Many Faces of Identity Theft

Stealing Public Information: Thieves steal the names and Social Security numbers of city residents from the municipal offices that publicly publish this information and use the information to set up new accounts to commit identity theft.

The Master Death List compiled by the Social Security Administration does not include individuals that have died prior to receiving social security benefits or individuals that have died but have not been reported. Consequently, thieves tend to acquire social security numbers from children or family members who have passed away and use these numbers to commit identity theft.

Another instance of identity theft with social security numbers arises with parents. There are a couple of instances in which a parent takes the social security number of his/her child to open new credit accounts because the parent's own credit history will not permit him/her to open a new account. Consequently, the parent creates a large amount of debt in his/her child's name.

Crooks also scan the obituaries, gathering the information provided in the obituary to impersonate the deceased during the period of time between death of the person and the recognition of that death by the person's financial institutions. A variant on this is not to scam the deceased's financial institutions, but using his/her name and information from the obituary (and from other sources) to open up fraudulent accounts, relying on the fact that the departed individual will not be vigilantly checking his/her credit records.

A thief searches through court documents for personal information on those who will not be filing income tax returns in the upcoming year. The thief then uses this information to file phony income tax returns in the person's name and have the money deposited to the thief's account.

Focus on the Military: American soldiers are at a great risk for identity theft for two reasons: 1) the serial number that is used to identify the soldier is his/her social security number and 2) soldiers have been taught that, if taken captive, they should provide their "name, rank and serial number." Obtaining this information, that is publicly available, makes it easy for thieves, as well as captors, to open new accounts, apply for loans, and acquire merchandise in the soldiers' names.

Stealing Drivers' Licenses: Thieves will buy or fabricate driver's licenses or identification cards and use them to open checking accounts. Once the checking accounts are opened, these thieves will write a large number of worthless checks for merchandise.

Mail theft: A suspect stole mail intended for a neighbor/landlord/roommate. He obtains social security account information and financial account numbers and uses that information to obtain ATM/debit cards and personal identification numbers. The suspect then used these access numbers to withdraw approximately a large amount of money in cash from the accounts or to open fraudulent accounts in the victims' names.

Disconnected Services: Thieves, posing as employees of utility companies, contact customers stating that there is an overdue balance on the customer's account, and if it isn't paid by closing time, the customer's utility will be disconnected and a fee will be charged to restore service. At this point, the customer usually insists that the bill was paid on time but the thief says no payment was received and that a disconnect notice was mailed. In the spirit of good service, the thief offers to search the records to see if he/she can locate the payment, but after not finding anything, the thief asks the customer for details of his/her bank, check number, and payment amount. The thief, still unable to find any information about the payment, asks the customer for the account numbers printed at the bottom of the check. The thief uses this information to write fraudulent checks on the customer's legitimate account. With access to checking account information, the thief may also obtain access to the customer's charge accounts.

Insider Stealing: Employees at various corporations, businesses, government entities, or health care facilities have access to sensitive information of both public employees and the people they serve, including their Social Security numbers. Many thieves use this information to open new accounts, add charges to existing accounts, or impersonate the individuals.

Another victim first became aware that she was a victim of identity theft when she received a bill from department store. The victim soon found that several accounts were opened fraudulently with various stores. The suspect has even obtained a car loan and car insurance. Fraudulent accounts were opened in the victim's name notwithstanding the fact that she placed fraud alerts on her credit file. The victim found that the suspect obtained her information through her medical insurance records since the suspect works for a firm that maintains HMO databases.

Phone calls: A thief, pretending to work for an obscurely-named finance company, cold calls vulnerable consumers and asks questions such as name, address, postcode and what store cards they own. The questions quickly proceed to information about the customer's mortgage and date of birth. The information is then used to open credit cards, accounts in the customers' name and eventually to spend a large amount of money on these cards. The elderly are susceptible to this type of identity theft.

A caller tells a customer that there has been an ongoing problem with his/her server, creating a danger of losing all the data. The caller needs to put the customer on another server; the customer will have to change his/her password and stick with it until the problem is resolved. The caller gives the customer a new password to use and waits while the customer makes the change and verifies that it works. Then, the hacker goes into the account and steals the customer's identity.

Computer Hacker: Thieves hack into computer systems of businesses, health care facilities, or even universities to obtain personal information that can be used to commit identity theft. Often these businesses, health care facilities, and universities have credit card information, as well as social security numbers on file.

Credit Card Fraud: The victim found that someone had used her and her husband's MasterCard fraudulently when she was contacted by the bank that issued the credit card asking if either the victim or her husband had made some uncharacteristic charges on the account. The victim soon afterwards learned of various new accounts opening in her name. The suspect had acquired driver's licenses and state IDs in the consumer's name and social security number from a different state than the victim lived, voiding her own driver's license. The victim found that she was driving on a cancelled license and had to spend many hours proving her innocence and applying for a new license. The suspect also purchased a Lincoln Navigator, a Ford Expedition, and insurance for both vehicles. Over two years later, the victim found that a second suspect accessed her checking, savings, and money market accounts with her bank for a large amount of money by walking into a branch office and showing a fake ID.

Cyber Identity Theft: There are numerous free websites on the Net which allow surfers to spoof the identity of another individual through tools which circumvent the need to crack passwords. These websites, in turn, camouflage the transmission route by engaging various proxy servers. The surfers then attempt to damage the reputation of a person via the misuse of his/her e-mail address by sending offending messages from the victim’s e-mail address and using his/her e-identity to transact illegal business deals.

Another example of cyber identity theft involves a $100 commercially available keystroke logging program. An identity thief in New York stole over 450 online banking passwords during a two year period by installing a keyboard-sniffing program on public Internet terminals at thirteen locations scattered throughout Manhattan. Unwitting customers using the terminals then had their keystrokes logged as they accessed information. With username and password information in hand, the thief then used the victims' personal and financial information to open new accounts under their names and transferred money from the victims' legitimate accounts into the new, fraudulent ones.

Handing the Thief Your Information: Upon paying their bill, customers give the wait staff their credit card. In some instances, the waiter or waitress then charges the customers account and keeps a copy of the account information, expiration date, and cardholder name for his/her own use. This waiter or waitress then sells this information to a third party or uses it for his/her own benefit.

Another way to obtain credit card information is by skimming. Skimming occurs when criminal gangs recruit people to find temporary work within restaurants, hotels and retail outlets. The recruits are given small, illicit, electronic devices known as skimmers that capture all of the credit or debit card’s details in the few seconds that it takes to swipe the card through the machine. Upon paying their bill, the customers give the recruit their cards which are first swiped through the legitimate credit card machine, and then, secretly, swiped through the skimmer machine. The recruits then pass the skimmers back to the gangs, at a cost. The counterfeiters download the information from the skimmer onto a computer and create fake cards. The new cards now include the details of the victims’ credit cards that were within the skimmer. The card is then sold on the streets for a price dependent upon the credit limit on the card.

Resume Misuse: People often use on-line job seekers to find new employment. A variety of these on-line services permit customers to post their resumes for potential employers to view. Thieves pose as a potential employer and log into this website to obtain these resumes, which include not only the person's address and phone number but also all of his/her employment history. The thieves then use this information to acquire new accounts or even a loan in this person's name. Consequently, the thieves charge many of their purchases to these accounts, putting the victim into great debt.

Dumpster Diving: Companies often throw into the garbage old records of customers or even patients. Individuals also tend to toss unnecessary mail received. Although it is not as prevalent as in the past, thieves search dumpsters and garbage cans for personal information to open new accounts or acquire a pre-screened account that the individual has trashed and consequently, commit identity theft with this information.

Impersonation: A thief obtains personal information about a person and impersonates that person in another city, state, or even country. This would include creating all new accounts and identification in the person's name, as well as literally becoming the person. One example was a man who acquired another man's name legally. Then, the suspect assumed the victim's identity by posing as a doctor, even though the suspect had never received a degree in medicine or had ever been licensed to practice medicine anywhere in the world.

Copycat charities: A thief, claiming to represent a well known charity or a charity that sounds similar to the well known charity, will contact a person and ask for money for the charity's specific needs. (Since the war in Iraq, many scams have asked for money for humanitarian needs, for the troops, and for veterans.) A person will then give them their credit card or checking account information, only to discover soon afterwards unauthorized purchases or withdrawals.

Shoulder Surfing: Thieves look over the shoulder of a victim while the victim is completing an application for credit or loan. The thieves then use this information to fill out a subsequent application at another store or financial institution.

E-mail Notification: Customers from a bank receive an e-mail from what appears to be a legitimate address. The e-mail informs the recipient that the bank has lost the recipient's online banking username and password and it directs users to a website where they can enter this information. The thief collects this information and uses it to withdraw money from the bank's customers.

Preying on Blood Donors: Many donors give their social security numbers to the American Red Cross or the organization that is sponsoring the blood drive before they give their blood. Thieves steal these social security numbers from the donors' records and use them to open bank accounts, apply for drivers' licenses or credit cards, and to purchase merchandise.

Sweepstakes Scam: Thieves call people telling them they've won a foreign sweepstakes, entitling them to a large amount of money. The thieves tell the people that they will receive the money once they send a specific amount for "insurance purposes" to this address in a foreign country. Many people, excited to win the money, send the amount to the address, only to discover that the sweepstakes is a scam. They never hear from the "sweepstakes spokesperson" or see their money again.

Mortgage Fraud: Thieves obtain the identity of another person and use it to purchase property. The thieves then quickly sell the property at illegally inflated prices and pocket the difference. Meanwhile, the people who have had their identities stolen are left with bad credit ratings and the mortgage companies (if used) are left with the losses.

Impersonating Technicians: Thieves dress as a normal technician and walk into a business. Upon entering the offices, they tell the person they are there to fix someone's computer or fix an electrical problem in an office. Often, the employees of the business trust that this person is there on legitimate business. People often let the technicians come right into their office and fix whatever they have to on their computer or within their office. While they are "fixing the problem," the thieves acquire the personal information about the individual by hacking into their computer or stealing their personal belongings.

Preying on Military Spouses: Con artists posing in military uniforms falsely informed the wives of soldiers deployed in Iraq that their husbands had suffered a serious injury. Knowing that the wives would be distraught, the con artists then sought personal information about the soldiers from the wives, including their Social Security numbers. The con artists may use this information to commit the various types of identity theft.

Preying on Terminally Ill Patients: One identity theft ring included a nurse at a Philadelphia hospital who obtained the names of terminally ill patients and bank insiders and mortgage brokers who provided biographical information and account balances of these patients, the legitimate account holders. Ring members then made identification, including driver's licenses, and used their own photos with the legitimate information to make withdrawals from the accounts. In addition to the large amount of money stolen from the terminally ill patients' accounts, the thieves also stole over $10 million in mortgages and purchased 20 new vehicles.

Phishing: Scam artists send fraudulent e-mails to unsuspecting customers of service providers or retail companies. The e-mails are designed to look like legitimate e-mails from these service providers or retailers and ask the customer to verify his/her account information. The customer then "clicks" to a website (a "phisher page"), designed by the scam artist to look exactly like the original provider's website. Here the customer submits his/her personal information, including account numbers, passwords, and sometimes a social security number. The thief then uses the information to purchase merchandise, steal from bank accounts, or steal the customer's identity.

Basic Theft: Thieves broke into a healthcare business and stole the company's computers. The computers contained the personal information of thousands of beneficiaries and employees within the business, all of whom are active duty or retied military members and their families. Although the personal information may not have been the intended theft, the thieves have at their fingertips all the information necessary to steal the customers' identities, open new accounts, or steal from the existing accounts.

Targeting Home Equity: Thieves look for elderly homeowners with only a few years left on their mortgages or those who have paid off their mortgages. Upon learning the address, the thief searches public records and local tax databases to learn all he/she can about the homeowner and the property. Sometimes, the thief confronts the homeowner face-to-face, claiming to be a real-estate agent working in the neighborhood and asking the homeowner questions about the value of the home and mortgage information. Once he/she acquires all the necessary information, the thief develops fraudulent documents and applies for a home-equity loan in the victim's name. In some extreme instances, the thief works with another identity thief to actually sell the home; one thief will apply for the mortgage to buy the home, while the other thief sells the home for which the mortgage was acquired. The thieves then split the mortgage money and vanish. Luckily identity theft victims would not be liable to repay the lost funds and do not lose their homes. However, this face of identity theft still costs the victims thousands of dollars to clean up their credit, as well as, costs the mortgage lenders the money they gave the thief.