IDENTITY THEFT

Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain

What GAO Found

Identity theft is a serious problem because, among other things, it can take a long period of time before a victim becomes aware that the crime has taken place and thus can cause substantial harm to the victim's credit rating. Moreover, while some identity theft victims can resolve their problems quickly, others face substantial costs and inconvenience repairing damage to their credit records. Some individuals have lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft. Millions of people become victims of identity theft each year. The Federal Trade Commission (FTC) estimates that in 1 year, as many as 10 million people—or 4.6 percent of the U.S. adult population—discover that they are victims of some form of identity theft, translating into reported losses exceeding $50 billion.

Several steps have been taken, both in terms of legislation and administrative actions to combat identity theft at the federal, state and local levels, although efforts to assist victims of the crime once it has occurred remain somewhat piecemeal. While there is no one law that regulates the overall use of personally identifiable information by all levels and branches of government, numerous federal laws place restrictions on public and private sector entities' use and disclosure of individuals' personal information in specific instances, including the use and disclosure of Social Security Numbers (SSN)—a key piece of information that is highly valuable to identity thieves. One intention of some of these laws is to prevent the misuse of personal information for purposes such as identity theft.

Despite efforts to prevent identity theft, vulnerabilities remain and can be grouped into several areas, including display and use of Social Security numbers, availability of personal information through information resellers, security weaknesses in federal agency information systems, and data security breaches. GAO's work indicates that persistent weaknesses appear in five major categories of information system controls, including access controls which ensure that only authorized agency personnel can read, alter, or delete data. As a result, federal systems and sensitive information are at increased risk of unauthorized access and disclosure, modification, or destruction, as well as inadvertent or deliberate disruption of system operations and services. GAO has reported that federal agencies continue to experience numerous security incidents that could leave sensitive personally identifiable information in federal records vulnerable to identity theft.