

G A O
Accountability · Integrity · Reliability

Highlights

Highlights of [GAO-05-1016T](#), a report to the Committee on Consumer Affairs and Protection and the Committee on Governmental Operations, New York State Assembly

Why GAO Did This Study

In 1936, the Social Security Administration established the Social Security number (SSN) to track worker's earnings for Social Security benefit purposes. Despite its narrowly intended purpose, the SSN is now used for a myriad of non-Social Security purposes. Today, SSNs are used, in part, as identity verification tools for services such as child support collections, law enforcement enhancements, and issuing credit to individuals. Although these uses can be beneficial to the public, the SSN is now a key piece of information in creating false identities. The aggregation of personal information, such as SSNs, in large corporate databases and the increased availability of information via the Internet may provide criminals the opportunities to commit identity theft.

Although Congress and the states have enacted a number of laws to protect consumers' privacy, the public and private sectors' continued use of and reliance on SSNs, and the potential for misuse, underscore the importance of strengthening protections where possible. Accordingly, this testimony focuses on describing (1) the public use of SSNs (2) the use of SSNs by certain private sector entities, and (3) certain federal and state laws regulating the use of SSNs and identity theft.

www.gao.gov/cgi-bin/getrpt?GAO-05-1016T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Barbara Bovbjerg at (202) 512-7215 or bovbjerg@gao.gov.

SOCIAL SECURITY NUMBERS

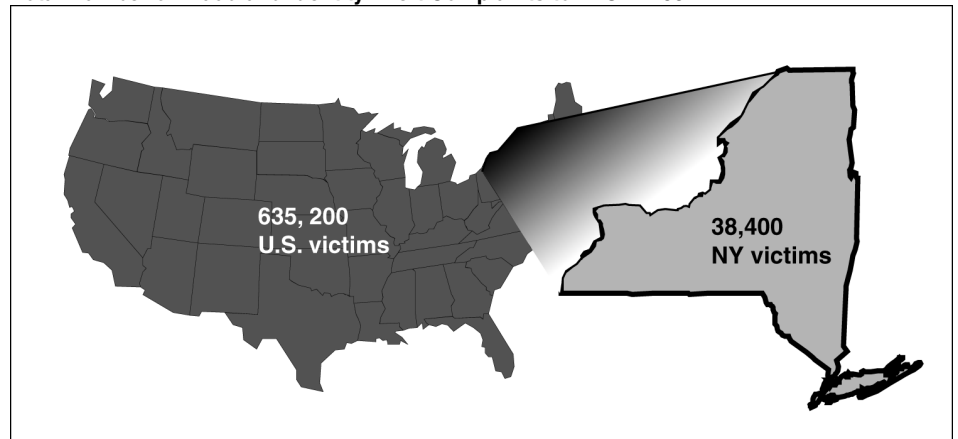
Federal and State Laws Restrict Use of SSNs, yet Gaps Remain

What GAO Found

The public and private sector use of SSNs is widespread. Agencies at all levels of government frequently collect and use SSNs to administer their programs, verify applicants' eligibility for services and benefits, and conduct research and evaluations of their programs. Although some government agencies are taking steps to limit the use and display of SSNs, these numbers are still widely available in a variety of public records held by states, local jurisdictions, and courts. In addition, certain private sector entities that we have reviewed, such as information resellers, credit reporting agencies (CRAs), and health care organizations, also routinely obtain and use SSNs. These entities often obtain SSNs from various public sources or their clients and use SSNs for various purposes, such as building tools that aid in verifying an individual's identity or matching records from various sources.

Given the extent to which government and private sector entities use SSNs, Congress has enacted federal laws to restrict the use and disclosure of consumers' personal information, including SSNs. Many states have also enacted their own legislation to restrict the use and display of SSNs, focusing on public display restrictions, SSN solicitation, and customer notifications when SSNs are compromised. Furthermore, Congress has recently introduced consumer privacy legislation similar to enacted state legislation, which in some cases includes SSN restrictions. Although there is some consistency in the various proposed and enacted federal and state laws, gaps remain in protecting individuals' personal information from fraud and identity theft. Some federal agencies are beginning to collect statistics on identity theft crime, which appears to be growing. For example, recent statistics show that identity theft is increasing in New York. In 2004, Federal Trade Commission (FTC) statistics indicated that over 17,600 New Yorkers reported being a victim of identity theft, which is up from roughly 7,000 in 2001.

Total Number of Fraud and Identity Theft Complaints to FTC in 2004



Source: GAO, FTC analysis and Art Explosion.