How much can you spend in two days? One Massachusetts man charged roughly $18,000 last fall at stores such as Home Depot, Pier 1 Imports, Banana Republic and Wal-Mart, but he didn’t pay a dime. Instead, a Massachusetts state legislator – a victim of identity theft – received the exorbitant bill.

Identity theft is the fastest growing white-collar crime and has been the number one crime reported to the Federal Trade Commission for the past four years. According to a 2003 survey by the commission, 9.9 million Americans were victims of identity theft in 2002, resulting in losses of roughly $48 billion for businesses and financial institutions and $5 billion in out-of-pocket expenses for the victims.

Today, states are wrestling with ways to reduce the risk of identity theft, to better identify possible cases of the crime, and to more effectively investigate and prosecute the record number of cases. States are also searching for improved methods to restore a victim’s identity and credit, which can be a long and frustrating process.

However, the problem of identity theft extends beyond state borders and policies, to private sector practices and the personal habits of individuals. Consequently, state strategies to address the problem are increasingly multi-disciplinary, involving a mix of government and business practices and public awareness campaigns.
“Although part of the dramatic rise may be the result of increased reporting, cultural trends suggest that identity theft is on the rise. The popularity of the Internet and its interconnectedness, the ease and frequency of online financial transactions, and growing reliance on credit cards all contribute to the problem.”

**Scope of the Problem**

The Fair and Accurate Credit Transaction Act of 2003 defines identity theft as a fraud committed using the identifying information of another person, such as a Social Security number, date of birth, address, credit card number or other financial information.

According to the FTC, 85 percent of all victims in 2002 reported financial misuse. The remaining 15 percent, 1.5 million people, reported use of their personal information for nonfinancial purposes. For example, a criminal may use someone else’s identity to obtain a government document or to mislead law enforcement when stopped or arrested for a crime.

Recent spikes in the number of identity theft cases may be slightly misleading since accurate methods to identify and report the crime did not exist before 1997. Many cases in the 1980s and 1990s likely went unreported. In 1997, the FTC created the Consumer Sentinel, a secure investigative tool and complaint database. The commission also established an Identity Theft Hotline and Web site soon after to improve information gathering.

Although part of the dramatic rise may be the result of increased reporting, cultural trends suggest that identity theft is on the rise. The popularity of the Internet and its interconnectedness, the ease and frequency of online financial transactions, and growing reliance on credit cards all contribute to the problem.

Other factors include the availability of personal information on documents such as driver’s licenses, birth and death certificates, and financial documents; the ease of obtaining this information in physical or cyber form; a lack of sanctions and deterrence by government; and the low priority placed on identity theft cases by the law enforcement community. Identity theft perpetrators are increasingly preying on the elderly, mainly because of their higher lines of credit, greater home equity, and abundance of financial resources compared to younger populations. According to the Privacy Rights Clearinghouse, the number of incidents of identity theft among people over the age of 60 increased from 1,821 in 2000 to 5,802 in 2001. This trend is especially alarming given the record number of people expected to retire in the next decade.
Another troubling trend is the theft of personal information from people who have died. According to the National Association for Public Health Statistics and Information Systems, approximately 2.3 million deaths are processed a year. Financial institutions often are not immediately notified when a customer dies and will keep an active credit file open for up to 10 years without activity. Unless a friend or family member notifies the financial institution, the current process is lengthy and paper-based. States must transmit death information to the Social Security Administration, which then notifies the financial institutions.

Identity thieves can easily obtain information about the deceased through obituaries, death certificates or the Internet. Many such cases involve family members who try to steal Social Security checks and other retirement benefits.

Who is Responsible?

Nearly every public agency, branch of government, business and citizen has a role in addressing identity theft. However, many state governments are taking the lead to address this growing problem.

As the flurry of legislative activity last year showed, state policymakers are establishing identity theft as a priority: 22 states adopted identity theft legislation in 2003. Most policy changes focused on the following aspects:

- Defining the crime of identity theft and related offenses.
- Assigning penalties.
- Reporting procedures for victims.
- Victims’ restitution.
- Empowering law enforcement agencies.
- Freezing credit reports and alerting credit agencies.
- Controlling the use of personal information and the electronic media.

Along with crafting policies to prevent identity theft, state practitioners also play a large role in addressing the crime once it occurs. State and local law enforcement agencies are playing heightened roles in reporting possible cases and tracking identity theft trends. The crime is also becoming a greater priority for investigative agencies and state and local prosecutors, especially given the greater authority and additional tools provided through the legislative process.

In addition, state motor vehicle and vital record administrators handle personal information on a regular basis. State-issued driver’s licenses not only grant driving privileges, they are also used to board airplanes, open bank accounts and apply for credit. State motor vehicle administrators, therefore, have an important responsibility to verify applicants’ identities. However, states often do not have the resources to check applicants’ Social Security numbers to ensure they are valid. In addition, law enforcement and financial institutions often fail to identify invalid driver’s licenses because of a lack of uniformity among states and lack of education as to what constitutes a valid license.

Similarly, states are responsible for maintaining vital records and statistics, including official records on live births, deaths, fetal deaths, marriages, divorces and adoptions. The death certificate function is especially prone to error and mismanagement given the complexities and the number of people involved, including funeral directors, physicians, medical examiners, coroners, hospitals, medical records professionals, and vital records and statistics officials.

Businesses and citizens also play important roles in protecting and managing personal information. Financial institutions and businesses that sell products maintain control over sensitive information such as Social Security numbers, dates of birth, home addresses and credit card information. Likewise, citizens have a responsibility to safeguard their own personal information.

Future Focus for State Governments

As states form strategies to address identity theft, they should focus on the following areas:

1. Empower law enforcement. State and local law enforcement officials need the authority and tools to identify, investigate and prosecute identity theft cases. Illinois and Louisiana recently took legislative steps to address this issue. Illinois H.B. 2188, signed into law by Gov. Rod Blagojevich in 2003, provides citizens with an avenue to initiate a law enforcement investigation by contacting the local law enforcement agency with immediate access to consumer fraud-related complaints. This information allows law enforcement personnel to identify trends at the local, regional and national levels.

2. Focus resources on the elderly. Given that the elderly are much more vulnerable to identity theft, states should consider dedicating greater attention and resources to assisting this population. Michigan Attorney General Mike Cox, for example, recently began an initiative entitled “MI Identity” that involves visits to adult care facilities to conduct interviews with residents and free credit checks to determine if they are victims of identity theft.

3. Implement electronic death registration systems. Although each state requires death records to be registered within a specific time period, many death certificates contain inaccurate entries or are not completed until months after the death occurred, and many coroner cases take weeks or even months to resolve.

Continued on Page 34
Identity Theft – Continued from page 21

In automating the death registration processes, states can help to prevent identity theft by shortening the time to notify the Social Security Administration and financial institutions. “Implementation of the electronic death registration system will tremendously improve accuracy and timeliness of death notification to the states and financial institutions,” said Kenneth Bean, executive director of the National Association for Public Health Statistics and Information Systems. Currently, only five states have such a system in place.

4. Continue to safeguard Social Security numbers and other personal information. State agencies should minimize the use of Social Security numbers. States should implement added layers of protection for paper and electronic personal information such as Social Security numbers, dates of birth, home addresses and phone numbers.

5. Review motor vehicle policies and documents. State vehicle administrators should check applicants’ Social Security numbers against the national Social Security data bank to ensure they are valid. Also, adopting minimum uniform standards for state-issued driver’s licenses would improve law enforcement officials’ ability to identify fraudulent cards and identifications.

6. Collaborate on the interstate issues. According to a Wisconsin Professional Police Association article by former Attorney General Jim Doyle, “obtaining records and pursuing offenders requires increased cooperation among law enforcement agencies and prosecutors in different counties and states.” State investigative and prosecutorial agencies need to develop and implement multistate agreements and protocols to effectively work across state borders on identity theft cases. Additionally, many businesses operate in several states, requiring them to try to adhere to multiple sets of standards and business practices, which can be difficult. When drafting and promulgating new laws, states need to consider the practical implications for businesses.

7. Implement public awareness campaigns. Most citizens today are familiar with the identity theft issue because of television commercials sponsored by credit card and banking institutions. State governments should use this publicity as a springboard for improved outreach and education for citizens. Through different media venues, states can communicate the importance of the issue and recommend personal protective measures.

8. Share solutions. Given the urgency of the identity theft problem, states are feverishly inventing new and effective ways to prevent and respond to the growing issue. A clearinghouse of innovative solutions and means to communicate practices across state lines would streamline the states’ efforts.

The openness created by the Internet, the rising frequency of credit card transactions, and general carelessness regarding personal information make identity theft a daunting challenge for government officials. It will require more than a single piece of legislation to deter future identity thieves and to change law enforcement priorities, business practices, and citizens’ habits.

Many states are taking the lead in addressing the problem, but it will surely take a team effort by all layers of government, businesses and citizens to curb this growing crime trend.

— Chad Foster is a public safety and justice policy analyst at The Council of State Governments.

Federal Policy

Initiatives


The Identity Theft and Assumption Deterrence Act of 1998 was the first major policy initiative by the federal government to address the crime. The act:
- Makes identity theft a federal crime with penalties of up to 15 years imprisonment and a maximum fine of $250,000.
- Establishes that the person whose identity was stolen is the true victim.
- Allows for the identity theft victim to seek restitution if there is a conviction.
- Empowers federal, state and local law enforcement agencies with the authority to address identity theft crimes.
- Establishes the Federal Trade Commission as a central agency to act as a clearinghouse for complaints, referrals and resources for assistance for victims of identity theft.

The Fair and Accurate Credit Transaction Act of 2003 provides added layers of protection for consumers against identity theft. Specifically, the act:
- Provides citizens with a free copy of their credit report to review for unauthorized activity;
- Requires merchants to leave all but the last five digits of a credit card number off store receipts.
- Creates a national alert system for fraud that is activated by one consumer phone call.
- Requires regulators to devise a list of red flag indicators of identity theft.
- Requires lenders and credit agencies to take action before cases of identity theft cause major damage.

Innovations Spotlight: MI Identity

Michigan Attorney General Mike Cox recently launched an identity theft campaign for 2004 to seek and prosecute identity thieves who target vulnerable adults. The initiative, named “MI Identity,” involves visits to adult care facilities to conduct interviews with residents and free credit checks to determine if they are victims of identity theft.

The campaign will also train local law enforcement on reporting and investigative techniques and provide consumers with additional information on ways to protect against the crime. For more information on Michigan’s initiatives, visit www.michigan.gov/ag.