Protect Yourself Against Identity Theft

Each year, about nine million American adults become victims of identity theft, according to annual surveys co-sponsored by Javelin Strategy and Research and the Better Business Bureau. This illegal activity is costing individuals and businesses in the U.S. more than $50 billion per year.

Staying aware of the problem and facing it head on can keep you ahead of the identity thieves. In this special report, OppenheimerFunds provides information and resources you can use to protect yourself from becoming a victim.

Defining Identity Theft

"Identity theft" has become a catch-all term for a variety of activities with a common purpose—to transfer wealth from one person to another, secretly and illegally. Nobody commits identity theft in broad daylight, and the motive usually is money.

On one level, identity thieves are akin to house burglars—but there are important differences that make stolen identities more devastating than purloined physical property:

- Many people don't know they have become victims of identity theft until well after the fact, when it's too late to recover losses or capture the guilty. The longer a pattern of theft goes undetected, the more devastating it can be
- Identity theft focuses not on tangible property that can be kept under lock and key but rather intangible financial assets—especially bank checking and debit/credit card accounts. Many people trust financial institutions to safeguard their assets in such accounts. But it can be far easier to open an account electronically, using the owner's personal data, than to break into a physical vault
- The most sophisticated type of identity theft, called "application fraud," occurs when a perpetrator opens **new** accounts using a stolen name and Social Security number. If statements are routed to a phony address, this activity can go undetected for months, especially if account activity and credit reports are not closely monitored
- In addition to losing property, identity theft victims can lose their sense of security, their credit standing and potentially their good names. In the worst cases, application fraudsters have been charged with felony crimes under assumed identities. Innocent people suddenly find they have outstanding warrants or criminal records to clear

Why Identity Theft Is a Growing Threat

Identity thieves thrive by exploiting a complex and interconnected web of systems—starting with the World Wide Web itself. Several years ago, many private companies and public records repositories began working toward a "paperless environment," which meant making personal data and transactions available electronically. For example, county clerks all over the U.S. began converting filing cabinets of paper documents into e-documents that could be accessed via the Web from anywhere in the world, often for free. The fact that many of these documents contained names, addresses and Social Security numbers—the raw materials of identity theft—did not attract much attention at first.

Meanwhile, banks moved from "eyeball transactions" between tellers and customers to impersonal ATM transactions, where only an account number and PIN number are needed to access cold cash. Tax preparers began to "outsource" work to foreign countries, which meant sending

the most sensitive and confidential data of Americans halfway around the world electronically. The credit reports of almost everyone became easily available online to anyone capable of posing as an employer, landlord or creditor.

In our "database age," vast amounts of sensitive personal data can be stored on portable electronic devices small enough to fit in a shirt pocket. When databases are "hacked" or such devices are lost or stolen, data can quickly filter through black-market channels into the hands of accomplished identity thieves. In February of 2005, one of the nation's largest data aggregators, ChoicePoint Inc., disclosed that it had been the victim of a break-in that compromised personal records of 145,000 people. However, this alert was sounded by the company five months after the fact. Authorities estimated that about 1,500 people were victimized and incurred losses from the scheme, allegedly orchestrated by a ring of seasoned identity thieves operating in Nigeria.

The post-9/11 environment of terror prevention also has helped identity thieves by causing financial institutions to demand more "know-your-customer" data. Now, at minimum, a thief who steals a bank application from an unlocked mailbox is almost guaranteed to get the applicant's name, address, date of birth, Social Security number and driver's license number. Finally, this trend has spawned a new global cottage industry among computer-literate people who live on the fringes of the U.S. economy or in impoverished nations abroad. To many of these individuals, it does not seem morally wrong to rip off Americans affluent enough to have financial accounts and credit cards. In some foreign jurisdictions, their crimes aren't a high priority of law enforcement.

While these trends together have created a new genre of American anxiety, consumers can take heart in one reality: Awareness about identity theft is growing, and awareness and education are the first steps in an effective defense.

What You Can Do About Identity Theft

OppenheimerFunds has identified specific actions you can take for theft prevention or loss recovery. The Identity Theft Checklist on page 6 can help you take steps that experts recommend to protect yourself.

Credit, debit and ATM access cards

- According to a survey conducted by the FDIC, two-thirds of all identity theft victims have had credit or debit cards misused. This is by far the biggest category of theft based on incidence and loss
- "Customer copies" of card transactions should never be casually discarded. Take them home and shred them. Do not sign any slip that includes a carbon copy (They are no longer used by reputable merchants.)
- Do not write credit card numbers on personal checks unless this is required by the merchant for a valid reason (In some states, it is illegal to require this.)
- On one sheet of paper, create a list of all personal credit and debit cards, including account numbers, expiration dates, and phone numbers to call in case of emergency. Keep this list in a safe place at home where it can easily be accessed to quickly report any loss or theft. (It's also a good idea to record on this list all bank account numbers and bank ATM access cards.) If this list is stored on a PC or personal digital device, make sure it is password protected or encrypted
- Memorize any PIN numbers attached to credit, debit or ATM access cards. Never carry written PIN numbers in a wallet or purse
- Check credit/debit card statements carefully each month with an eye for fraudulent charges. Report any such charges immediately, and freeze that account pending investigation and resolution
- Consolidate spending by using only one or two cards. Remove other cards from wallets or purses and lock them in a safe place. (Better yet, cancel them.) This makes reporting easier if the wallet or purse is lost or stolen. It also simplifies monthly statement checking
- Several anti-identity theft organizations urge consumers to use credit cards instead of debit or ATM access cards. The federal Fair Credit Billing Act limits the customer's responsibility on a credit card to the first $50 when it can be determined that the card was used without authorization. However, Privacy Rights Clearinghouse advises that there is no such limit on debit card losses: "Your checking account could be wiped out in minutes. Further, debit and ATM cards are not protected by federal law to the extent credit cards are"

Credit and credit reports

- Households with substantial assets and reputations to protect should consider purchasing a credit monitoring service. For a fee of $7–$15 per month, these services provide daily alerts on all credit activity, including inquiries, new account applications, changes of address and public record filings. These alerts can detect both plain-vanilla credit thefts and also the more sophisticated application fraud. The premier level of credit monitoring service includes up to $25,000 of

identity theft reimbursement coverage plus consolidated reports from all three leading credit reporting services: Equifax, Experian and TransUnion. The organization "Fight Identity Theft" offers an online comparison of leading credit monitoring services on its site: www.fightidentitytheft.com

- As an alternative to paying for credit monitoring, U.S. consumers now are entitled to receive a free report from each of the three reporting services once per year. By spacing these requests four months apart, it usually is possible to detect problems before they escalate. Once a report of suspected theft of fraud is filed with a credit reporting company, free credit reports are automatically available

- When a theft happens, request a "fraud alert." Each of the three credit reporting agencies offers an 800 or 888 (toll-free) number for reporting suspected credit fraud (See the Recovery Steps on page 7.)

- Once an alert is requested at one of the three services, the account usually will be flagged by all. If a thief then tries to set up accounts or obtain credit, financial institutions should know to contact the customer directly before issuing an approval. An alert automatically removes a customer's name from all pre-approved credit offers for two years

- Federal law now accords specific rights to victims of fraud, including the right to block any information in a credit report that has resulted from theft or fraud, the right to obtain copies of documents used to commit theft or fraud, and the right to block debt collection activities resulting from theft or fraud

Social Security numbers

- Social Security cards should never be carried in wallets or left visible on desks. Each number should be memorized by its owner and then the card should be stored in a safe place, such as a locked drawer or safety deposit box

- Whenever a Social Security number is requested by any federal, state or local government, it must be accompanied by a disclosure statement that explains whether providing it is mandatory. It's a good idea not to release the number unless required

- The only time a private establishment has a right to ask for a Social Security number is when it is required for identity verification (as on credit applications) or for IRS reporting. When a consumer voluntarily gives the number to a private business and it is then misused, there is little recourse

- In the past, many colleges have used Social Security numbers as student ID numbers. However, Social Security numbers now fall under protection of the "Buckley Amendment," which requires the student's written consent prior to the release of educational records. Public schools and all schools receiving federal funding may not make student Social Security numbers publicly available

- Many types of public records routinely capture Social Security numbers. They include divorce and bankruptcy filings, deeds, liens, mortgages and affidavits. When these records are scanned into public databases, the Social Security numbers become easily accessible to the world. To make this point, privacy watchdogs posted online a copy of a deed filed by Florida Governor Jeb Bush and his wife, including their clearly legible Social Security numbers. Fortunately, Florida was the first state to pass a "redaction law," which allows individuals to request that their Social Security numbers be redacted (blurred) in public access filings. (Governor Bush has since had his own "dirty deed" redacted.) Many states and counties nationwide have announced initiatives to use software programs for automatically redacting Social Security numbers. However, privacy rights advocates say there is not yet a software program on the market that is 100% successful in recognizing and redacting **handwritten** numbers. When a citizen requests removal under redaction laws, public officials must blur that individual record by hand, if necessary. In filing any public record that requires a Social Security number, it's a good idea to type the number on the document, so mechanical redaction is easier

Financial and tax business in general

- Identity theft is a strong reason for choosing reputable financial companies and consolidating assets and accounts with them. This can result in fewer statements floating through the postal system or cyberspace and more convenience in monitoring account activity each month

- Under federal law (Gramm-Leach-Bliley), all financial institutions are required to send customers an annual notice describing how they collect and share information. The notice may include instructions or a form on which consumers consent or decline to have their information shared with nonaffiliated companies. Consumers should read and consider these "elections" carefully. Taking no action often can result in "implied consent" to have information shared

- One major exception that falls outside the scope of Gramm-Leach-Bliley is called a CLUE report. It allows information to be freely shared between companies that issue homeowner's insurance and automobile insurance, without notification or consent. Consumers should know that they have a right to receive a copy of their CLUE reports and dispute any errors

- Another major exception that falls outside Gramm-Leach-Bliley is a loophole that allows financial data to be shared with foreign companies. This has become an issue in the

tax preparation industry, because large U.S. chains are electronically transmitting millions of personal tax returns per year overseas for preparation by outsourced vendors, often in developing nations. In some countries, low wage scales make it easier for workers to sell financial data to thieves. U.S. taxpayers should ask whether their personal data will be transmitted outside the office to which the tax return is delivered, and under what circumstances. Since high volume "assembly line" tax prep firms are the biggest users of foreign outsourcing, it can be a smart strategy to use reputable local CPAs or independent tax professionals who perform their own work "in the same building"

Other helpful ideas

- Aside from the Social Security number, the most important piece of data that identity thieves can use to crack into accounts (or create new ones) is the driver's license number. Be very careful about sharing this number. Be wary of writing this number on checks, unless it is required by a reputable merchant

- Low cost personal shredders can be a simple defense against "dumpster diving"—the art of searching through garbage receptacles for sensitive personal information. Electronic documents (which can't be shredded) also offer rich opportunities for identity thieves. Social Security numbers, driver's license numbers, and personal account numbers should not be included in emails, posted on Internet bulletin boards, or shared with strangers online

- Some types of scams are not very common but can still be costly and frustrating when they occur. For example, ordinary common ballpoint pen ink can be chemically removed from checks by a skilled scammer, creating an opportunity to prowl unlocked mailboxes and then write "blank checks." The remedy is to sign checks with special pens containing permanent, non-erasable ink. Also, identity thieves at times may pose as a real person (in the flesh) and open store charge accounts with false names and addresses. The remedy is to periodically check personal credit reports or use a monitoring service that issues automatic daily alerts whenever a merchant inquiry is made

- Travelers are especially vulnerable to identity theft because they usually carry extensive personal identification and various credit, debit or ATM access cards. It's a good idea not to take Social Security cards or checkbooks on vacations or business trips. When money and valuables are locked away in room safes, make sure sensitive personal information and documents go into the safe as well

- Unsecured computer connections can be "easy pickings" for sophisticated identity thieves. When using an unfamiliar broadband connection or network to access the Internet, always ask if it is secure before typing sensitive personal data. In most popular browsers, it is advisable to use the highest security setting possible for such transactions

- These settings also can protect against being routed to bogus websites that appear legitimate

- Using relatively inexpensive software packages, it is possible to encrypt sensitive personal data stored on PCs or in databases. Small businesses that must store sensitive customer records electronically should use encryption to guard against data accidents or theft

- Never throw cancelled checks or check stubs away unshredded. They contain all the data that a sophisticated check fraudster needs to wipe out a checking account

- Unlocked mailboxes are one of the easiest targets. Never leave sensitive mail for pick up in unlocked receptacles, such as the drop baskets of hotel lobbies. Sensitive mail includes: 1) checks; 2) credit card statements or numbers; and 3) Social Security or driver's license numbers

- Do not discard old computers that contain sensitive personal data on hard drives. Do not allow computer repair services to "recycle" a defective hard drive when they replace it. Deleting sensitive files or reformatting a drive does not permanently remove all data. According to one provider of hard drive security software: "The only way to erase hard drive data is to overwrite your hard drive with random information"

- Aside from the insurance included in credit monitoring services, several leading insurance companies offer separate identity theft insurance. For a modest premium, these policies reimburse specified losses or costs including lost wages and recovery activities (in some cases), up to a limit. The Insurance Information Institute (III) offers a list of carriers at: www.iii.org/individuals/other/insurance/-identitytheft

Keep in mind that this insurance does not protect against one major type of loss—the emotional impact of having one's personal identity invaded and exploited. According to Privacy Rights Clearinghouse: "The emotional impact of identity theft has been found to parallel that of victims of violent crime."

Don't Be a Victim

You've worked the better part of your lifetime building assets and your reputation for using credit wisely. Don't let identity theft rob you of these accomplishments. Take some time to review the ideas in this report, as well as the additional resources on the following pages.

Resources

Glossary of Identity Theft Terms and Practices

Dumpster diving: Rummaging through trash cans and bins for discarded personal documents. Shredders will usually thwart dumpster divers.

Hacking: The act of breaking into computer networks, databases or personal PCs to obtain sensitive or confidential data. While most hackers focus on penetrating big data caches, some troll unsecured networks seeking individual targets. Some sophisticated hackers can initiate requests for credit or account withdrawals from the victim's own PC.

Keylogging: Software that can monitor Internet sessions and log specific keystrokes, including account numbers, PINs and Social Security numbers. Any time individuals work on an unsecured Internet connection (especially a wi-fi hotspot), they are vulnerable to keyloggers.

Phishing: Sending emails that appear to come from a legitimate financial institution, with a link back to a fraudulent email address or website in the name of that same institution. Phishers usually want access to personal bank account numbers, PIN numbers and Social Security numbers. They can be thwarted by refusing to supply personal data in response to unsolicited email.

Pretexting: Obtaining personal information under false pretexts as would be the case when a thief pretends to be a potential employer or landlord in order to obtain a credit report. Pretexters often contact relatives or close friends of their targeted victims, asking to "verify" information. They also take advantage of gullible children to obtain data about parents.

Shoulder surfing: This is the nosiest kind of identity theft—looking over the shoulder of a person using an ATM machine to steal a PIN. In extreme cases, surfers use telephoto-equipped video cameras. Avoid crowded ATM lobbies and cover the touch screen or keypad with your free hand.

Skimming: Capturing a customer's credit card number in a retail store or restaurant while the transaction is being made. Skimmers often double swipe cards: once legitimately and again to capture data for themselves. The only defense is to watch the swipe closely, if possible, and patronize honest establishments.

Spyware: Software applications that invade PCs and track their activities or change their settings without warning. While most spyware is designed to increase Internet traffic or advertising exposure, some have more sinister intent. Firewalls and antispyware programs can increase protection at a low cost.

Useful Links for Learning More About Identity Theft

www.consumer.gov/idtheft
This is the Federal Trade Commission's official site for combating identity theft. It contains useful links to a variety of other resources, including instructions on how to file a complaint with the FTC when a suspected violation has occurred.

www.privacyrights.org/identity.htm
This information-packed site is sponsored by the organization Privacy Rights Clearinghouse. It includes numerous, brief FAQs on identity theft, plus quizzes that can help to test knowledge about effective prevention.

www.idtheftcenter.org
This is the home page of the Identity Theft Resource Center's site. This nonprofit organization was founded by Linda Foley, who was herself an identity theft victim. It offers resources for recovering victims of identity theft.

www.ssa.gov/pubs/idtheft.htm
This is Social Security's gateway to information on the subject, focusing primarily on ideas for protecting Social Security numbers. It also offers a link to the Office of the Inspector General and its hotline for reporting suspected fraud involving Social Security numbers or data.

www.fightidentitytheft.com
This unique site was built by a concerned individual, Dave Nielsen, to distribute useful information on the subject. It contains one of the best identity theft blogs on the Net and objective reviews of credit reporting and monitoring services.

www.opcva.com/watchdog
This interesting site was created by "Virginia Watchdog" Betty Ostergren, a woman who has garnered attention for publishing sensitive personal data belonging to leading politicians and policymakers. She does not "out" them by actually putting their data online (which would be a crime in some cases). Rather, she publishes links to public databases where this information is available for free (or low cost). Her goal is to force influential public figures to pass "redaction laws" that give everyone the right to blur personal data in public filings. She also blogs many news accounts involving identity theft or fraud.

Identity Theft Checklist

Question	Check if "Yes"	Remedies or Action Steps if "No"
1. *Do you avoid carrying sensitive personal data (Social Security number, PIN numbers) in your wallet?*		
2. *Is your home mailbox locked? Do you avoid dropping off mail in unlocked boxes?*		
3. *When asked by a merchant for your Social Security number, do you ask if this is required and why?*		
4. *Do you avoid using your Social Security number as a general ID number at school, work, clubs, etc?*		
5. *Do you subscribe to a credit monitoring service? Or do you take advantage of free credit reports from each reporting service once per year?*		
6. *Do you own and use a personal shredder to dispose of sensitive data or documents?*		
7. *If you store sensitive personal data on a hard drive, is it located in a place in your home or office that is not easily accessible? Is any sensitive data on it encrypted?*		
8. *If you access the Internet via a home or wi-fi network, is it secure?*		
9. *When you make a charge on your credit card, are you careful to watch how it is handled?*		
10. *Do you have a detailed record of all the credit, debit or ATM access cards that you own—and addresses for reporting loss or theft of each?*		
11. *Do you review your credit or debit card statements and bank accounts each month with an eye toward unauthorized charges or withdrawals?*		
12. *Do you always avoid sharing sensitive personal information with strangers via phone or email?*		
13. *Have you checked public databases to be sure your Social Security number is not easily accessible? Are you aware of any redaction laws in your state?*		
14. *Have you consolidated your financial business with a few solid companies whom you can trust?*		
15. *Are you sure your tax return is being prepared locally, so that your tax data stays in the same office to which it was delivered?*		

Identity Theft Recovery Steps

1. ***File a fraud alert with a credit reporting company.***

   Normally, a report to one will trigger reporting to all three:
   Equifax: 1.800.525.6285; P.O. Box 740241, Atlanta, GA 30374
   Experian: 1.888.397.3742; P.O. Box 9532, Allen, TX 75013
   TransUnion: 1.800.680.7289; P.O. Box 6790, Fullerton, CA 92834-6790

2. ***Review credit reports to see how extensive the theft or fraud activity has been.***

   After a fraud alert has been filed, the consumer is entitled to receive a free copy of his/her credit report. If the theft or fraud is believed to be extensive, consumers can take a further step and request a "security freeze" on their credit reports. This prevents anyone from accessing the credit file until the consumer unfreezes it.

3. ***File an identity theft report with a local, state or federal law enforcement agency.***

   Under federal law, filing this report is the first step in blocking fraudulent information from appearing on a credit report. The next step is to send a letter to the credit reporting agency or agencies reporting to them that specific information is fraudulent. The information in question must be blocked within four days of receipt of this letter.

4. ***Contact the issuer of each credit card involved in the theft or fraud.***

   The first contact should be by phone and the next by letter, sent to the address for "billing inquiries." These contacts trigger the limit on liability of $50 per card for unauthorized charges.

5. ***If debt collectors are a problem due to fraudulent debts, write the collector a letter instructing them: 1) to stop collection efforts; and 2) that the money in question is not owed.***

   Under federal law, the collection agency must stop all contact, except to advise in writing of specific actions it intends to take.

6. ***File a complaint with the FTC.***

   Use the online complaint form located at www.consumer.gov/idtheft. Click on "File a Complaint." The FTC can instigate law enforcement investigations, especially if it detects a pattern of repeat thefts or frauds.

Before investing in any of the Oppenheimer funds, investors should carefully consider a fund's investment objectives, risks, charges and expenses. Fund prospectuses contain this and other information about the funds, and may be obtained by asking your financial advisor, calling us at 1.800.525.7048 or visiting our website at www.oppenheimerfunds.com. Read prospectuses carefully before investing.

Oppenheimer funds are distributed by OppenheimerFunds Distributor, Inc.
Two World Financial Center, 225 Liberty Street, New York, NY 10281-1008

CC0000.136.1006 November 24, 2006

OppenheimerFunds®
The Right Way to Invest