Trends in data security: Business risk and legal exposure

By Richard M. Alexander and Ronald D. Lee, Arnold & Porter LLP

Data security is much on the minds of global bankers and their customers as a result of highly-publicised incidents in which personal information was compromised. This article defines data security, and highlights the reputational risks financial institutions incur when they do not maintain data security. We then touch on recent data security initiatives by the United States' financial regulators and the Federal Trade Commission, and on state laws (exemplified by California) requiring notification of security breaches. The article concludes with a brief summary of the regulatory requirements for an information security programme and practical suggestions for managing data security risks.

There has been considerable publicity recently regarding the loss or compromise of confidential personal information by financial institutions and other service providers. Regardless of the immediate cause of the breach or where the fault lies, these episodes bring intense and sudden reputational and financial risk to the financial institution and loss of customer confidence. They also draw the scrutiny of regulators, legislators, and the financial markets.

While there is no sure means to defeat the ingenuity of criminal hackers, or to prevent human error, a comprehensive programme for assuring an institution's data security (also known as information security) rests on a shared corporate understanding of the importance of protecting data. Such a programme also must comply with US federal and state legal requirements and enforcement priorities while anticipating future regulatory developments. Finally, it must include careful advance planning to respond to a breach of data security if and when one ever were to occur.

THE CRITICAL IMPORTANCE OF DATA SECURITY

One of the best ways to foster a shared commitment to a robust information security programme throughout an organisation is to assure that each director, officer, employee, and vendor fully endorses the concept of data security and its paramount business importance. Data security may be defined as assuring the confidentiality, authentication, integrity, and availability of data in its entire lifecycle of collection, storage, processing, transmission, use, and destruction.

Confidentiality signifies that only those authorised to access the data can in fact retrieve and use the data; authentication signifies that the stated originator or signer of the data is in fact the person who originated or signed the data; integrity means that the data have not been altered, damaged, or destroyed; and availability of course implies that the information technology systems handling the data function to make the data available as needed. While some regulatory regimes, as discussed below, apply to a subset of data - generally, personal information about "customers" - in practice all of a company's business data needs to be part of a well-managed and integrated data security programme.

Data security obviously is of critical importance to any financial institution. Confidential financial information is the lifeblood of the banking business, and the value that the bank is able to generate for its customers and its shareholders is directly related to its ability to process data confidentially, accurately, and efficiently. Moreover, because the financial data that individuals and enterprises entrust to banks are highly sensitive and valuable, assuring the security of these data is a core customer trust and relationship issue. Conversely, breaches or potential compromises of data security – and any failure forthrightly and comprehensively to respond – can quickly undermine or destroy that trust.

The Gramm-Leach-Bliley law and its implementing regulations place the ultimate responsibility for establishing and overseeing an information security programme squarely on the shoulders of the financial institution's Board of Directors; thus, the development and implementation of a comprehensive data security programme should be viewed as a core corporate governance responsibility.

In addition, a failure of data security can lead to potential regulatory sanctions and exposure to civil liability to those who claim they were damaged by the data breaches. For all of these reasons, how a bank protects data security – and how it responds to

an actual or potential breach of that security – involves several dimensions of reputational risk.

THE REGULATORY LANDSCAPE: THE CONTOURS OF AN INFORMATION SECURITY PROGRAMME CIRCA 2005

Both the functional regulators and the Federal Trade Commission (FTC) have been active in efforts to require financial institutions to enhance data security. In addition, California and a number of other states have recently enacted laws requiring notification of consumers when a breach of security results in a compromise or potential compromise of their personal information. This section briefly describes the agencies' and California's recent initiatives on data security issues and then outlines the requisite components of an information security programme for a financial institution (or other company) that is subject to the jurisdiction of either the functional regulators or the FTC.

Agencies. Section 501(b) of the Gramm Leach Bliley Act required the federal banking agencies to establish standards to ensure the security and confidentiality of consumer information, protect against any anticipated threats and protect against any unauthorised access to or use of such information. The agencies have issued guidelines and guidance addressing these statutory requirements.

Agency guidance requires a financial institution to conduct a risk assessment of its operations in developing its information security programme and to design a programme specifically tailored to address those risks. The agencies have established minimum standards for all such programmes, including the need to implement access controls on customer information systems and perform background checks for employees with responsibilities for access to customer information.

In addition, the guidance directs that a financial institution develop and implement a response programme designed to address incidents of unauthorised access to information maintained by an institution or its service provider. Such a programme must include procedures for:

- assessing the nature and scope of the incident, and identifying what customer information systems and types of customer information have been accessed or misused;
- notifying regulators when a security breach involves access to so-called "sensitive customer information" - generally, a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's licence number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account;
- notifying appropriate law enforcement agencies; and
- notifying customers when warranted.

The customer notification requirement is one of the most controversial and complex components of the applicable regulatory regime. The agencies have provided subjective guidance – but not specific objective standards – governing the circumstances when notice should be provided to customers, the group of customers who should receive notice and the contents of such notice. Under agency guidance, a substantial burden is placed on the affected institution in deciding whether, when and to whom notice should be provided.

Federal Trade Commission. The Federal Trade Commission (FTC or Commission) has become increasingly aggressive in its enforcement policy relating to the protection of sensitive customer data. In June 2005, the Commission announced that BJ's Wholesale Club, Inc. (BJ's) had agreed to settle charges that "its failure to take appropriate security measures to protect the sensitive information of thousands of its customers was an unfair practice" that violated Section 5 of the FTC Act.

BJ's operates warehouse clubs, whose member-customers typically use credit cards or debit cards to make purchases. Hackers had accessed more than 40,000 customer names along with associated credit or debit card information and other personal data that had been stored on BJ's computer system in unencrypted form, on in-store computers that were accessible using default user ID's and passwords and equipped with unsecured wireless access points. The Commission alleged that BJ's had failed to employ reasonable and appropriate measures to secure personal information it had collected.

According to the FTC, this failure was an "unfair practice" because it caused or was likely to cause substantial injury that was not reasonably avoidable and was not outweighed by countervailing benefits to consumers or competition. As part of the consent agreement settling the case, and without admitting wrongdoing, BJ's agreed to establish, implement, and maintain a comprehensive information security programme "reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."

Despite variations, there are considerable similarities in the requirements for an information security programme under both the GLB Safeguards Rule and under the FTC's consent agreement with BJ's. These requirements suggest best practices and therefore form a useful reference point for a financial institution's ongoing efforts to

assure data security; even if the company is not specifically subject to the jurisdiction of either the functional regulators or the FTC. In brief, a comprehensive information security programme includes:

- designation of an employee to coordinate and be accountable for the information security programme;
- identification of material risks to the security, confidentiality, and integrity of personal information that could result in the unauthorised disclosure, misuse, loss, or destruction of such information, and assessment of the sufficiency of any safeguards in place to control such risks. This risk assessment should include employee training and management; information systems; and prevention, detection, and response to attacks, intrusions, or other systems failures; and
- design and implementation of reasonable safeguards to control identified risks, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

State laws requiring notification of data security breaches. Several states have recently enacted laws requiring a company to notify affected individuals when the company suffers a security breach leading to actual or potential disclosure of the personal information of those individuals. While the data to which the statute applies and the precise definition of an event triggering the duty of customer notification vary among these state laws, we briefly discuss the California statute because, as in some other consumer protection areas, California was the first state to enact a law on this subject and because of the broad applicability and commercial significance of the California statute.[1]

The California law, which became effective on July 1, 2003, requires that any business in California that owns or licenses computerised data that include "personal information" shall disclose "any breach of the security of the system" following discovery or notification of the breach to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorised person. The statute defines "personal information" to mean an individual's first name or first initial and last name in combination with one or more of the following data elements (when either the name or the data elements are not

encrypted): (i) Social Security Number; (ii) driver's licence number or California ID card number; and (iii) account number, debit, or credit card number, in combination with any required security code, access code, or password that would enable access to an individual's financial account. In addition, "breach of the security of the system" is defined as unauthorised acquisition of computerised data that compromises the security, confidentiality or integrity of personal information.

Comparison of Interagency Guidelines and California standards for notification. The Interagency Guidelines do not by their terms preempt state law requirements for notifying customers when their personal information has been or may have been compromised. Therefore, the facts of each incident involving a potential breach of data security require analysis under both the Guidelines and the applicable state law or laws.[2]

As noted above, the Interagency Guidelines apply only to "customer information" where the definition of "customer" is provided by the GLB Safeguards Rule; thus, the Guidelines may not apply to certain categories of personal information held by a bank to which the California statute (or another state statute) does apply.

The Guidelines require a financial institution that becomes aware of an incident of unauthorised access to "sensitive customer information" to determine the likelihood of misuse of the information; if such misuse has occurred or is reasonably possible, the institution should notify the affected customer as soon as possible. The Guidelines define "sensitive customer information" as a customer's name, address, or telephone number, together with the customer's Social Security Number, driver's licence number, account number, credit or debit card number, or a personal identification number or password allowing access to a customer's account.

The Guidelines' notification provision - misuse or the reasonable possibility of misuse - arguably imposes a higher threshold showing before notification must be made than does the California law, which requires disclosure even if personal information is only "reasonably believed to have been acquired" by an unauthorised person compromising the security of the data.

Two other differences are worth noting. Unlike the California law, the Guidelines apply even if the information was encrypted. Moreover, the Guidelines apply to all forms in which customer information is held, not only computerised media.

PRACTICAL SUGGESTIONS

As we noted at the beginning of this article, there is no guaranteed way to prevent a data security breach from occurring or to forestall the intense regulatory, political and public scrutiny that may ensue. Nevertheless, we suggest that banks follow a number of practices focused on reducing risk or mitigating loss. Needless to say, the choice of particular practices must be tailored to the business model, operational requirements, customer base, and threat and regulatory environments of each financial institution. Implementing each of these suggestions, however, is likely to achieve benefits in risk reduction.

First, no information security programme is valuable if it remains static. It needs to be periodically tested and updated to respond to new threats and criminal techniques, to take into account emerging technologies, and to incorporate lessons learned from the experience of the bank itself and of other financial institutions and companies. Changes in the company's business model, scope and scale of operations, types of customer information handled, and other business changes are also appropriate occasions to determine whether corresponding changes in the data security programme are warranted.

Second, a financial institution should carefully scrutinise the information security programmes of all service providers who handle data from the financial institution. Negotiating to allocate the financial damages that may arise from a service provider's breach of security resulting in loss of the financial institution's data is necessary, but may not be sufficient. By the time an indemnification or damages clause kicks in, the reputational damage has been done.

The financial institution needs to satisfy itself that its service providers have their own appropriate data security programmes in place and that they are handling the financial institution's data with the same or similar safeguards, training, doctrine, and procedures that the financial institution itself would use. This is an assurance to be obtained not only at the beginning of the contractual relationship with the service provider through due diligence, but throughout the performance of the contract, through periodic audits, assessments, and reviews.

The financial institution should also bear in mind that if the service provider will perform some or all of the contracted-for work abroad, additional measures may be warranted to familiarise the service provider with the applicable security requirements, to verify the service provider's compliance with its contractual commitments, and to assure the enforceability of these commitments.

Finally, it is essential to plan and prepare for a data security breach, which could range from a relatively minor and isolated "low tech" incident to one affecting tens of millions of the financial institution's customers and its core business processes. While such a

plan will vary greatly in its details from bank to bank, and will need to be tailored to specific situations that arise, at a minimum it should address:

- working with the bank's service providers and business partners to prevent, evaluate, and mitigate the risk of fraud, identity theft or other losses to customers;
- procedures for notification of and cooperation with regulators and law enforcement officials;
- processes for determining whether a customer notification requirement under the Interagency Guidelines, or under California or similar laws is triggered, which in some cases may include the need to retain computer forensic and financial fraud experts to advise on the likelihood of misuse or compromise of the data;
- an initial draft notification to customers, which of course will have to be modified according to the particular situation; and
- preparing for the possibility of Congressional inquiries and hearings, as well as litigation and intense regulatory, media and public attention.

This list is far from exhaustive, but its elements form the basis for creating a plan which may facilitate mobilisation and decision-making in the initial, often frenetic phases of identifying and responding to a data security breach crisis.

CONCLUSION

Because of the evolution in threats to data security, and changes in the regulatory responses to that evolution, even the best and most comprehensive information security programme requires continuing attention. In this sense, reaching data security is a journey and not a one-stop destination. Ideally a financial institution's data security programme will function as an integral part of internal management controls designed to prevent any breach of data episodes, but it is also essential to prepare to respond to any such breach and to fold lessons learned from any and all sources back into ongoing efforts to assure information security.

Over time, as data security breach incidents continue to impact the industry, the markets as well as the regulators are likely to focus on leading-edge information security as a strategic differentiator among well-run financial institutions.

Notes:

[1] A California statute also requires businesses that own or license personal information about a California resident to implement and maintain reasonable security measures to protect the personal information from unauthorised access, destruction, use, modification, or disclosure.

[2] At the time this article was written, federal legislation requiring notification to consumers of breaches in data security under various circumstances had been proposed but not enacted.

This article was written by Richard M. Alexander, Partner, and Ronald D. Lee, Partner, arnold & Porter LLP, 555-12th St. NW, Washington, DC 20004, US. Tel: 1 202 942 5728, 1 202 942 5380, Fax: 1 202 942 5999, Email: richard_alexander@aporter.com, ronald_lee@aporter.com