New Privacy Concern for Employee Benefit Plans: Combating Identity Theft

Susan E. Bernstein
Special Counsel
Schulte Roth & Zabel LLP

Employers should review benefit plan administration policies to minimize the danger of identity theft.

Identity theft occurs when a criminal appropriates an individual's personal information such as name, address, date of birth or Social Security number to assume that person's identity to commit theft or multiple types of fraud. By exploiting personal and financial information, an identity thief can obtain a person's credit history; access existing financial accounts; file false tax returns; open new credit accounts, bank accounts, charge accounts and utility accounts; enter into a residential lease; and even obtain additional false identifying documents such as a duplicate driver's license, birth certificate or passport. Social Security numbers are the most widely used record identifier and the key link to sensitive personal information including individuals' credit reports, banking accounts and personal confidential records.

In 1998, Congress recognized the gravity of this problem by making identity theft a federal crime with penalties of up to 15 years of imprisonment and a maximum fine of $250,000.[1] Over the last five years, identity theft has become one of the fastest growing white-collar crimes in the United States.[2] The magnitude and prevalence of identity theft cases is disturbing:

- The Federal Trade Commission's Identity Theft Clearinghouse received 161,819 reports of identity theft in 2002.[3]
- The Social Security Administration's Fraud Hotline received approximetely 72,500 reports of Social Security number misuse in 2002.[4]
- Two consumer reporting agencies each recorded approximately 90,000 long-term fraud alerts in 2000.[5]

The proliferation of identity theft cases as well as the severity of the cost of the crimes to victims, the financial services industry and the criminal

Keywords: *identity theft; benefit plan administration; Social Security numbers*

DOI = 10.1177/0886368703261122

EXHIBIT 1

The California law prohibits any person or entity doing business in California from:

- Publicly posting or displaying an individual's Social Security number
- Printing a Social Security number on any card required by the individual to access products or services (such as on a health insurance identification card)
- Requiring an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted
- Requiring an individual to use his or her Social Security number to access an Internet web site, unless a password or unique personal identification number or other authentication is used
- Printing an individual's Social Security number on any materials (other than applications or forms) that are mailed to the individual, unless state or federal law requires the Social Security number to be on the document to be mailed

justice system demonstrates the need for strong action to protect individual privacy.

Federal Privacy Legislation Pending

In response to the disconcerting statistics, costs and consequences of identity theft, Senator Dianne Feinstein introduced federal legislation, known as The Privacy Act of 2003, to set new boundaries for the use of Social Security numbers and force more responsible handling of Social Security numbers.[6] The Privacy Act of 2003 would limit the abuse of sensitive personal information by requiring an individual's consent prior to selling or marketing such information.

Several other bills are also pending before Congress that would combat identity theft. The bills would restrict the sale, purchase or display of Social Security numbers; strengthen the authority of the federal government to protect individuals from the sale and purchase of Social Security numbers; establish civil and criminal penalties for the sale or purchase of Social Security numbers; and impose a ban on government-wide uniform identifying numbers.[7] By limiting access to and disclosure of Social Security numbers, lawmakers speculate that the proposed legislation will afford consumers greater privacy protection.

Efforts on the State Level

California was the first state to enact a law that restricts employers and employee benefit plans from using or disclosing Social Security numbers in any written material or communications unless certain conditions are met. The California law, which became effective July 1, 2002 (with a phased-in compliance schedule to be completed by July 2005), is intended to stop identity theft and restrain consumer credit reporting agencies that are accessing personal information through Social Security numbers.[8] (See Exhibit 1.)

Impact on Benefit Plans

Because the Social Security number is a unique identifier that does not change over time, it is widely used by employee benefit plans to identify plan participants, track account activity, manage records and provide participants with online access to their account activity. There is no legal requirement for employee benefit plans to safeguard Social Security numbers, other than compliance with the privacy requirements set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA, which restricts the use and disclosure of protected health information, including demographic information

EXHIBIT 2

Working without Social Security Numbers
Employee benefit plan administrative practices that do not require use of Social Security numbers include:

- Plan administration and tracking
- Identification on health insurance cards and other documents widely seen by others
- Distributing quarterly benefit statements, explanation of benefits, enrollment materials or other documents through the mail
- On-line services for participants to access benefit information
- Phone call verification to authenticate the caller
- Customer service to look up records for an individual
- Storing records on computers
- Sharing information with other organizations or companies

such as a Social Security number,[9] applies only to group health plans.

It would be a great proactive measure for plan sponsors to minimize the use of the Social Security numbers just as the Treasury Department recently elected to remove Social Security numbers from all Treasury checks. Plan sponsors should review all employee benefit plans, policies and practices with regard to the use of Social Security numbers. For example, plan sponsors that currently have a policy to use Social Security numbers when participants leave the plan administrator a voice-mail message or use Social Security numbers to look up plan-participant records, could implement new policies that require the use of different identifiers and thereby maximize the protection of participant's personal information.

To the extent that plan sponsors use Social Security numbers merely for administrative and record-keeping purposes, it would be prudent for plan sponsors to change current practices to eliminate or reduce the use of Social Security numbers when displaying, accessing or collecting information. Plan sponsors could help take Social Security numbers out of circulation by using an alternative identifier or by using truncated Social Security numbers by means of a bar code. (See Exhibit 2.)

In addition, plan sponsors should consider developing written policies for handling records with Social Security numbers, providing employees with training on responsibilities for safeguarding records and monitoring employees' access to such records. In most circumstances, the benefits to the employee benefit plan of using the Social Security number for administrative purposes does not outweigh the risks to participants of the continual use and disclosure of Social Security numbers.

Because the Social Security number is a unique identifier that does not change over time, it is widely used by employee benefit plans to identify plan participants, track account activity, manage records and provide participants with online access to their account activity.

By implementing policies and controls that abandon the use of Social Security numbers as participant identifiers, plan sponsors can help individuals manage and protect their personal information. Even if plan sponsors want to avoid some of the obvious economic costs and logistical barriers associated with implementing new administrative practices and procedures, plan sponsors should, at a minimum, implement a mechanism whereby individuals who want increased privacy could request the use of an alternative personal identifier in lieu of their Social Security number.[10]

Notes

1. Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (1998).
2. U.S. General Account Office. (2002, March). *Identity Theft. Prevalence and Cost Appear to Be Growing.* GAO 02-363.
3. Federal Trade Commission. (2003, January 22). *National and State Trends in Fraud and Identity Theft, January-December 2002.*
4. Social Security Administration Office of the Inspector General. (2003, July).
5. U.S. General Account Office. (2002, March). *Identity Theft. Prevalence and Cost Appear to Be Growing.* GAO 02-363.
6. Privacy Act of 2003, S. 745, 108th Cong., 1st Sess. (2003).
7. See, for example, Social Security Number Misuse Prevention Act, S. 228, 108th Cong., 1st Sess. (2003); Identity Theft Prevention Act, S. 223, 108th Cong., 1st Sess. (2003); and Social Security Number Privacy and Identity Theft Prevention Act of 2001, S. 1014, 107th Cong., 1st Sess. (2001).
8. Cal. Civ. Code § 1798.85.
9. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 2021. (1996).
10. For more information on identity theft, see http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm.

Susan E. Bernstein is special counsel with the New York law firm of Schulte Roth & Zabel LLP. Her employee benefit practice focuses on the design, implementation, administration and communication of tax qualified and nonqualified single employer and multiemployer defined benefit, defined contribution and welfare plans, supplemental retirement plans, deferred compensation plans and executive compensation. She received a B.A. from the University of Pennsylvania and a J.D. from the Benjamin N. Cardozo School of Law.