NAMIC®

Issue Brief

A Public Policy Paper of the National Association of Mutual Insurance Companies July 2005

Security Breach Notification Laws:
What Threats Do They Pose for Insurers?

By David B. Reddick
State Affairs Manager – Southeast Region

Executive Summary

State legislators have moved quickly this year to enact security breach notification laws in the wake of some high profile security breaches. As of July 1, 19 states have enacted notification laws and bills are pending in seven other states.

While most new laws follow the California security breach notification law enacted in 2002, some important differences exist that could make insurers potentially more vulnerable to the new laws. These differences should be closely monitored and avoided in new bill introductions.

1. **Personal Information**. While most states follow California's definition for "personal information," four states expanded their definitions. These additions will make it more difficult for multi-state insurers to comply with such laws. For that reason, definitional expansions should be avoided in new bill introductions.

2. **Notice Triggers.** Most states follow California's disclosure trigger standard or some variation of it. However, Florida requires a 45-day disclosure deadline and requires businesses to maintain documentation for up to five years of possible security breaches that were judged not likely to harm individuals. These requirements should be avoided in new bill introductions.

3. **Further Notice Requirements**. Nine states require businesses to notify consumer-reporting agencies of security breaches, but the threshold that triggers the notice varies. Where new bill introductions are proposed, the threshold should be as high as possible to avoid further expenses for insurers.

4. **Notice Exemptions**. Eight states have specific exemption language that goes beyond the California law which allows businesses to follow their own disclosure procedures if consistent with the law. To ensure against any misunderstanding as to whether insurers must comply with these notification laws, new bill introductions should include specific exemption language.

5. **Penalties.** States vary widely on penalties for violations of the notification laws with at least 11 states following existing civil penalties or fraud laws. New bill introductions should avoid a private cause of action as allowed in five state laws, or a sliding penalty structure as outlined in the Florida law.

Background

Identity theft – the appropriation of one's unencrypted personal information by unauthorized individuals – has emerged as one of the most dominant white collar crime problems of the 21st century.[1]

A recent Federal Trade Commission (FTC) survey[2] found that nearly 10 million people – or 4.6 percent of the adult population – became victims of identity theft in a one-year period. Losses to businesses and financial institutions from identity thefts annually total $52.6 billion, [3] and identity theft has topped the FTC's annual complaints list for the fifth year in a row.[4]

Surveys show most identity thieves gain access to an individual's personal information not by electronic means, but through lost or stolen wallets, personal information stolen by family and friends or by mail stolen from one's mailbox.[5] Often, victims are unaware of the theft until credit card issuers or financial institutions alert them to suspicious account activity.[6] Researchers claim the emotional impact of identity theft parallels that of violent crime victims with individuals often spending up to 600 hours of their own time and $1,000 or more in out-of-pocket expenses trying to repair their credit standing.[7]

While many people may view identity theft as simply one individual perpetrating a crime against another individual, a growing number of more sophisticated identity thieves are stealing large batches of unencrypted personal information by hacking into computer systems and stealing computers or backup data tapes. Since February, the *Privacy Rights Clearinghouse* estimates that nearly 50 million individuals have had some portion of their personal information compromised through more than 40 different security breaches.[8] One of the most recent incidents involved CitiFinancial, a subsidiary of Citigroup, which reported that the account information for 3.9 million customers was lost when a backup tape being shipped to a credit bureau did not reach its destination.[9]

Identity theft has not gone unnoticed by state policymakers. Legislators have moved quickly to increase criminal penalties for persons convicted of identity theft and have enacted laws to limit the use of individual Social Security numbers, particularly by state agencies.[10]

State lawmakers also have looked to protect consumers from identity thieves by enacting laws that require consumers to be advised by mail or electronic means when the security of a data system, containing the consumer's personal information, has been compromised. In 2002, California lawmakers enacted the country's first security breach notification law[11] after computer hackers broke into the state's payroll database. So far in 2005, 19 states[12] have enacted similar laws with bills still pending in Massachusetts, Michigan, North Carolina, Ohio, Oregon, Pennsylvania and Wisconsin.

California's Security Breach Law

On April 5, 2002, computer hackers broke into the payroll database for the state of California. For more than a month, hackers rooted around in the personal information of 265,000 state employees, ranging from then Gov. Gray Davis to maintenance workers and clerks.[13]

To make matters worse, the California Controller's Office, which maintained the database at the time, did not discover the breach until May 7 and then did not alert state employees of the problem until May 21. When the hacking incident finally became public, lawmakers and state employees, whose Social Security numbers, bank account information, and home addresses were fair game for hackers, became outraged and demanded immediate action. The result was the country's first security breach notification law, which was signed in September 2002 and took effect on July 1, 2003.[14]

The California law defines "personal information" as an individual's name used in combination with the individual's Social Security number, driver's license or California Identification Card number, credit or debit card numbers and any information that permits access to an individual's financial account. The definition adds that the "good faith acquisition" of personal information is not a breach of security, provided that the information "is not used or subject to further unauthorized disclosure."

A "security breach" occurs when there is the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency, (person or business)."

Once a security breach has been detected, disclosure by a state agency, person or business must be made to the customer "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement." The law

also requires that any agency, person or business that maintains computerized data but does not own it to notify the owner or licensee of any breach "immediately" following the discovery. The California law, however, contemplates situations where the notice can be delayed if law enforcement officials determine it could impede their criminal investigation.

Notices may be sent either by a written or electronic format as long as the format is consistent with Section 7001 of the U.S. Code.[15] A "substitute" procedure is allowed if the cost of the notice exceeds $250,000 or more than 500,000 customers are affected. In those instances, a "substitute" notice can be satisfied by sending the affected customers an e-mail notice, posting a notice of the breach on the website of the agency, person or business, or sending a release to the major statewide media. If the agency, person or business has its own notification procedures as part of an information security policy, it is deemed compliant with the law.

Finally, California allows a customer injured by a violation of the law to institute a civil action to recover damages. Further, any agency, person or business violating the law can be enjoined, and rights and remedies under the law are cumulative.

Security Breach Laws in 2005

On February 15, 2005, ChoicePoint revealed that it had inadvertently turned over 145,000 consumer accounts to identity thieves in California posing as legitimate business people.[16] This announcement became a catalyst of sorts for some lawmakers, who rushed to enact security breach notification laws. A case in point is Arkansas, where lawmakers enacted their security breach notification law in slightly more than three weeks.[17]

Of the 19 states to enact security breach laws so far this year, most closely follow the California law, especially in defining a "security breach," but other important differences exist.

For example, California's law applies specifically to state agencies as well as to persons and businesses. Connecticut, Delaware, Maine, Minnesota, Montana, North Dakota and Texas, however, chose not to include state agencies in their laws, and the Indiana law is limited to state and local governmental agencies. The Georgia law applies only to "information brokers," defined as, "any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes."

Most states followed California's definition of "personal information." However, Arkansas and Delaware added "medical information" to their definitions while North Dakota added data elements covering an individual's birth date, mother's maiden name, employee ID number and the individual's digitized or electronic signature. New Jersey added an additional line to its definition which reads as follows: "Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data."

California law specifies that when a security breach is detected, disclosure "shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement." Most states followed this standard, but Connecticut, Indiana and Montana apply only a "without unreasonable delay" standard while Texas requires that notices be sent as "quickly as possible." Florida imposes an "unreasonable delay" standard, but requires that notices be sent within 45 days of the security breach being detected.

Most states also followed California's notification standard where the business entity does not own the data. The notice to the owner or licensee of the data must be "immediately following discovery" of a security breach. Maine and Louisiana applied the "most expedient time possible and without unreasonable delay" standard for data that businesses both own and do not own. Florida employs an "as soon as practicable" standard, but also specifies that the notice must be sent within 10 days. Illinois was the only state not to incorporate the law enforcement delay provision in its law.

Protocols for issuing the security breach notice are fairly straightforward in the California law and allow for a "substitute notice" procedure under certain circumstances. Businesses also are allowed to follow their own disclosure procedures if consistent with the law.

Most state laws followed California's lead, but Delaware requires a copy of the notice be promptly provided in writing to the Consumer Protection Division of the Department of Justice. New York requires notice to the state Attorney General, the Consumer Protection Board, and the state Office of Cyber Security and Critical Infrastructure Coordination. Maine requires the Director of the Office of Consumer Credit Regulation within the Department of Professional and Financial Regulation be notified when a "substitute" notice is contemplated.

Florida added a unique provision to its law that requires businesses to maintain documentation for up to five years of any incidents where the security breach was investigated and it was determined that the breach would not likely harm individuals. Businesses that fail to keep such documentation can be fined up to $50,000.

Arkansas, Delaware, Louisiana, Minnesota, Nevada, North Dakota, Rhode Island and Tennessee contain specific notification exemptions that go beyond the California provision. In Arkansas and Delaware, the language simply refers to compliance standards that offer greater protections than the security breach law provides. Nevada and Tennessee refer to the Gramm-Leach-Bliley Act, Minnesota mentions the Health Insurance Portability and Accountability Act of 1996, and Louisiana and North Dakota exempt financial institutions subject to compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. Rhode Island mentions all of these exemptions in its law.

Florida, Georgia, Indiana, Minnesota, Nevada, New Jersey, New York, Tennessee and Texas added a further notification procedure, requiring a separate notice to consumer reporting agencies when the security breach affects a certain number of customers. Unfortunately, this threshold varies widely, ranging from a low of 500 customers in Minnesota to a high of 10,000 Georgia and Texas residents. Florida, Indiana, Nevada, New Jersey and Tennessee each have a 1,000 person threshold while New York's threshold is 5,000 persons. Minnesota also requires the notices be sent to the consumer reporting agencies within 48 hours.

Not surprisingly, states vary widely on how they intend to approach violations of their laws. Louisiana, Maine, Tennessee, Texas and Washington, for example, followed the California approach, which allows individuals to bring a civil action if injured by a violation of the law. In Maine, businesses also will be subject to a fine of no more than $5,000 per violation, up to a maximum of $25,000 per each day the business is in violation of the law. Rhode Island imposes a civil penalty of $100 for each violation up to a maximum penalty of $25,000. The fines apply to state agencies as well as businesses.

State Attorneys General in Arkansas, Connecticut, Delaware, Louisiana, Minnesota, New York, North Dakota and Texas can bring penalties against violators, using existing civil penalties. Illinois and New Jersey violations are subject to their states' fraud laws. In Montana, violations can be brought under either the Trade and Commerce Code or the Insurance Code. Georgia and Indiana did not specifically mention penalties in their laws while Nevada took a totally different approach. Their law allows "data collectors" to commence action and seek restitution against any individual that unlawfully obtains or benefits from personal information stolen from them.

Florida enacted the most elaborate penalty structure. Businesses that fail to send notices within 45 days of a security breach will be fined $1,000 a day for up to the first 30 days. Thereafter, the penalty increases to $50,000 for each 30-day period up to 180 days. Beyond that timeframe, businesses can be fined up to $500,000. The same penalties apply to an individual acting on behalf of the business entity if the entity is not notified within 10 days. State agencies are exempt from the penalties, but a contractor or third-party administrator working on behalf of a state agency is subject to them. The Department of Legal Affairs is responsible for assessing and collecting fines.

Implications for Insurers

Security breach notification bills have had the attention of state policymakers so far this year, and this trend is likely to continue in other states for the remainder of the year and into next year.

For the property/casualty industry, it will be important to ensure that new bill introductions do not negatively affect insurers with requirements that deviate in significant ways from the existing laws.

At least five provisions in some of the enacted security breach notification bills have the potential to make insurers more vulnerable and should be avoided in new bill introductions.

Personal Information. While most states follow California's definition for "personal information," Arkansas, Delaware, New Jersey and North Dakota added additional language to their definitions. These additions will make it more difficult for multi-state insurers to comply with such laws. For that reason, definitional expansions should be avoided in new bill introductions.

Notice Triggers. Most states follow California's disclosure trigger standard of "shall be made in the most expedient time possible and without unreasonable delay." However, Florida requires a 45-day disclosure deadline and requires businesses to maintain documentation for up to five years of possible breaches that were judged not likely to harm individuals. These requirements should be avoided in new bill introductions.

Further Notice Requirements. Florida, Georgia, Indiana, Minnesota, Nevada, New Jersey, New York, Tennessee and Texas require businesses to notify consumer-reporting agencies of security breaches, but the threshold which triggers the notice varies. Obviously, this lack of uniformity is problematic for multi-state insurers. Where new bill introductions are proposed, the notice threshold should be as high as possible to avoid further expense for insurers.

Notice Exemptions. Arkansas, Delaware, Louisiana, Minnesota, Nevada, North Dakota, Rhode Island and Tennessee have specific exemption language that goes beyond the California law which allows businesses to follow their own disclosure procedures if consistent with the law. To avoid against any misunderstanding as to whether insurers are subject to these notification laws, new bill introductions should include specific exemption language.

Penalties. States vary widely on penalties for violations of the notification laws with Arkansas, Connecticut, Delaware, Illinois, Louisiana, Minnesota, Montana, New Jersey, New York, North Dakota, and Texas following existing civil penalties or fraud laws. New bill introductions should avoid a private cause of action as allowed in Louisiana, Maine, Tennessee, Texas and Washington, or a sliding penalty structure as outlined in the Florida law.

Even if specific monetary penalties can be avoided, the consequences of the state laws that allow customers to bring civil actions are not yet fully known. In California, a class action lawsuit against ChoicePoint was filed one week after news of a security breach involving 145,000 individuals became public in February. The plaintiff is seeking damages under the state's unfair business practices and fraud and deceit statutes and is seeking to divide the suit into two parts, one for California residents and the other for individuals around the country affected by the breach.[18] At least one privacy advocate has characterized this lawsuit as "the tipping point that's needed to enable people to sue the entity that mishandled their information."[19]

Members of Congress also have been actively engaged in the identity theft debate. In 2003, Congress enacted the "Fair and Accurate Transactions Act of 2003" (FACTA),[20] which was motivated, in part, by the scheduled expiration of provisions of the Fair Credit Reporting Act. FACTA contains several provisions, including one that allows a consumer to place a "fraud alert" in their files with credit reporting agencies. This year, Congress has held two public hearings in the wake of the ChoicePoint breach, and Senator Diane Feinstein (D-Calif.), for one, already has introduced S. 115,[21] a bill that closely follows her state's security breach notification law, but includes monetary penalties of "not more than $5,000 per violation, to a maximum of $25,000 per day while such violations persist." The bill also contains language that would supersede state laws if enacted.

Conclusion

Security breach notification legislation is likely to remain a subject of great debate among state lawmakers and Congress for the foreseeable future, so new bill introductions should be monitored closely and certain provisions should be avoided to ensure that new notification laws do not impose unreasonable requirements that disrupt how insurers conduct their business affairs.

Endnotes

[1]This conclusion is reached in a Federal Bureau of Investigation publication entitled, "Financial Crimes Report to the Public May 2005."

[2]See"Federal Trade Commission – Identity Theft Survey Report" published in September 2003.

[3]See "2005 Identity Fraud Survey Report" produced by Javelin Strategy & Research on behalf of the Better Business Bureau, January 2005.

[4]See "National and State Trends in Fraud & Identity Theft," published by the Federal Trade Commission, February 2005.

[5]See Javelin study.

[6]Ibid.

[7]See "Identity Theft: The Aftermath 2003" published by the Identity Theft Resource Center, Summer 2003.

[8]See "A Chronology of Data Breaches Reported Since the ChoicePoint Incident," published by the Privacy Rights Clearinghouse.

[9]See "Personal Data for 3.9 Million Lost in Transit," New York Times, June 7, 2005 and "Customer Data Lost, Citigroup Unit Says," Washington Post, June 7, 2005.

[10]The National Conference of State Legislatures has charts showing what identity theft legislation has been enacted so far this year.

[11]California lawmakers actually enacted two similar bills in 2002 dealing with security breach notices. They were Assembly Bill 700, (Chapter 1054, Laws of 2002) Both were effective on July 1, 2003.

[12]The list of states to enact security breach laws so far in 2005 include:

Arkansas Senate Bill 1167 (Act 1526, Laws of 2005)
Connecticut, Senate Bill 650 (Public Act 05-148)
Delaware House Bill 116
Florida House Bill 481 (Chapter 229, Laws of 2005)
Georgia Senate Bill 230 (Act 163, Laws of 2005)
Indiana Senate Bill 503 (Act 503, Laws of 2005)
Louisiana Senate Bill 205
Maine Legislative Document 1671
(Chapter 379, Laws of 2005)
Minnesota House File 2121
(Chapter 167, Laws of 2005)
Montana House Bill 732
(Chapter 518, Laws of 2005)
Nevada Senate Bill 347 (Chapter 485, Laws of 2005)
New Jersey Assembly Bill 4001
New York Senate Bill 3492
North Dakota Senate Bill 2251
(Chapter 447, Laws of 2005)
Rhode Island House Bill 6191
Tennessee Senate Bill 2220
(Chapter 473, Laws of 2005)
Texas Senate Bill 122
Washington Senate Bill 5418
(Chapter 342, Laws of 2005)

[13]See "Computer Break-ins: Your Right to Know," Business Week Online, November 11, 2002.

[14]California Assembly Bill 700 (Chapter 1054, Laws of 2002) and Senate Bill 1386 (Chapter 915, Laws of 2002).

[15]This citation refers to the Electronic Signatures in Global and National Commerce Act.

[16]See "ChoicePoint Security Breach Will Lead To Increased Regulation," CSO: The Resource for Security Executives, March 3, 2005.

[17]The Arkansas legislation was introduced in the Senate on March 7 and passed that body on March 21. The House passed the bill on Mach 30 and the Governor signed the bill on April 4.

[18]See "ChoicePoint Security Breach Will Lead To Increased Regulation," CSO: The Resource for Security Executives, March 3, 2005.

[19]Ibid.

[20]See The Fair and Accurate Credit Transactions Act of 2003, P.L. No. 108-159 (2003) (FACTA).

[21]See S. 115, which was introduced by U.S. Senator Diane Feinstein (D-Calif.) on January 24, 2005.