June 2007

PERSONAL INFORMATION

Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-737, a report to congressional requesters

Why GAO Did This Study

In recent years, many entities in the private, public, and government sectors have reported the loss or theft of sensitive personal information. These breaches have raised concerns in part because they can result in identity theft—either account fraud (such as misuse of credit card numbers) or unauthorized creation of new accounts (such as opening a credit card in someone else's name). Many states have enacted laws requiring entities that experience breaches to notify affected individuals, and Congress is considering legislation that would establish a national breach notification requirement.

GAO was asked to examine (1) the incidence and circumstances of breaches of sensitive personal information; (2) the extent to which such breaches have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements. To address these objectives, GAO reviewed available reports on data breaches, analyzed 24 large data breaches, and gathered information from federal and state government agencies, researchers, consumer advocates, and others.

What GAO Recommends

This report contains no recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-737.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David G. Wood at (202) 512-8678 or woodd@gao.gov.

What GAO Found

While comprehensive data do not exist, available evidence suggests that breaches of sensitive personal information have occurred frequently and under widely varying circumstances. For example, more than 570 data breaches were reported in the news media from January 2005 through December 2006, according to lists maintained by private groups that track reports of breaches. These incidents varied significantly in size and occurred across a wide range of entities, including federal, state, and local government agencies; retailers; financial institutions; colleges and universities; and medical facilities.

The extent to which data breaches have resulted in identity theft is not well known, largely because of the difficulty of determining the source of the data used to commit identity theft. However, available data and interviews with researchers, law enforcement officials, and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft, particularly the unauthorized creation of new accounts. For example, in reviewing the 24 largest breaches reported in the media from January 2000 through June 2005, GAO found that 3 included evidence of resulting fraud on existing accounts and 1 included evidence of unauthorized creation of new accounts. For 18 of the breaches, no clear evidence had been uncovered linking them to identity theft; and for the remaining 2, there was not sufficient information to make a determination.

Requiring affected consumers to be notified of a data breach may encourage better security practices and help mitigate potential harm, but it also presents certain costs and challenges. Notification requirements can create incentives for entities to improve data security practices to minimize legal liability or avoid public relations risks that may result from a publicized breach. Also, consumers alerted to a breach can take measures to prevent or mitigate identity theft, such as monitoring their credit card statements and credit reports. At the same time, breach notification requirements have associated costs, such as expenses to develop incident response plans and identify and notify affected individuals. Further, an expansive requirement could result in notification of breaches that present little or no risk, perhaps leading consumers to disregard notices altogether. Federal banking regulators and the President's Identity Theft Task Force have advocated a notification standard—the conditions requiring notification—that is risk based, allowing individuals to take appropriate measures where the risk of harm exists, while ensuring they are only notified in cases where the level of risk warrants such action. Should Congress choose to enact a federal notification requirement, use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications of breaches that present little risk.