LITIGATION NEWS ONLINE

May 2006

New Jersey Enacts Identity Theft Protection Act

By Garth T. Yearick, Litigation News Associate Editor

Congress weighs similar legislation

Computers and computer networks operated by many businesses are storehouses for sensitive data about almost every American consumer, including social security and credit card numbers and other personal financial information. At present, many databases remain vulnerable to identity theft.

In response to this growing concern, New Jersey recently enacted an Identity Theft Protection Act to enable consumers to protect their personal financial data. The law allows consumers to place a security freeze on their consumer credit reports, which often will prohibit consumer-credit reporting agencies from releasing or changing credit information without the consumer's consent.

The New Jersey Act also creates a private cause of action for violations of certain of its provisions. Further, a credit reporting agency that willfully fails to comply with the law's security freeze provisions may be liable for punitive damages and attorneys' fees. The Act also specifies the manner in which businesses must notify consumers of security breaches affecting computerized records that contain personal information.

Congress is actively pursuing its own Identity Theft Protection Act. The current version of Senate Bill 1408 would also allow consumers to place a security freeze on their credit reports. It would also require businesses to create and enforce written procedural safeguards to ensure the security and confidentiality of sensitive personal information the businesses collect, maintain, sell, dispose of, or transfer.

Piecemeal state regulation often makes national compliance programs extraordinarily expensive and sometimes even impossible.

Like the New Jersey law, S.B. 1408 contains consumer notification provisions for security breaches involving sensitive personal information. In general, consumers would have to be notified within 45 days of discovery of the breach.

Significantly, S.B. 1408 would "preempt any State or local law that requires, or holds liable, a covered entity for safeguarding sensitive personal information, notifying affected individuals of breaches of security, or allowing a consumer to place, remove, or temporarily suspend a security freeze on his or her credit report." Instead of allowing consumers to bring private causes of action for violations, the Act specifies that enforcement authority would reside primarily with the Federal Trade Commission.

Congress has previously enacted several measures in this area, including the Identity Theft and Assumption Deterrence Act of 1998, which makes it a crime to intentionally transfer or use another person's means of identification for an unlawful purpose.

"When Congress is considering a comprehensive regulatory scheme, the regulated industry often will support even a very strict scheme in return for express preemption of state regulation," notes Gail E. Lees, Los Angeles, Co-Chair of the Section of Litigation's Consumer and Personal Rights Litigation Committee. She adds that state-by-state, "piecemeal regulation often makes national compliance programs extraordinarily expensive and sometimes even impossible because of conflicting

requirements."

Lois C. Greisman, Washington, DC, Co-Chair of the Section's Consumer and Personal Rights Litigation Committee and a former supervisor of the FTC's identity theft program, says S.B. 1408 clearly suggests Congress is seeking to create a single national standard. Greisman believes the bill would be beneficial because it would clarify when a consumer must be notified of a security breach. "Consumers can take steps to protect themselves, but only if they know of the breach," she says.

Greisman adds that S.B. 1408 builds upon existing federal law, particularly the Gramm-Leach-Bliley Act, by extending data security measures to nonfinancial institutions. She cautions that the bill's preemption of private causes of action in state court will be "the subject of much debate and possible litigation."

Greisman recommends that litigators pay close attention to these new measures in order to advise clients what steps to take to safeguard consumers' personal information, and what to do in the event of a breach.

» **Tell Us Your Thoughts on This Topic**

MORE INFORMATION

» **Current Issue**

» **Issue Archive**

» **About Litigation News**

» **Editorial Board**

RELATED RESOURCES

ONLINE RESOURCES:

» **Identity Theft Protection Act**

» **Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028**

» **Report of the Committee on Commerce, Science, and Transportation on S.B. 1408 |**

» **Consumersunion.org, "Lock up Your Credit Files"**

» **FTC Facts for Consumers on Identity Theft**

» **N.J. Stat. Ann. §§ 2C:21-17.6, 56:8-161-166, 56:11-30, 44-50**

ONLINE RESOURCES:

» Financial Services Modernization Act of 1999 (Gramm Leach Bliley Act), Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999)

Back to Top