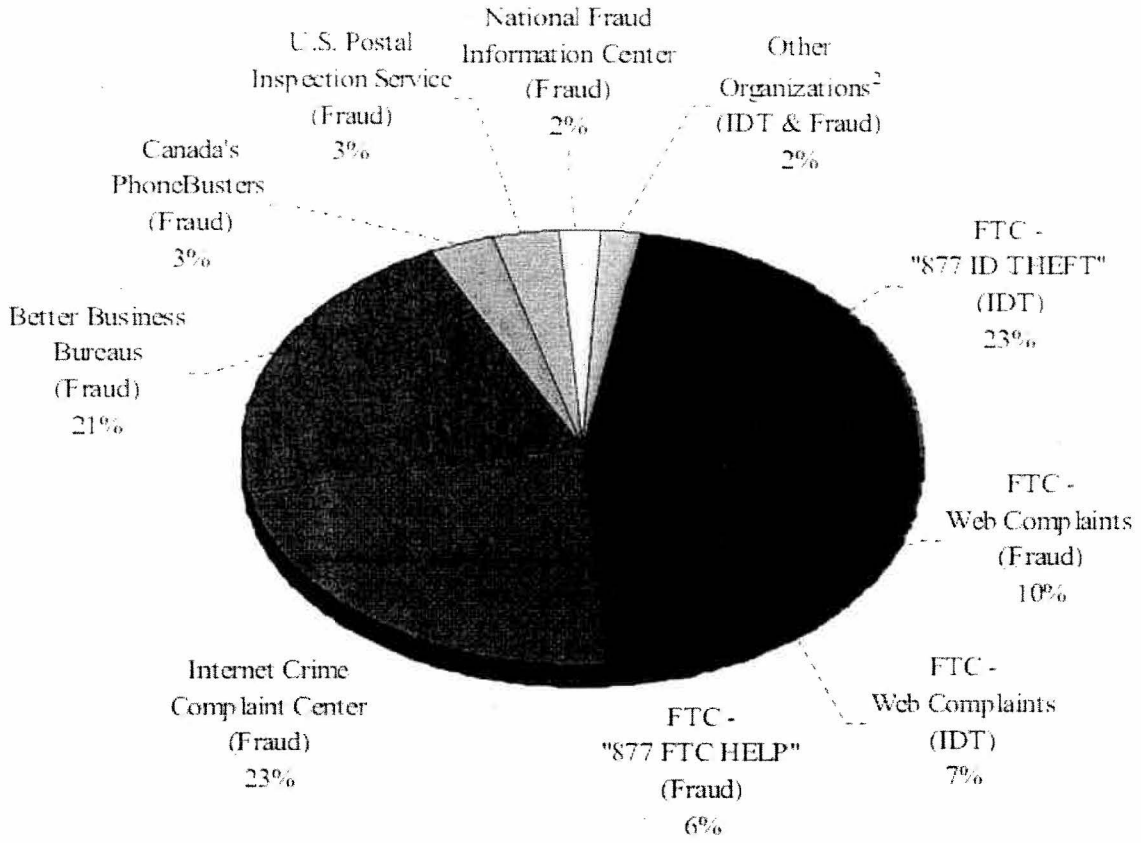
Figure 1

In Figure 1, the Consumer Sentinel reports the number of identity theft and fraud complaints received for years 2005, 2006, and 2007. Of the 813,899 complaints reported in 2007, 258,427 or 32 percent were identity theft complaints. In 2005 and 2006 there was 246,124 and 255,627 identity theft complaints reported respectively.[4] The identity theft data for 2007 show an increase of 12,303 complaints over 2006 and an increase of 2,800 over 2005, which, at the surface level, indicates that identity theft is modestly increasing. But does this report reflect the actual identity theft activity for this time period? The answer is no. According to the FTC, the 2007 data is understated because "some future data transfers from other organizations will contain complaints from 2007 that have not yet been received."[5] Furthermore, the FTC

acknowledges the understatement of the identity theft complaints for all three years in the report by stating that (1) as many as 9 million Americans have their identities stolen each year, and (2) this report isn't based on a survey; the complaint figures presented are derived from self-reported and unverified consumer complaints in the FTC's database.[6]

Appendix A2: Sentinel Data Contributors[1]

January 1 – December 31, 2007



[1]Percentages are based on the total number of Sentinel complaints (813,899) received between January 1 and December 31, 2007. The type of complaints provided by the organization is indicated in parentheses.

[2]For a list of other organizations contributing to Sentinel, see Appendix A3.

Figure 2

This analysis is supported by Figure 2, which reports the Sentinel's major contributors of fraud and identity theft data for 2007. As noted above, 32 percent of the complaints registered by the Sentinel in 2007 were identity theft complaints. The major contributors of the identity theft complaint data are the FTC through its Web site (7 percent), telephone (23 percent), and "other organizations" (2 percent).[7] The FTC strongly encourages all victims of identity theft and fraud to fill out a report on its Web site or via the telephone. The reporting organizations in the "other organizations" category include only two federal agencies, four attorney general offices, six other state and local agencies, 25 police departments/sheriff offices, and two other entities.[8]

If the FTC is correct in its estimation of 9 million identity theft victims annually, then the data in Figures 1 and 2 indicate that a relatively large percentage of identity theft victims and possible entities that accumulate identity theft data aren't reporting it to the FTC and the Sentinel. Regardless of the deficiencies in the data, the FTC annual report can be perceived as reflective of actual identity theft activity and, as such, is invaluable. On the other hand, we must be very careful when we interpret or draw inferences and conclusions from the data in this report so that we don't under- or overstate the severity of the identity theft problem.

METHODS USED BY THIEVES TO STEAL IDENTITIES

All of us have trails of personal information that follow us throughout our lives and even after our deaths. For example, we have a name, address, Social Security number (in the United States and many countries), and most of us have other information like a checking and savings account and debit and credit cards. We're involved in daily transactions that involve our personal information. We receive and send items through the mail or the Internet. We use our debit/credit cards when we shop at various business establishments, eat out, or purchase items via the Internet. We write checks for various purposes and deposit money into our financial accounts.

The information that we generate becomes a potential gold mine for identity thieves. According to the FTC,[9] here are some of the ways identity thieves obtain our personal information:

Dumpster diving They rummage through trash looking for bills and other papers containing your personal information.

Skimming They steal credit/debit card numbers with a special storage device when processing your card.

Phishing They pretend to be financial institutions or companies and send spam pop-up messages to get you to reveal your personal information online. This message gets your attention by claiming that you have a problem with your account.

Changing your address They divert your billing statements to another location using a change-of-address form.

Old-fashioned stealing They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personal records or bribe or con employees who have access. They might steal records while on the job or hack into data records. They might get your credit report by posing as someone who could have a legal right to your report. They might also steal personal information from your home.

Pre-texting Through the use of the telephone they use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.

TYPES OF IDENTITY THEFT FRAUDS

The Consumer Sentinel's data for three years in their 2007 report show the different types of frauds that occur when an identity theft victim's personal information is misused. The major types of identity theft for 2007 include credit card fraud (23 percent), phone or utilities fraud (18

percent), employment-related fraud (14 percent), bank fraud (13 percent), government documents or benefits fraud (11 percent), loan fraud (5 percent) and other identity theft-related frauds (25 percent). The latter major type includes two sub-types: "uncertain" and "miscellaneous" that account for 76 percent of the frauds in that category. In addition, the data includes another category called "attempted identity theft" (5 percent).[10]

These percentages don't add up to 100 percent because identity theft victims can include more than one type of identity theft in their complaint reports. Also, in most cases, the total of the percentages for the identity theft fraud sub-types don't match what's stated in the report. For example, in the phone or utilities fraud identity theft type, the total of the percentages for the sub-types is actually 20 percent and not 18 percent as shown. Because these mathematical concerns are minor, the analysis that follows will be based on the data in the report and we'll take that data at face value.

Even though credit card fraud in 2007 still represents the most common type of reported identity theft, it appears that its occurrence over the past three years as a percent of total identity theft complaints has decreased modestly in total and in new and existing accounts. Similar decreases in the percentages have also occurred for new wireless accounts in the phone or utilities fraud category, electronic fund transfer and existing accounts in the bank fraud category, and issued and forged driver's license in the government documents or benefits category. On the other hand, the identity theft-related frauds that have shown modest or significant increases in their percentages include new telephone accounts in the phone or utilities fraud category, and employment-related fraud and fraudulent tax returns filed in the government documents or benefits fraud category.[11]

Identity theft-related frauds that have shown no significant increases in their percentages over the three-year period included the attempted identity theft category, utilities' new accounts and unauthorized charges to existing accounts in the phone or utilities fraud category, new accounts in the bank fraud category, business/personal/student loan, auto loan/lease and real estate loan in the loan fraud category, government benefits applied for/received and other government documents issued/forged in the government documents or benefits fraud category, magazines, bankruptcy, child support, securities/other investments, property rental, insurance, apartment or house rental, Internet/e-mail, medical, evading the law, and miscellaneous/uncertain in the other identity theft category.[12]

WAYS THAT INFO MIGHT BE MISUSED

The following identity theft specifics are excerpted from the FTC publication, www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

Credit card fraud They might open up new credit card accounts in your name. When they use the cards and don't pay the bill, the delinquent accounts appear on your credit report or they might change the billing address on your credit card so that you no longer receive bills and then run up charges on your account. It might be some time before you realize there's a problem because your bills are sent to a different address.

Phone or utilities fraud They might open a new phone or wireless account in your name, run up charges on your existing account, or use your name to get utility services like electricity, heating, or cable TV.

Employment-related fraud They might get a job using your name.

Bank fraud They might create counterfeit checks using your name or account number, open a bank account in your name and write bad checks, or clone your ATM or debit card and make electronic withdrawals in your name and then drain your accounts.

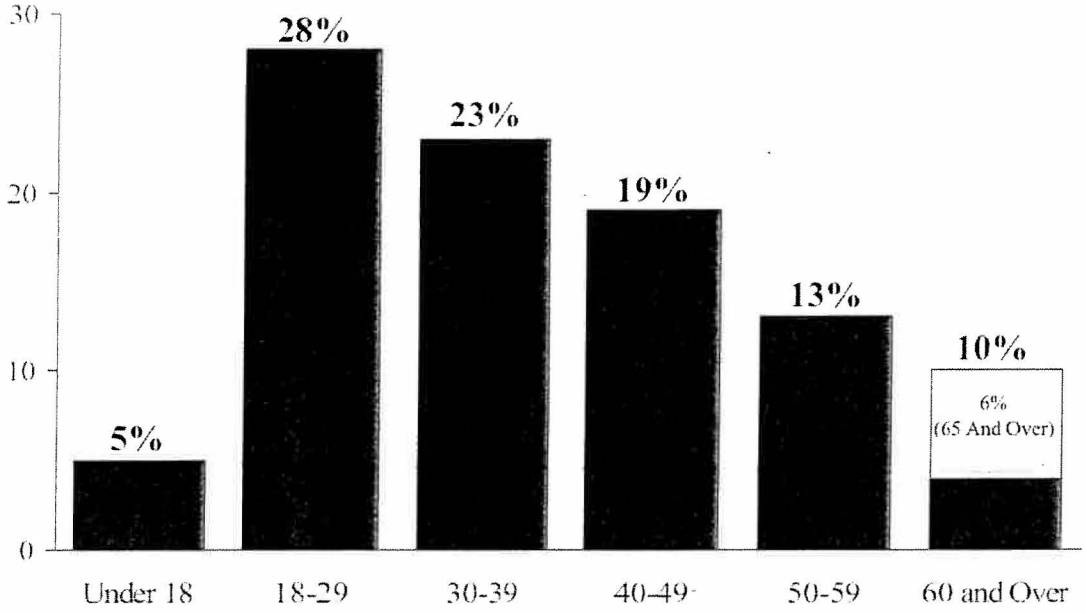
Government documents or benefits fraud They might get a driver's license or official ID card issued in your name but with their pictures on them, use your name and Social Security number to get government benefits, or file a fraudulent tax return using your information.

Loan fraud Using your name, they might take out a business, personal, or student loan; buy or lease a car and take out an auto loan; or take out a real estate loan.

Other identity theft frauds Using your name they might buy securities, health insurance, high-speed Internet, magazine subscriptions, or child support services, or rent an apartment or house. An identity thief might even say he is you and give your personal information to a police officer during an arrest. If he doesn't show up for his court date, a warrant for arrest is issued in your name.

Identity Theft Complaints by Victim Age[1]

January 1 – December 31, 2007



[1]Percentages are based on the total number of identity theft complaints where victims reported their age (231,576). 95% of the victims who contacted the FTC directly reported their age.

Figure 3

IDENTITY THEFT BY AGE

Figure 3 identifies theft complaints in which victims reported their ages. The age group reporting the largest per cent of complaints is the 18-29 year olds with 28 per cent. They were followed by the 30-39, 40-49, and 50-59 age groups with 23, 19, and 13 percent of the reported complaints respectively. The lowest per cent of complaints were reported by the 60-64 age group with 4 percent. Following them were the under 18 age group with 5 percent and the over-65 age group with 6 percent.[13]

MANDATORY PROGRAMS FOR TEENS

Even though state officials, the media and other businesses have provided programs or information to educate the public on how to detect and prevent identity theft, it's obvious from the statistics that more needs to be done especially at the high school and university levels. High schools should make it mandatory for all students to attend a two- to three-hour identity theft detection and preventative workshop, which should be taught by identity theft experts. Educating this captive audience should help to reduce identity theft significantly over time.

BUILDING ON THE FOUNDATION

In this first column, we've laid a basic statistical foundation that we'll build on in future columns with such topics as: what to do if you become a victim; detection and preventative measures; new related fraud schemes; and an update and evaluation of current and proposed laws at the state, federal, and international levels. The ACFE's members can get involved to help influence the content of proposed legislation at all governmental levels.

***Robert E. Holtfreter, Ph.D, Educator Associate Member**, is Distinguished Professor of Accounting and Research at Central Washington University in Ellensburg, Wash.*

His e-mail address is: **holtfret@cwu.edu**

[1] "About Identity Theft." Federal Trade Commission. February 2008.
[2] "Consumer Fraud and Identity Theft Complaint Data." Federal Trade Commission. February 2008.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] Op.Cit. "About Identity Theft."
[10] Op.Cit. "Consumer Fraud and Identity Theft Complaint Data."
[11] Ibid.

[12] Ibid.
[13] Ibid.