WILMER CUTLER PICKERING
HALE AND DORR LLP

FINANCIAL INSTITUTIONS LAW UPDATE

April 19, 2005

Recent Developments in Data Security and Data Privacy

For the past several months, large data security breaches suffered by well-known companies and institutions have been splayed across the front pages of newspapers throughout the country stirring up public anxiety about the dangers of identity theft and creating a lawmaking frenzy on both the state and federal level. The list of companies announcing security breaches grows on a weekly basis and includes the full spectrum of institutions from data brokers (such as ChoicePoint and LexisNexis) to financial institutions (such as Bank of America and Household Bank) to retailers (such as DSW, Inc.) to universities and colleges (such as Boston College and Tufts University). Personal information about over 2 million individuals may have been compromised in these recent security breaches. In the wake of these highly publicized security breaches, a Washington Post-ABC News poll found that 84 percent of respondents said companies that collect and sell personal information are not doing enough to safeguard it.

Energized by the media coverage and public outcry, many state and federal lawmakers have pushed data privacy and security to the forefront of their agendas. Legislative proposals run the whole gamut from (1) requirements for customer notification of security breaches to (2) direct regulation of data brokers to (3) security freeze laws to (4) new data sharing restrictions to (5) restrictions on the use or sale of Social Security numbers.

- On the federal level, the Senate Judiciary Committee held a hearing last week, and Senate and House committees held hearings last month on data security and, in particular, how data brokers collect, handle and sell personal information and whether new federal laws or rules should be enacted to protect personal information. Republican and Democratic members of Congress alike have joined the fray, introducing over ten bills since the first of the year that directly address data security and privacy and promising many more such measures to come.
- Nearly two years after releasing their initial proposal, the Banking Agencies[1] have resurrected their long-dormant guidelines on security breach response programs, issuing Final Guidelines at the end of March and refusing to provide a delayed effective date or to grandfather or transition provisions for existing contracts with service providers.
- State lawmakers have been equally active. As of the end of March, there were over 100 bills under consideration in 31 states bearing directly on financial

1. The Banking Agencies include the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation and the Office of Thrift Supervision.

wilmerhale.com

Baltimore
Beijing
Berlin
Boston
Brussels
London
Munich
New York
Northern Virginia
Oxford
Waltham
Washington

"As of the end of March, there were over 100 bills under consideration in 31 states bearing directly on financial privacy or security."

privacy or security. In New York alone, the state legislature has 21 bills under consideration on topics ranging from data security/breach notification to opt-in requirements for data sharing.

This newsletter summarizes some of the current developments and issues in these areas.

I. Tell Me About It–Data Security Breach Notification

A. California–Leading the Pack

California's security breach notification law, the first in the country, has been credited by many for bringing to the public light the recent rash of data security incidents. That law, which became effective last year, applies to any person or business that conducts business in California and that owns or licenses computerized data that includes personal information.[2] While the California law states that it applies to persons or businesses that conduct business in California, it has been asserted that it may also apply to persons or businesses that merely maintain computerized data that includes personal information regarding California residents.

The California law requires disclosure of any security breach to California residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person following the financial institution's discovery or notification of the breach. Notice of the breach must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Generally, notice must be provided in writing or electronically (consistent with E-Sign), but in certain circumstances where the cost of providing notice or the number of notices exceed threshold levels, substitute notice–consisting of email, posting on the entity's Web site, *and* notification to major statewide media–is permitted. A private right of action for damages is provided for customers injured as a result of a violation of the law.

B. The Federal Banking Agencies–Awakened From a Slumber

Nearly two years after issuing proposed guidelines, the federal Banking Agencies have recently released final guidelines on response programs for data security breaches ("Response Program Guidelines" or "Guidelines"). The agencies released the final Guidelines as a supplement to the Security Guidelines issued on February 1, 2001.[3] Because the agencies contend that the Guidelines are a further elaboration of existing requirements, they declined to phase in the requirements and made them effective immediately. The agencies did recognize that not every financial institution will have a response program currently in place that meets the requirements of the final Guidelines but stated that they expect all financial institutions to implement the final Guidelines as soon as possible. In the meantime, the agencies "will take into account the good faith efforts made by each institution to develop a response program that is consistent with the final [Guidelines], together with

2. Under the California law, "Personal Information" is defined as "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social Security number. (2) Driver's license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." It does not include publicly available information that is lawfully made available to the general public from government records.

3. The scope of the Response Program Guidelines and definition of terms are identical to those in §501(b) of the Gramm-Leach-Bliley Act and the Security Guidelines.

all other relevant circumstances, when examining the adequacy of any institution's information security program."

Under the Response Program Guidelines, a financial institution must develop and implement a response program to address incidents of unauthorized access to, or use of, customer information maintained by the institution or its service provider[4] that could result in substantial harm or inconvenience to a customer. The key difference from the original proposal to the final Guidelines is a shift away from rigid requirements toward more flexibility in allowing an institution to design a response program according to its size, complexity and the nature of its operations. In addition, unlike the proposed guidelines, the final Guidelines limit an institution's obligation for notifying regulators and/or customers to breaches involving "sensitive customer information" in an attempt to balance the competing interests, on the one hand, of protecting the types of information most likely to be misused by identity thieves and, on the other hand, of minimizing the notification burden on industry and the dulling effect that receiving a multitude of notices would have on regulators and consumers.

"Sensitive customer information" is defined as "a customer's name, address or telephone number, in conjunction with the customer's Social Security number, driver's license, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account" and it "also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number." It is important to note that this definition is broader than its counterpart under the California law in several important respects:

- The Response Program Guidelines do not contain a blanket exclusion for encrypted information on the grounds that not all levels of encryption effectively protect customer information. Of course, stronger levels of encryption will make it less likely that an institution will be required to notify customers of a security breach by making it less likely that misuse of sensitive customer information has occurred or is "reasonably possible."
- The Response Program Guidelines do not require the information at issue to include the customer's *name* in combination with other data elements in order for it to constitute "sensitive customer information." Instead, the Guidelines treat the customer's address and phone number in the same manner as his or her name because of the potential for deriving a customer's name from that information.
- The Response Program Guidelines do not limit "sensitive customer information" to personal information that includes a security code, access code or password that would permit access to an individual's financial account. Instead, the agencies noted that a customer's name and account number alone may be sufficient to access a person's account by, for example, creating fraudulent checks.
- The Response Program Guidelines are not limited to security breaches involving *computerized* data.

Although emphasizing an institution's flexibility to adapt a response program to its particular needs, the Response Program Guidelines set forth minimum

"Because the Banking Agencies' Response Program Guidelines became effective immediately, financial institutions should review their data security programs as soon as possible to ensure that they include response programs that comply with the Guidelines."

4. Although the Guidelines do not apply directly to a financial institution's foreign offices, branches, or affiliates, a financial institution is nevertheless responsible for the security of its "customer information," as that term is defined by the Response Program Guidelines, whether that information is maintained within or outside of the United States (e.g., by a service provider located outside of the United States).

requirements that should be included in such a program. Under these provisions, a financial institution's response program should contain procedures for:

1. **Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused.** The risk assessment should *not* be limited to unauthorized access to sensitive information but rather should allow the financial institution to establish the nature of *any* information improperly accessed.

2. **Notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information.** This requirement is unique to the federal Guidelines and does not have a counterpart in the California breach notification law. The financial institution must notify its regulator at the time the institution initiates its investigation to determine the likelihood that the information has been or will be misused, so that the regulator will be able to take appropriate action, if necessary. However, the agencies declined to create a formal SAR-like process for notification, contemplating instead that institutions will notify regulators "as quickly as possible, by telephone, or in some other expeditious manner."

3. **Notifying appropriate federal law enforcement authorities,** in addition to filing a timely SAR in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing.

4. **Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of information,** for example, by monitoring, freezing or closing affected accounts, while preserving records and other evidence.

5. **Notifying affected customers[5] when the financial institution determines that *misuse* of sensitive customer information has occurred or is "reasonably possible."** This standard is narrower than the standard under the California law, which requires customer notification in the event of the "unauthorized acquisition" of computerized data that compromises the security, confidentiality or integrity of personal information. Presumably, there could be circumstances where a security incident involves unauthorized acquisition of customer information that triggers the California law but that would not trigger the Response Program Guidelines customer notification requirement because, despite the unauthorized acquisition of information, the financial institution determines that misuse has not occurred or is not "reasonably possible." Faced with this discrepancy, financial institutions that conduct business on a nationwide or regional level can decide to maintain two separate notification standards–one for customer information about California residents and one for customer information about their other customers–or, if they determine that the cost, burden, or risk of maintaining and defending separate notification standards is too high, they can choose voluntarily to follow the more stringent California notification standards for all of their customer information.

5. If the financial institution can determine precisely which customers' information has been misused or is reasonably possible to be misused, it may limit notification of the security incident to those customers. However, if it determines that a group of files has been accessed improperly but is unable to identify which specific customers' information has been accessed, it must notify all of the customers in the group if it determines that misuse of the information contained in the group of files has occurred or is reasonably possible.

Notification under the Guidelines should be provided "as soon as possible" after the financial institution concludes that misuse of a customer's information has occurred or is reasonably possible.[6] However, notification may be delayed when an appropriate law enforcement agency determines that it will interfere with a criminal investigation and provides the institution with a written request for the delay. In a footnote, the Banking Agencies state that this includes circumstances where a financial institution confirms that an oral request for delay from law enforcement will be followed by a written request. Where notice is delayed due to the request of a law enforcement agency, a financial institution should maintain contact with the agency to determine when customer notice will no longer interfere with the investigation and should notify its customers as soon as such a determination is made.

Customer notice must be provided in a clear and conspicuous manner. The agencies set forth certain provisions that all customer notices should include and certain recommended provisions that should be included "when appropriate."

All customer notices should include:

- A description of the incident in general terms and the customer's information that was the subject of unauthorized access or use;
- A telephone number that customers can call for further information and assistance (note that the financial institution should ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to customer inquiries or requests for assistance);
- A reminder of the need to remain vigilant over the next 12 to 24 months;
- A recommendation to promptly report incidents of suspected identity theft; and
- A general description of what the institution has done to protect the customer's information from further unauthorized access.

Customer notices should also include the following *when appropriate:*

- A recommendation that customers review account statements and immediately report any suspicious activity to the institution;
- A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports;[7]
- A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;
- An explanation of how the customer may obtain a credit report free of charge;
- Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft and information about, and encouragement to use, the FTC's website

6. When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, it should conduct a reasonable investigation to determine promptly the likelihood that the information has been or will be misused. A full-scale investigation may not be required in all cases, however, a financial institution cannot forego an investigation to avoid a conclusion of the likelihood of misuse and cannot unreasonably limit the scope of the investigation.

7. The agencies declined to shift costs that may be incurred by credit reporting agencies from increases in customer inquiries, requests for copies of credit reports, or requests for fraud alerts that may occur following notification by a financial institution of a security incident. However, the Response Program Guidelines do encourage a financial institution that includes in its customer notice contact information for nationwide credit reporting agencies to notify the credit reporting agency prior to sending out large numbers of notices.

or toll-free telephone number to report any incidents of identity theft or to obtain the FTC identity theft guidance.

Customer notices should be "delivered in any manner that is designed to ensure that a customer can reasonably be expected to receive it." Non-exhaustive examples in the Guidelines of possible delivery methods include telephone, mail and email (for customers for whom the financial institution has valid email addresses and who have agreed to receive electronic communications from the financial institution). Unlike the California law, the federal Guidelines do not contain specific provisions regarding substitute notice (such as posting notice on the web or through the media). However, this does not mean that use of such delivery methods automatically renders an institution noncompliant. Rather, if the institution can make a persuasive argument that the delivery is "designed to ensure a customer can reasonably be expected to receive it" then it presumably should be in compliance with the regulations regardless of the exact mechanics or delivery method of notification. This would seem to give institutions more latitude than the California law which limits substitute notice to situations involving threshold cost levels for notification or numbers of notices required.

If a security incident involves an unauthorized intrusion into systems maintained by a service provider, the financial institution is still responsible for all notification requirements that may arise–including notice to regulators[8] and customers. However, it may contract with the service provider to require the service provider to give the actual notice. (Note, however, that if the service provider fails to provide notice that meets the requirements of the Guidelines, the financial institution will be responsible for the noncompliance.) In addition, it can contractually shift the costs of having to provide notice to the service provider, for example, where the notification requirement is triggered by negligence on the part of the service provider.

The Banking Agencies declined to determine the extent to which the Guidelines may preempt state law, finding the issue outside the scope of the Guidelines. They also declined to adopt a safe harbor such as one that would protect from liability any financial institution that takes reasonable steps that regulators require to protect information, but, nonetheless, experiences an event beyond its control that leads to the disclosure of customer information. They did clarify, however, that the breach notification requirement applies only to information within the control of the financial institution and its service providers and would not apply to information directly disclosed by a customer to a third party such as through phishing.

C. Federal Legislative Proposals

There are a number of data security breach notification bills under consideration on the federal and state level. On the federal level, Senator Feinstein, who has been extremely active in the areas of privacy and data security, has introduced two bills–S. 115 (the Notification of Risk to Personal Data Act) introduced in January and S. 751, a follow-up bill introduced last week as a tougher version of S. 115.

S. 115 would create a generally-applicable national requirement for breach notification. Not surprisingly, since Senator Feinstein represents California, the federal bill largely mirrors the California law. Like California's law, S. 115 would require notification as expediently as possible and

*8. Even if the security incident involves an unauthorized intrusion into systems maintained by the service provider, and not the financial institution, the financial institution's **own** primary regulator must still be notified and not merely the regulator of the service provider.*

without unreasonable delay to any resident whose unencrypted personal information "was, or is reasonably believed to have been, acquired by an unauthorized person."

Even if passed, however, S. 115's impact on financial institutions would be limited by a safe harbor provision that deems certain entities, such as financial institutions, to be in compliance if they maintain their own reasonable notification procedures as part of an information security policy, and they send out notifications in accordance with that policy in the event of a security breach. In order to qualify for this safe harbor, however, an institution would also be required to: (1) use a security program reasonably designed to block unauthorized transactions before they are charged to the customer's account; (2) provide for notice to be given by the owner or licensee of the database (directly or through a person acting on its behalf) after the security program indicates that a security breach has resulted in fraud or unauthorized transactions, but does not necessarily require notice in other circumstances; and (3) be subject to examination for compliance with the requirements of the Act by one or more federal functional regulators with respect to the operation of the security program and the notification procedures.

S. 115 would also preempt any inconsistent provisions of state or local law regarding notification of any breach of security of an electronic database containing personal information, except as provided by certain provisions of the California Civil Code. The bill has been referred to the Committee on the Judiciary.

Last week, Senator Feinstein introduced S. 751, a follow-up data security breach notification bill that generally tracks her earlier bill but tightens up several restrictions and requirements. Like S. 115 and the California breach notification law, S. 751 contains a broader notification trigger than the Banking Agency Guidelines, requiring customer notification upon the mere unauthorized acquisition (or reasonable belief of unauthorized acquisition) of personal information.[9] It also contains some significant changes from the earlier bill, S. 115, including:

- Broadening the definition of "personal information" to include encrypted information and to include account numbers and credit and debit card numbers absent security or access codes or passwords where access to the individual's account is possible even without such codes or passwords. This change is consistent with the Banking Agency Guidelines' definition of "sensitive customer information."
- Increasing the cost threshold for authorizing substitute notice[10] and altering the required delivery methods for substitute notice. S. 751 eliminates email as a delivery method for substitute notice and, instead, requires substitute notice to be provided by *both* conspicuously posting notice on the entity's public Internet site *and* notifying major media.[11] Unlike S. 115, S. 751 specifically requires notification to both print and broadcast

9. S. 751 requires notice to be given to "any individual of the United States" whereas S. 115 requires notice to be given to "any resident of the United States." Presumably, this change in drafting is intended to broaden the class of individuals to whom notice must be sent, perhaps including such groups as non-resident US citizens.

10. S. 115 permits substitute notice if: (i) the agency or person demonstrates that the cost of providing direct notice would exceed $250,000; (ii) the affected class of subject persons to be notified exceeds 500,000; or (iii) the agency or person does not have sufficient contact information for those to be notified. In contrast, S. 751 raises the cost threshold to $500,000 but retains the class size threshold and the provision for insufficient contact information.

*11. Unlike the California law (and S. 751), S. 115 permits an entity to provide substitute notice through email notice, conspicuous posting on the entity's public Internet site, **or** notification to major media.*

"State laws could be much more rigorous than the federal Response Program Guidelines."

media, including major media in metropolitan and rural areas where the individual whose personal information was, or is reasonably believed to have been, acquired resides. In addition, media notice must include a toll-free telephone number where an individual can learn whether or not his or her personal data was included in the security breach.

- Expressly setting forth required contents for customer notice, including the provision of a toll-free number that an individual may call to contact the entity and learn what types of information the entity maintains about him or her or about individuals in general and whether or not the entity maintained information about him or her.
- Eliminating the safe harbor permitting compliance through alternative self-imposed notification procedures that is found both in the California breach notification law and S. 115.
- Placing the burden of proof of notice on the entity required to provide notice.
- Providing for higher civil penalties. S. 751 provides for $1,000 per individual a financial institution failed to notify, to a maximum of $50,000 per day while the failure to notify persists; S. 115 provides penalties of not more than $5,000 per violation, to a maximum of $25,000 per day while violations persist.

As a result of these changes, S. 751 could impose additional, more rigorous notification requirements than those currently applicable to financial institutions under the Banking Agency Guidelines.

D. State Legislative Proposals

On the state level, bills have been introduced in 23 states–including New York, New Jersey, Pennsylvania, Texas and Illinois–that would require companies to notify customers whenever sensitive data has been lost or stolen. While generally patterned after the California notification law, many of these bills contain substantive differences that could create a compliance thicket for companies that operate on a nationwide level. For example, in New York State, there are at least seven notification bills currently under consideration in the state legislature. The bills differ from each other in material respects; a small sample of those differences include:

- The timing for notification (e.g., provisions requiring notice "in the most expedient manner possible and without unreasonable delay"; "within seven business days from the date the entity discovers and confirms that a breach of security of the system has occurred"; or "as soon as practicable");
- The method of delivery of notice (e.g., provisions requiring various combinations of delivery methods such as requiring written notice unless certain conditions are met in which case permitting substitute notice by email, posting on the entity's website, *and* notice to major statewide media; permitting the choice between written notice and email notice; requiring a combination of delivery methods in the first instance; or permitting entities more latitude in determining delivery methods); and
- Remedies (e.g., provisions granting or declining to grant private rights of action for actual or statutory damages or permitting class actions).

The Bottom Line

Because the Banking Agencies' Response Program Guidelines became effective immediately, financial institutions should review their data security programs as soon as possible to ensure that they include response programs that comply with the Guidelines. As part of that review, financial institutions should consider provisions requiring service providers to send any necessary notices (to customers and/or to the financial institution's primary regulator) for breaches of security on systems maintained by the service providers and, where possible, shifting costs for

notification to the service provider where the breach was a result of the service provider's negligence.

With respect to the current federal legislative proposals, it is impossible to tell which, if any, of the bills will be enacted. A proposal introduced by Senator Feinstein and similar to S. 115 failed last year. However, the regulatory momentum may be shifting with the recent rash of security breaches, and it is possible that one of her latest notification bills, or some other not yet introduced bill, could be pushed through Congress. If such a bill contained a safe harbor provision for financial institutions that comply with the Banking Agencies' Response Program Guidelines (like S. 115), the direct impact on financial institutions could be minimal. However, even legislation containing a safe harbor could have a significant indirect impact on financial institutions by applying to their joint marketing partners, affiliates, private label or affinity partners, or other non-financial institutions with which they share information.

On the state level, it seems likely that at least some states will pass breach notification bills. The result would be a hodge-podge of requirements for financial institutions that operate on a national, or even regional, level. In addition, state laws could be much more rigorous than the federal Response Program Guidelines. For example, they could contain hair triggers that would require notification at the slightest security breach; they could require notification through more costly delivery methods or could require a combination of delivery methods; and they could permit private rights of action and/or class actions. For these reasons, the passage of a federal law that preempts state or local laws governing breach notification could be advantageous for financial institutions. This would be especially true if such a federal law was no more rigorous than the federal Banking Agency Response Program Guidelines or included a safe harbor for compliance with the Guidelines.

II. What to Do With Data Brokers?

Both the House and Senate, driven by the security breaches at ChoicePoint and LexisNexis, conducted hearings last month regarding the regulation of data brokers (or current lack thereof). FTC Chairperson Deborah Majoras testified at the hearings, describing the role that data brokers play, the information they collect, and the various laws generally governing data collection and security. Before and after the hearings, a number of members of Congress have indicated intentions to introduce legislation aimed at regulating data brokers.

Currently, however, only one bill has been introduced at the federal level directly dealing with data brokers. That bill, the Information Protection and Security Act (S. 500, H.R. 1080), directs the FTC to promulgate regulations governing the conduct of information brokers and the protection of personally identifiable information held by such brokers. Under the bill, such regulations would be required to include rules: (1) requiring procedures for maximum data accuracy, confidentiality, user authentication and tracking, the prevention and detection of illegal or unauthorized activity, and mitigation of potential harm to individuals; (2) allowing individuals to obtain disclosure of information about them held by an information broker, to be informed of each entity that procures their personal information, and to request and receive prompt correction of errors; and (3) prohibiting brokers from engaging in any activity that fails to comply with FTC regulations. The bill also would authorize states (after providing notice to the FTC and the Attorney General) to bring civil actions for injunctive relief, damages, restitution or other relief on behalf of state residents in federal district court, and it would establish a private right of action. The bill is currently before the Senate Committee on Commerce, Science and

"If Congress (or the FTC) draws the net too broadly, it could restrict financial institutions' access to personal information used to authenticate customers, prevent fraud, evaluate credit risks, or market products and services."

"Currently, about twenty additional states, including New York, are considering enacting their own security freeze bills."

Transportation and the House Committee on Energy and Commerce.

The Bottom Line

Some form of law or regulation may be enacted at the federal level to ensure that data brokers are expressly covered by privacy and data security laws or regulations. Following her congressional testimony, FTC Chairperson Majoras has been quoted in the press as saying "We may have some gaps in the law and there may be some need for legislation." Her sentiments have been echoed by a number of lawmakers and consumer organizations. What such legislation might look like, however, is far from clear. Despite the pronouncements of various members of Congress of their intention to draft legislation to address data brokers, only one bill has been introduced thus far and that bill provides no clear idea on the nuts and bolts of regulation, instead assigning that task to the FTC.

The danger lurking in this uncertainty is that overbroad legislation could result that would impede access to personal information held by data brokers for legitimate purposes. If Congress (or the FTC) draws the net too broadly, it could restrict financial institutions' access to personal information used to authenticate customers, prevent fraud, evaluate credit risks, or market products and services.

Even absent legislation, the major data brokers may cut back on access to personal information such as Social Security numbers in an attempt to diffuse legislative alarm over the security of personal information. For example, last month, Westlaw announced that it would curb access to Social Security numbers. In a news conference, Senator Schumer illustrated how easy it was to obtain Social Security numbers by using a service provided by Westlaw to obtain the Social Security numbers of Vice President Cheney and Paris Hilton. As a result, Westlaw, which is not among the companies recently suffering security breaches, quickly announced that it would no longer permit its corporate clients to have access to Social Security numbers, and it would limit government offices other than law enforcement agencies to partial numbers. Such self-imposed restrictions are likely to grow as the data broker industry attempts to avert the enactment of an overly restrictive data broker law.

III. Security Freezes

Security freeze laws permit a consumer, for a fee, to freeze access to his or her credit report and credit score. Generally, the consumer can temporarily lift the freeze to permit access to a particular creditor or to permit access generally for a specified period. Such laws also provide certain exceptions to the freeze, permitting access, for example, to existing creditors or to law enforcement agencies.

As of the end of last month, four states–California, Louisiana, Texas and Vermont–have enacted security freeze laws. California and Louisiana permit anyone to freeze their credit report whereas Texas and Vermont limit freezes to victims of identity theft. Currently, about twenty additional states, including New York, are considering enacting their own security freeze bills.

The Bottom Line

It appears likely that the number of state security freeze laws may increase in the coming months. The problem for financial institutions is that such freezes add a layer of complexity and can impede the development of consumer credit relationships. They can delay credit applications and decisions regarding the extension of credit and can frustrate a financial institution's attempts to market its financial products and services to the detriment of both the financial industry and consumers alike.

Federal preemption is possible, although less likely under current federal law. States and consumer advocates claim that security freeze laws are not preempted by current

law because they do not regulate the content of credit files, but rather who can access them. A counter argument can be made that the laws relate to information contained in consumer reports and are therefore preempted by the Fair Credit Reporting Act, as amended by the Fair and Accurate Credit Transactions Act of 2003. However, it is unclear whether such an argument would be successful.

IV. Privacy Revisited

A. Privacy Notices–In or Out?

On the privacy side, the debate continues over what paradigm should control the sharing of personal information among entities. Federal law currently provides that financial institutions are permitted to share personal information with nonaffiliated third parties–under the Gramm Leach Bliley Act (GLBA)–and affiliated third parties–under the Fair Credit Reporting Act (FCRA)–as long as they provide consumers with notice and an opportunity to opt-out prior to sharing the information and the consumers do not opt-out of disclosure. Under the FCRA, however, a financial institution need not provide notice and an opportunity to opt-out before sharing information with its affiliates if the information is limited to the financial institution's transactions or experiences with the consumer.

Several states have enacted tougher privacy restrictions than those provided under federal law. California, Vermont, New Mexico and North Dakota forbid entities from sharing personal information with third parties unless a consumer affirmatively "opts-in" (affirmatively consents) to the disclosure. The GLBA expressly permits states to adopt tougher privacy laws governing the sharing of personal information with *nonaffiliated* entities. However, there is uncertainty about whether the FCRA permits similar state laws with respect to sharing personal information with *affiliated* entities. The American Bankers Association and others filed suit challenging the California data sharing statute's limitations on sharing personal information with affiliated entities. In that suit, *ABA v. Lockyer*, the ABA claimed that California's limitations on data sharing with affiliates were preempted by the FCRA. The federal district court upheld the California law, and the ABA appealed. The federal Banking Agencies and the FTC filed a brief supporting the ABA's position. The Ninth Circuit heard oral argument last fall, and a decision could be issued any day.

In January, Senator Feinstein introduced the Privacy Act of 2005 (S. 116) that, in part, would amend the GLBA to require businesses to obtain the consent of an individual prior to the sale or marketing of personally identifiable information to nonaffiliated entities. The bill would also require financial institutions to permit consumers the opportunity to opt-out of information sharing under a joint agreement between financial institutions; under the current GLBA, such sharing is exempt from the opt-out requirement. Although it would permit financial institutions to offer incentives to consumers to encourage consent, the bill would prohibit financial institutions from denying a consumer a financial product or service as a result of the consumer's refusal to consent to disclosure. Similar bills are being considered in a number of states including Connecticut, Missouri and New Jersey.

B. Preemption of State Law

Congress is considering a number of other privacy bills as well. Of particular interest is a bill sponsored by Congressman Stearns that would apply privacy and data security provisions beyond the financial arena to "data collection organizations" defined broadly as entities that collect, sell, disclose for consideration or use personally identifiable information of a consumer. The bill contains a safe harbor provision that would deem compliance with another applicable federal privacy law–such as the GLBA–to constitute compliance with the bill, and it expressly states that such existing laws are not modified, limited or superseded by its provisions. The

"On the privacy side, the debate continues over which paradigm should control the sharing of personal information among entities."

"The big question regarding state bills will be preemption–especially with regard to limitations on sharing data with affiliates."

interest in the bill, therefore, lies not in the substantive obligations imposed but rather in its broad preemption provision which states:

> This title preempts *any* statutory law, common law, rule or regulation of a State, or a political subdivision of a State, to the extent such law, rule, or regulation *relates to or affects the collection, use, sale, disclosure, retention or dissemination of personally identifiable information* in commerce (emphasis added). No State, or political subdivision of a State, may take any action to enforce this title.

This broad provision could be read to preempt existing and proposed state laws on data sharing and data security.

The Bottom Line

Although prior attempts in Congress to introduce opt-in laws have failed, there is no way to be certain about what will happen this year given the media's focus on recent security breaches. One thing that is extremely likely, however, is that additional states will join the "opt-in" ranks. The big question regarding state bills will be preemption–especially with regard to limitations on sharing data with affiliates. The Ninth Circuit could provide an answer to that question any day in its ruling on *ABA v. Lockyer*. If the Ninth Circuit affirms the lower court's ruling and upholds the California law, many more states may pick up the mantle and pursue legislation limiting affiliate sharing.

V. Social Security or Insecurity

Finally, there have been a number of bills introduced in 2005 that would limit the use and disclosure of Social Security numbers.[12] Some proposals (such as S. 29 and S. 116) would amend the federal criminal code to prohibit the display, sale or purchase of Social Security numbers without the affirmative consent of an individual. Others would amend the civil code in various ways:

- The Privacy Act of 2005 (S.116) would prohibit the sale and disclosure of personally identifiable information by a commercial entity to a non-affiliated third party unless specific procedures for notice and opportunity to opt-out are followed and would prohibit a commercial entity from requiring disclosure of an individual's Social Security number in order to obtain goods or services.
- The Social Security Number Protection Act (HR 1078) would prohibit any person from selling or purchasing a Social Security number or Social Security account number in a manner that violates FTC regulations and would direct the FTC to promulgate regulations imposing restrictions and conditions on the sale and purchase of Social Security numbers that are no broader than necessary to provide reasonable assurance that Social Security numbers and Social Security account numbers will not be used to commit or facilitate fraud, deception or crime and to prevent an undue risk of bodily, emotional or financial harm to individuals.
- The Social Security On-Line Privacy Protection Act (HR 82) would prohibit interactive computer services from disclosing to third parties an individual's Social Security number or related personally identifiable information without the individual's prior informed written consent.

The Bottom Line

Financial institutions will likely find it increasingly difficult to obtain and to use Social Security numbers, especially for marketing purposes. Given public pressure and the current momentum of privacy

12. A number of states—including California, Texas and New York—have already enacted laws limiting the use or disclosure of Social Security numbers.

advocates, some form of federal limitation on the use and sale of Social Security numbers may result. Even absent legislative action, however, data brokers may follow Westlaw's lead and take the initiative to limit non-governmental clients' access to Social Security numbers.

VI. The Final Word

For financial institutions, regulation of data security and data privacy is a moving target. Faced with the media and public backlash following the string of recent security incidents, federal and state lawmakers alike are pressing data security and privacy agendas. While it currently is not possible to tell which laws will pass and which laws will not, it seems fairly certain that the coming year will bring a new crop of data security and privacy regulation. With this in mind, it is critical that the financial industry, and other industries that rely upon personal data, keep a close eye on these developments and make certain that the concerns of privacy advocates are appropriately balanced by consideration of the legitimate needs of business.

If you have any questions or need additional information, please contact:

Washington:

David Medine
+1 (202) 663 6220
david.medine@wilmerhale.com

J. Beckwith Burr
+1 (202) 663 6695
beckwith.burr@wilmerhale.com

Franca Harris Gutierrez
+1 (202) 663 6557
franca.gutierrez@wilmerhale.com

Helen G. Foster
+1 (202) 663 6892
helen.foster@wilmerhale.com

Natacha D. Steimer
+1 (202) 663 6534
natacha.steimer@wilmerhale.com

New York City:

Michael A. Ross
+1 (212) 230-8858
michael.ross@wilmerhale.com