By Paul R. Paradise

IDENTITY THEFT

Help! Someone is using my Social Security number to get a job.

From a consumer complaint to the Federal Trade Commission, Sept. 20, 1999

Before he was busted, Abraham Abdullah, a Brooklyn busboy, stole millions from high-powered luminaries including Steven Spielberg, Martha Stewart, Oprah Winfrey and many others. He did it by obtaining personal information about them and then "stealing" their identities, otherwise referred to as identity-theft.

Abdullah, a high school drop-out, used computers in the local library to log on to the Internet. Once online he obtained detailed credit reports on rich personalities, duping companies such as Equifax, TRW and Experian. He then used the confidential data to impersonate his famous prey, obtaining information and access to credit cards and, eventually, financial accounts at top-tier brokerage houses. Goldman Sachs, Bear Stearns and others all became unknowing victims, until Abdullah was caught. He got away with his crimes unnoticed for six months before he was apprehended.

Identity theft is ranked as one of the top ten business crimes by the F.B.I. It often begins simply enough; obtaining a social security number or other personal information and then impersonating the owner. Surprisingly, the information is relatively easy to locate. Think about it: everyday people write checks at the supermarket or hardware store, use their credit card to purchase tickets to a rock concert or to rent a car, mail their tax returns or rent payment and call home on their cell phone. All of these everyday transactions require giving out personal information, and all can be the start of a nightmare. After obtaining personal information about a Louisiana dentist, Benito Castro of Boca Raton, Fla. opened up more than 12 credit card accounts in the dentist's name and ran up thousands of dollars in bills during a six month spree.

The rich and famous are often targeted – and occasionally nailed. Recently, a drifter and ex-convict named Anthony Lemar Taylor obtained the birth date and Social Security number (SSN) of one Eldrick T. Woods, better known in the world of golf as Tiger Woods. Taylor acquired a California driver's license and credit cards as Eldrick T. Woods and went shopping, amassing an impressive stash of consumer goods before he was apprehended.

The real Eldrick *Tiger* Woods ended up flying into Sacramento aboard his private jet to testify for the prosecution. Under California's 'three strikes and you're out' sentencing guidelines, Judge Michael Virga imposed the maximum sentence on Taylor. He was found guilty on eight charges of theft and two charges of perjury. The Judge ordered Taylor to serve all eight counts consecutively rather than concurrently, for a total of 200 years in prison.

"If you make it easy for people to steal from you, they will," says Frank Abagnale. If anyone knows the ease with which one can impersonate it's Abagnale, a man who has posed as a pilot, an assistant attorney general, a college professor and a pediatrician in his lifetime.

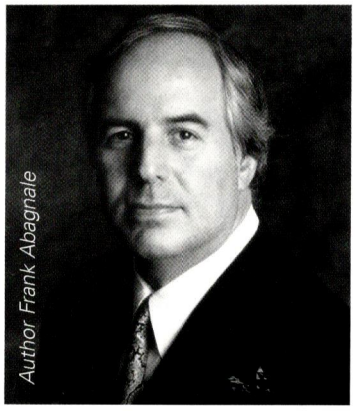
When his parents divorced, 16 year-old Abagnale ran away. For the next 5 years Abagnale and his high IQ and photographic memory, lived on the lam. Using a forged Pan Am identification card and a pilot's uniform, Abagnale, who looked mature for his age, traveled the globe. At one point he was on the FBI's 'Most Wanted' list for passing an estimated $2.5 million in bad checks. Apprehended by the French police when he was 21, Abagnale was released without remuneration on the condition that he help the government write new policies and procedures to curtail white-collar crime. The bigscreen adaptation of Abagnale's book, *Catch Me If You Can*, is currently in production and will star Leonardo DiCaprio. His recently published second book, *The Art of the Steal*, includes a chapter on identity theft.

Advances in technology are fueling the growing problem of identity theft, according to Abagnale. "When I was teenager thirty years ago, you had to be a very skilled printer to print a check or a birth certificate. Now, all you need is a good photocopying machine, an ink jet printer or a PC computer with a scanner. Today's technology has made the crime I did 200 times easier."

Nowadays, Abagnale is a much sought after consultant in the

area of secure documents. He designed the official American Express cheque and assisted in developing the pass for Disney World. He blames a lowering of ethical standards as a contributing factor in the increase in identity-theft and other white-collar fraud. "Young people today see politicians and sports figures cheating, and they say if these people do it and get away with it, so can I."

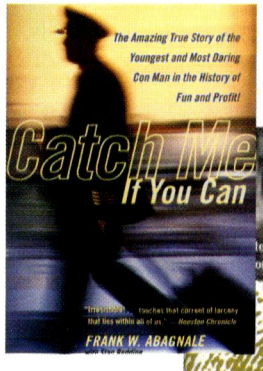
Identity theft has been called the fastest growing white-collar crime. An estimated 500,000 Americans are victimized each year.

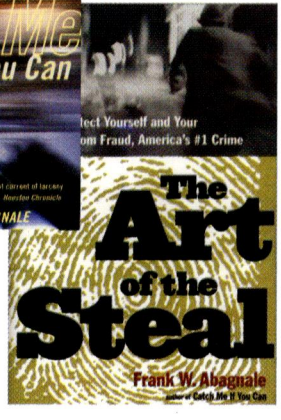

Author Frank Abagnale

Based on a survey conducted by The California Public Interest Research Group (CALPIRG) and the Privacy Rights Clearinghouse (PRC) in May of 2000, victims of identity theft have a long haul in front of them. It takes an average of $808 and 175 hours actively working to clean up their credit reports and other complications, including denial of loan and credit to false arrest and criminal records.

According to the Federal Trade Commission, there are four common forms of identity theft. Credit card fraud is widespread; where a credit card account is opened in a consumer's name or an existing credit card account is 'taken over' by the thief. Communications services fraud involves the identity thief opening a telephone, cellular, or other utility service in the victims name. Bank fraud, where a checking or savings account is opened in the victim's name, and/or fraudulent checks are written is harder to pull off, but it happens. The final area is fraudulent loans, where the identity thief gets a loan, such as a car loan, in the consumer's name only to run with the money.

Passage of the Identity Theft and Assumption Deterrence Act in October, 1998 and numerous state statutes have made little dent in the huge Internet market for fake IDs. There are dozens of websites where the going price is $40 for a Social Security card, $79 for a birth certificate and $90 for a driver's license. For several hundred dollars, an identification kit can be purchased which includes a military ID and a college diploma. Some sites manufacture the phony IDs while others offer templates that are available for downloading onto a CD-ROM.





Police in Nassau County, NY arrested a 16 year-old honors student who had downloaded templates from the Internet to create phony driver's licenses from New York and more than twenty other States. The student had also used downloaded templates to obtain permits for guns, identification cards from several universities and paycheck stubs. He was caught when he went into business for himself with the templates and tried to sell phony IDs to undercover cops. "The quality of the finished product was amazing," says the assistant district attorney who is prosecuting the teenager.

In July, 2000 Sen. Susan Collins (R-Maine), chairwoman of the permanent subcommittee on investigations, introduced a bill called the "Internet False Identification Act of 2000." Collins introduced the legislation after conducting a five-month investigation, during which time her staff procured an impressive collection of phony IDs from the web. Many of the websites are based outside of the United States, which makes prosecution difficult.

Money is not necessarily the only motive behind identity theft. For example, in April, 2000 Gregory Marcinski of Brick, NJ used a fake computer-generated FBI identification kit to impersonate an FBI agent. Marcinski duped a Kentucky motel owner into letting him enter the room of a man who was dating his ex-girlfriend. Marcinski kidnapped and killed the man, burned the body and buried the remains in a swamp.

In an effort to determine the identities of the 19 hijackers who caused the World Trade Center and the Pentagon bomb attacks, the FBI released a list of names of suspected terrorists on September 14, 2001. The list drew objections from the Saudi Arabian government as six of the names were identical to Saudi citizens. Two of the names were the same as Saudi pilots. Two were sons of a Saudi diplomat. The fifth worked for the Saudi Royal Commission in the city of Yanbu, and the sixth name was the same as that of a Saudi man studying in the United States who had had his passport stolen. The need for these stolen identities was obviously not money, but something chillingly terrifying.

On September 27th, 2001 the FBI released new photographs of the suspected terrorists and clarified the spellings of seven of the names. Robert Mueller, Director of the FBI, asked for the public's assistance in identifying the men. "What we are currently doing is trying to determine when these individuals came into the United States, what were their real names, and whether they changed their names using false identification," Mueller told reporters.

Almost all identity thieves engage in pretexting, which is the practice of obtaining personal information about their victims. Pretexters have many tactics, one of which is 'dumpster diving.' Dumpster diving involves rummaging through the trash searching for unopened letters for a pre-approved credit card and other personal information. The crook simply applies for the credit-card, but has it sent to a new address. Once he has the first credit card, the crook begins to make greater inroads by applying for additional cards or securing larger lines of credit.

In another typical ruse the pretexter calls the victim, claiming he's from a survey firm and wanting to ask a few questions. The pretexter slyly obtains the name of the unsuspecting person's financial institution. Next, he pretends to be his or her victim - or someone with authorized access to their account. He might call the bank and say that he's forgotten his checkbook and needs information about his account. If he's lucky, the pretexter may be able to obtain additional personal information such as an SSN or bank and credit card account numbers.

Abraham Abdallah was a master of pretexting. He was finally caught when he sent an email request to Merrill Lynch to transfer $10 million from an account to a new account in Australia. The account belonged to Thomas Siebel, founder of Siebel Systems. Although Siebel is extremely wealthy, the transfer could not be completed because there were not enough funds in this particular account. The brokerage house contacted the real Siebel, who said he had never made the request. Merrill Lynch's computer unit traced the email addresses that were used and cross checked them with all accounts in the company database. The computer unit discovered that the addresses of five other wealthy clients matched the e-mail addresses being checked.

Merrill Lynch's computer unit alerted major brokerage houses about the email addresses. Not surprisingly, the email addresses had been widely used for fund transfers. The police were called

in to sort out the puzzle. They began checking business addresses and found that many being used were non-existent. The police eventually discovered mailboxes in the Wall Street area that were rented in the names of Microsoft co-founder Paul Allen and also James Cayne, head of Bear Stearns. The mailboxes had been arranged by phone and with the aid of faxed, impressively real-looking corporate stationery. The mailboxes were paid with the actual credit card numbers of both men.

The investigation eventually discovered that Abdallah had managed to forge genuine-looking stationary that bore the company names of Merrill Lynch, Goldman Sachs and Bear Stearns. Using the stationery, Abdallah was able to dupe the companies into supplying credit reports on his victims, reports that included the Social Security number, mother's maiden name and other personal information of his targets. More digging discovered that Abdallah wormed his way into the financial houses by using information scammed out of several leading companies that provide credit profiles, including TRW, Equifax and Experian. The police staked out the mailboxes in the Wall Street area and eventually arrested Abdallah and a confederate.

Sooner or later, identity thieves resort to forged documents, most of which are easy to produce. Checks can be ordered through the mail and are inexpensive. Computers and scanners are readily available. "Secure documents is a major concern in the United States printing industry," says Lewis Kontnik, publisher of Authentication News and Holography News. "Securing documents so they cannot be simulated is relatively new in the US, whereas security printing is much more evolved in Europe."

Criminals who engage in identity theft can be investigated by federal law enforcement agencies, including the US Secret Service, the FBI, the US Postal Inspection Service and other agencies. A conviction for identity theft under the Identity Theft and Assumption Deterrence Act can bring a maximum sentence of 15 years imprisonment, a fine and forfeiture of personal property used or intended to be used by the criminal.

Since the mid-1990s there has been a 16-fold increase in the occurrence of identity theft, prompting the call for a national identity card. After the September 11th attack on the World Trade Center and the Pentagon, Larry Ellison, the CEO of Oracle, offered to provide the software for a nationwide central database that would be used for national identification cards. Such a database would contain a digitized photograph and thumbprint of all US citizens.

"The idea for a national identification card sounds great in principle, but may cause more problems than it solves," states Jay Foley, Assistant Director of the Identity Theft Resource Center, a non-profit organization located in San Diego, California. "For example, many organizations would need to have access to the information, so who controls that access? Computerized information needs to be updated and validated - but by whom and how?"

On average it takes an estimated 14 months for identity theft victims to discover the crime, and 175 hours spread over two years to repair the damage. The best defense is prevention, according to Foley, whose wife was an identity theft victim. People should shred documents with important information before putting them into the trash. They shouldn't carry their Social Security Card with them and they should be very careful when making credit card purchases. Another good idea is to call 888.567.8688 to have their names removed from mailing lists for credit card offers.

Foley advises against people subscribing to any of the various credit monitoring services. "Our organization has not seen any that are outstanding One problem is that the services usually update you quarterly. A thief using your name on a credit card can ring up a fortune in a short time." What Foley does suggests is calling the fraud departments of the major credit bureaus and requesting that a fraud alert be placed on your file. You can also request that creditors call you before opening or changing your accounts. You should also order a copy of your credit report each year to ensure its accuracy. [Equifax, 800-525-6285. Experian, 888-397-3742. Trans Union, 800-680-7289].

Persons who have been a victim of identity theft can call the Federal Trade Commission's Identity Theft Hotline 1.877.IDTHEFT or 202.326.2502. The Truth in Lending Act limits a person's liability for unauthorized credit card charges in most cases to $50 per card. Additionally, the Fair Credit Billing Act established procedures for resolving billing errors on your credit card accounts. The most important of these procedures is for a person who has been victimized to send a letter to the billing inquiries address of the creditor as soon as possible, disputing any unauthorized charges. Not only must the creditor acknowledge your complaint in writing within 30 days of receiving your letter, but they must resolve the dispute within two billing cycles, which is usually not more than 90 days.

Paul R. Paradise's most recent book is Trademark Counterfeiting, Product Piracy, and the Billion Dollar Threat to the U.S. Economy

Paul R. Paradise

How identity thieves get your personal information:

- They steal wallets and purses containing your identification and credit and bank cards.
- They steal your mail, including your bank and credit card statements, pre-approved credit offers, telephone calling cards and tax information.
- They complete a "change of address form" to divert your mail to another location.
- They rummage through your trash, or the trash of businesses, for personal data in a practice known as "dumpster diving."
- They fraudulently obtain your credit report by posing as a landlord, employer or someone else who may have a legitimate need for - and a legal right to - the information.
- They get your business or personnel records at work.
- They find personal information in your home.
- They use personal information you share on the Internet.
- They buy your personal information from "inside" sources. For example, an identity thief may pay a store employee for information about you that appears on an application for goods, services or credit.

How identity thieves use your personal information:

- They call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to the new address, it may take some time before you realize there's a problem.
- They open a new credit card account, using your name, date of birth and SSN. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.
- They establish phone or wireless service in your name.
- They open a bank account in your name and write bad checks on that account.
- They file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.
- They counterfeit checks or debit cards, and drain your bank account.
- They buy cars by taking out auto loans in your name.

Source: Federal Trade Commission