Identity Theft Facts and Information

Identity Theft: An Overview

Identity theft is one of the fastest growing crimes in the nation, estimated by the U.S. Federal Trade Commission (FTC) as being a $50 billion a year industry [(1)] that continues to expand its reach. It can take on many forms. Identity thieves may rent an apartment, obtain a credit card, or establish a telephone account in someone else's name.

Victims may not find out about a theft until they review their credit report or a credit card statement and notice charges they didn't make. Or they may discover the issue when contacted by a debt collector regarding delinquent payments.

While some identity theft victims can resolve their problems quickly, others spend thousands of dollars and many months repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities or be denied loans for homes, cars, or education because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

Identity Theft Statistics

- Identity theft is on the rise, affecting almost 10 million victims in 2008 (a 22 percent increase from 2007) [(5)]
- According to the 2009 Federal Trade Commission report, more than a quarter of the more than 1.2 million complaints they received during the 2008 calendar year involved identity theft [(6)]
    - The report states that credit card fraud was the most common form of reported identity theft at 20 percent, followed by government documents/benefits fraud at 15 percent, employment fraud at 15 percent, phone or utilities fraud at 13 percent, bank fraud at 11 percent and loan fraud at four percent [(6)]
- In 2007 the U.S. Federal Trade Commission (FTC) stated that credit card fraud was the most common form of reported identity theft [(1)]
- A 2007 FTC report states that 91 percent of adults surveyed fear their identities could be stolen [(2)]
- Forty-seven percent of identity theft victims have trouble getting credit or a loan as a result of identity theft [(2)]
- Seventy-one percent of fraud happens within a week of stealing a victim's personal data [(5)]
- Low-tech methods for stealing personal information are still the most popular for identity thieves. Stolen wallets and physical documents account for 43 percent of all identity theft, while online methods account for only 11 percent [(5)]
- Forth-three percent of identity theft victims believe they know the person who stole their identity [(2)]
- Victims of identity theft spend anywhere from three to 5,840 hours repairing damage [(2)]
- Identity theft victims can be affected for more than 10 years after the crime was discovered. The effects include increased insurance or credit card fees, inability to find a job, higher interest rates, battling collection agencies and more [(2)]
- Since March 2007, the FTC has distributed more than 22,000 of its Consumer Education Kits, which equip consumers to give presentations in their communities on avoiding ID theft [(4)]
- In February 2008, the President's Task Force and the U.S. Postal Service sent the FTC's ID theft brochure to *every* household in the U.S., numbering 121 million pieces [(4)]

What Is Done With Stolen Identity

Once identity thieves have the victim's personal information, they may use it in a variety of ways:

- Open new credit card, phone, or utilities accounts
- Change the billing address on accounts to run up charges without the victim's knowledge
- Take out major loans and not pay off the debt
- Begin an entire new life to hide their criminal record, getting a driver's license or official I.D.

How Identities Are Stolen – General Overview

There is a lucrative black market for stolen identities, leading to sometimes elaborate schemes to steal people's data. Identity theft rings have also developed and engage in carefully orchestrated thefts of large amounts of data. Here are some common methods thieves employ:

- **Hacking** into a bank, credit union or credit card company's database [(3)]
- **Phishing**, which is when a scammer sends an e-mail that appears to come from a bank or company, asking for personal information such as credit card or Social Security number
- **Stealing** bank or credit card statements from the mail
- **Cloning** information at restaurants and bars where customers swipe credit and debit cards or hand them to servers who process the charge behind closed doors
- **Theft of information from retailers**, which may be low-tech, like grabbing a day's receipts, or high-tech, as when a hacker breaks into a store's customer rewards program database
- **Dumpster diving** –going through garbage for mail, bank statements or other personal data
- **Stealing passwords** belonging to someone with legitimate access to obtain consumer data
- **Stealing from other sources, such as:**
    - **Laptops:** Thieves may only be after the hardware, but then discover data on the hard drives
    - **Doctor's offices or medical insurance companies**, where Social Security numbers may be stored or used as a policy number
    - **County Recorder's** office where deeds is registered and recorded
    - **County Municipal Hall** which houses official marriage certificates, birth certificates, and death certificates
    - **Social Security Administration,** where social security numbers and other data is stored
    - **Hospitals** are where new parents fill out applications for their child's SSN
    - **Car dealerships** usually attach customers' latest credit reports and scores to purchase documents
    - **Veterans Administration**, its affiliates and hospitals. They not only have information on military personnel but also on the families and beneficiaries of veterans
    - **Previous Employers**: They keep employee SSNs, past and present names (aka maiden name), addresses, W2s, 401K and beneficiary forms, etc.
    - **Human Resource departments** keep applicants' personal information
    - **Personally identifiable information can also be obtained from these sources:**
        - Frequent flyer clubs
        - Grocery store clubs
        - Library cards
        - Pay day check cashing outlets
        - Sports associations
        - Passport centers

Ways to Protect Personal Identity

- Do not provide Social Security numbers unless necessary by law, such as for employment, tax forms or bank records. Many forms may ask for a Social Security number even though it's not required
- Don't have driver's license numbers printed on checks
- Keep Social Security cards stored and safe, not in a wallet
- Do not make PINs or passwords obvious or easy to guess
- Choose online or "paperless" statements. Fewer documents going through the mail with personal information means fewer opportunities for thieves
- Shred all sensitive information before throwing in the trash
- Monitor changes to credit reports. No matter how vigilant people are about protecting personal information, I.D. thieves are resourceful and there can be security breaches that are out of their control

Members of ProtectMyID.com™ have automatic credit monitoring, so if signs of potential fraud appear in a member's credit report, they are alerted and have additional peace of mind knowing a dedicated Fraud Resolution Agent is there to help them clean up the mess and reclaim their identity.

In addition to identity theft resolution assistance, ProtectMyID.com is backed by a $1 million Product Guarantee. Members who become a victim of identity theft, due to a failure of the product, while enrolled in and using ProtectMyID.com will be reimbursed for certain identity-theft-related expenses such as lost wages, legal fees and stolen funds not reimbursed by the bank or credit card service provider. The Guarantee is subject to limitation.

# # #

(1) *Federal Trade Commission Customer Fraud Survey, 2007*
(2) *Prepared Statement of the Federal Trade Commission before the Maryland Task Force to Study Identity Theft, 2007*
(3) *The Javelin 2006 Identity Fraud Survey Report*
(4) *The FTC in 2008: A Force for Consumers and Competition -- Federal Trade Commission March 2008*
(5) *The Javelin 2009 Identity Fraud Survey Report*
(6) *Federal Trade Commission Consumer Sentinel Network Data Book for January-December 2008 (Released in 2009)*