dataprotectionlaw&policy

FEATURED ARTICLE
03/07

cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

Massachusetts Bill: shifting the costs of data breaches

Recent high-profile US-state security breaches have ensured state legislators continue to formulate laws to address the problem. A Massachusetts proposal would, if introduced, have the most far-reaching security breach regulatory impact to date, requiring commercial entities to reimburse banks, on behalf of affected consumers, for costs incurred in connection with a breach. Agnes Bundy Scanlan, Laurie Burlingame and Jacqueline Klosek, of Goodwin Procter LLP, examine the proposal.

Over the past several years, there have been a number of highly public data security breaches. According to the Privacy Rights Clearinghouse, a San Diego based consumer rights organization, since 2005, the data records of more than 104 million US residents have been exposed to security breaches. While breaches of data security can be detrimental in a number of ways, a lot of the concern about security breaches has centered around the fact that such breaches, when involving certain types of personal data, can result in identity theft.

Security breaches occur in numerous ways and can impact either a small or large group of consumers at one time. A review of some of the recent breaches show the very wide range of ways that breaches can and have occurred. While many breaches have occurred as a result of hacking into and tampering with computer networks, others have occurred after documents containing personal information fell off transport trucks; after company employees were tricked into selling data to fraudsters; and after employees made errors in disclosing more information than they were authorized to disclose.

Regardless of the number of consumers affected, these security breaches take a serious toll on victims, as they must spend hours to get new identifying information and have their credit reports cleared up. Breaches also result in losses for financial institutions. Generally, it is the credit card issuing banks that end up paying for the losses associated with security breaches. It is estimated that losses associated with security breaches totaled approximately $2 billion in 2006.

Two of the more recent newsworthy security breaches occurred in retailers headquartered in Massachusetts. The first of these security breaches evolved from the computerized systems of TJX, the operator of T.J. Maxx, Marshalls HomeGoods and A.J. Wright stores in the United States and Puerto Rico, the T.K. Maxx stores in the United Kingdom and Ireland and the Winners and HomeSense stores in Canada. TJX has not released information regarding the nature or volume of the personal information that was compromised, but it is believed to be broad, covering customer transactions from the United States, Puerto Rico and Canada in 2003, periodically through 2005, and from May to December 2006. While originating in Massachusetts, this breach quickly became a worldwide event, as customer information obtained in this breach was used to rack up fraudulent charges by criminals as far away as Sweden and Hong Kong. An investigation into the TJX security breach is still in progress.

The second of the Massachusetts retailers affected by a security breach was Quincy-based Stop & Shop Supermarket Companies. In mid-February, Stop & Shop confirmed that customer information had been stolen from several of its stores in Rhode Island and at least one of its stores in Massachusetts. In this case, individuals removed checkout-card readers, installed bugs into the readers to steal consumer information and then reinstalled the readers. To combat this problem, Stop & Shop announced that it had bolted down card readers at all of its stores throughout New England, New Jersey and New York. Several individuals have been arrested in connection with this security breach.

As a result of the increase in security breaches, such as the TJX

and Stop & Shop cases described above, state legislatures have begun to develop laws to address the problem. The US Congress has also taken an interest in the area. Recently, Representative Michael A. Costello of Newburyport, Massachusetts, proposed a Bill in the Massachusetts House of Representatives that, if passed, would have the most far-reaching security breach regulatory impact to date.

Massachusetts proposed solution

The Massachusetts Bill, the stated purpose of which is to enhance the confidentiality and protection of identifying consumer information, would impose two major requirements on commercial entities that experience breaches in the security of computerized data systems, resulting in the exposure of personally identifiable data. The Bill defines the term 'commercial entity' broadly to include both for-profit and not-for-profit corporations, all forms of partnerships, estates, limited liability companies, associations, joint ventures, governments and government subsidiaries, organizations, or any other legal entity. Under the Bill, a breach of the security of the system refers to 'the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information.' Finally, 'personal information' is defined as a resident's name along with one other element of identity, such as Social Security Number, driver's license number or account number with its access code.

As observed above, the proposed legislation would result in two new obligations for covered entities. First, the Bill would require both commercial entities and individuals that maintain computerized personal information about consumers to notify consumers if their computerized data systems are breached in such a way that information about a Massachusetts resident has been misused, or this is reasonably likely to occur. Notice under this section is supposed to occur in the most effective manner possible and 'without unreasonable delay.'[1] Under the Bill, notice can be directly provided to consumers in several forms: written, telephonic or electronic, as long as it complies with federal law. In addition, if the cost of providing notice directly to affected residents exceeds $250,000, the number of residents to be notified exceeds 500,000, or the affected entity does not have sufficient contact information of residents, the entity can provide a form of substitute notice that requires email notification to all residents for which it has email addresses, a conspicuous posting of a notice on the entity's website and notice to major statewide media.

The Massachusetts Bill would only cover breaches of systems for which the personal data had not been encrypted

Second, the Bill would apply to any commercial entity that was required to provide notice to consumers of a system security breach in which personal information has been misused or is reasonably likely to be misused, requiring it to reimburse banks on behalf of the affected consumers for any costs that the bank occurred in connection with the security breach. According to the Bill, these potential costs include: costs of canceling or reissuing credit cards; costs of closing bank accounts and stopping payment on certain transactions; costs associated with opening new bank accounts; and costs associated with refunding customers for unauthorized credit transactions. Currently, this Bill is pending in the Massachusetts Legislatures' joint committee on consumer protection.

Reactions to the proposed legislation

The numerous data security breaches occurring over the past few years have raised the attention of state lawmakers. Many states have responded to the concern over security breaches and the resulting risk of identity theft by enacting legislation to require companies experiencing breaches in certain types of data to notify consumers about those breaches. The Massachusetts Bill is very interesting in that it takes a novel approach to the problem. As such, the Bill has already incited a great deal of commentary and debate. The notification provision of the Bill has not raised much concern because, as observed above, this requirement is not novel since at present, approximately thirty-five states have either enacted or proposed similar notification statutes.[2] However, the section of the Bill that would require retailers to pay for costs associated with restoring the consumers' credit has engendered many different viewpoints.

Some analysts have contended that imposing these costs on the retailers is necessary to get them to upgrade their existing security systems, which are woefully inadequate to protect sensitive consumer information.[3] According to Visa, although credit card companies instituted security rules for businesses accepting credit card information almost two years ago, only one-third of large retailers have complied with these rules. Unfortunately, companies oftentimes do not want to update their security systems since such updates are costly, thereby impacting the institution's bottom-line.

Those who support the Massachusetts Bill claim that this requirement will enable companies to contemplate security

enhancements as a long-term investment, because if a company experiences even one security breach, the aggregate of the direct costs and indirect costs associated with damage to its reputation are likely to be very high.

Individuals on the other side of the argument suggest that the Massachusetts Bill is targeting the wrong group to bear the costs associated with security breaches. For example, retailers claim that they already pay for potential fraud *a priori,* as the banks charge them interchange fees for every transaction made with a credit card.

It is estimated that the credit card industry generated some $30 billion in fees in 2006, with between $21 billion and $27 billion of that amount directed to the issuing banks. In addition, the credit card companies also impose fines on merchants who do not comply with security standards. Hence, the retailers feel that an additional government fine would be excessive and amount to a 'pyramiding of fees.'

Yet others have taken the position that the retailers should not be held accountable for security breaches because it is not always possible to completely secure such systems from hackers, who are typically highly versed in computer operations. These individuals claim that the problem is with the credit card networks themselves, which are not secure and require enhancements to better protect transaction data (for example, by requiring individuals to authenticate their card through a constantly changing access code). These individuals also claim that it makes more sense to solve the problem on the network level, as there are only a few networks in existence, while there are thousands of retailers with varying levels of security in place.

Commentary

Determining which party should bear the costs associated with data security breaches is clearly a difficult issue which requires a great deal of analysis and is beyond the scope of this article. However, one item of interest is to note that the Massachusetts Bill would only cover breaches of systems for which the personal data had not been encrypted. Therefore, many retailers who currently encrypt personal data would not fall under the ambit of the law. One can only question whether the law, if enacted, should be so limited in scope.

A likely outcome of the Massachusetts and other state legislation is that we are more likely to see security breach federal legislation in the near future. Chairman of the House Financial Services Committee, Barney Frank (D-MA) appears to be in favor of this Bill, but claimed that he would prefer a national trigger for notification about the security breach. Although the contours of such a federal law are unknown, it would likely include the notification trigger described by Chairman Frank and potentially could shift liability from banks to retailers, as in the Massachusetts Bill. In addition, Congress might consider a provision that would allow consumers to place security freezes on their credit accounts without cost, a notion that has been supported by several states, including Massachusetts.[4]

Although some fear a federal rule, it seems that such a rule would offer greater clarity for businesses that are presently struggling to comply with the complex patchwork of state laws that currently exist or have been proposed. In this manner, all businesses will be treated the same, thereby not unfairly punishing entities in one geographic region due to stricter security standards. In addition, consumers across the country deserve the same level of protection from identity theft and the right to be promptly notified after such an incident occurs.

Agnes Bundy Scanlan Counsel
Laurie Burlingame Associate
Jacqueline Klosek Counsel
Goodwin Procter LLP
abundyscanlan@goodwinprocter.com
lburlingame@goodwinprocter.com
jklosek@goodwinprocter.com

1. Under the Bill, one would not need to give notice if such delay was required for law enforcement to conduct an investigation, hence suggesting that this type of action would be a cause for reasonable delay.
2. See, for example, National Conference of State Legislatures, 2006 Breach of Information Legislation (last updated Jan. 7, 2007) for a summary of the different state laws and proposals.
3. Companies would likely be required to upgrade their security systems if this Bill were passed, not only due to the fear of costs associated with regulatory action for non-compliance, but also due to the fact that insurers would likely not insure entities that had failed to comply with all required government regulations. This would place even greater stress on companies to upgrade their security systems.
4. In fact, Representative Costello has co-sponsored another Massachusetts Bill, H. 328, which proposes such a measure.

cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

Registered number 2676976 Registered address 141 Wardour Street, London W1F 0UT VAT registration 577806103

e-commerce law & policy

Many leading companies, including Amazon, BT, eBay, FSA, Orange, Vodafone, Standard Life, and Microsoft have subscribed to ECLP to aid them in solving the business and legal issues they face online.
ECLP, was nominated in 2000 and again in 2004 for the British & Irish Association of Law Librarian's Legal Publication of the Year.
A twelve month subscription is £390 (overseas £410) for twelve issues and includes single user access to our online database.

e-commerce law reports

You can now find in one place all the key cases, with analysis and comment, that affect online, mobile and interactive business. ECLR tracks cases and regulatory adjudications from around the world.
Leading organisations, including Clifford Chance, Herbert Smith, Baker & McKenzie, Hammonds, Coudert Brothers, Orange and Royal Mail are subscribers.
A twelve month subscription is £380 (overseas £400) for six issues and includes single user access to our online database.

data protection law & policy

You can now find in one place the most practical analysis, and advice, on how to address the many problems - and some opportunities - thrown up by data protection and freedom of information legislation.
DPLP's monthly reports update an online archive, which is an invaluable research tool for all those who are involved in data protection. Data acquisition, SMS marketing, subject access, Freedom of Information, data retention, use of CCTV, data sharing and data transfer abroad are all subjects that have featured recently.
Leading organisations, including the Office of the Information Commissioner, Allen & Overy, Hammonds, Lovells, BT, Orange, West Berkshire Council, McCann Fitzgerald, Devon County Council and Experian are subscribers.
A twelve month subscription is £355 (public sector £255, overseas £375) for twelve issues and includes single user access to our online database.

world online gambling law report

You can now find in one place analysis of the key legal, financial and regulatory issues facing all those involved in online gambling and practical advice on how to address them. The monthly reports update an online archive, which is an invaluable research tool for all those involved in online gambling.
Poker, payment systems, white labelling, jurisdiction, betting exchanges, regulation, testing, interactive TV and mobile gaming are all subjects that have featured in WOGLR recently.
Leading organisations, including Ladbrokes, William Hill, Coral, Sportingbet, BskyB, DCMS, PMU, Orange and Clifford Chance are subscribers.
A twelve month subscription is £485 (overseas £505) for twelve issues and includes single user access to our online database.

world sports law report

WSLR tracks the latest developments from insolvency rules in football, to EU Competition policy on the sale of media rights, to doping and probity. The monthly reports update an online archive, which is an invaluable research tool for all involved in sport.
Database rights, sponsorship, guerilla marketing, the Court of Arbitration in Sport, sports agents, image rights, jurisdiction,domain names,ticketing and privacy are subjects that have featured in WSLR recently.
Leading organisations, including the England & Wales Cricket Board, the British Horse Board, Hammonds, Fladgate Fielder, Clarke Willmott and Skadden Arps Meagre & Flom are subscribers.
A twelve month subscription is £485 (overseas £505) for twelve issues and includes single user access to our online database.

priority order form

FAX +44 (0)20 7729 6093
CALL +44 (0)20 7012 1380
EMAIL dan.towse@e-comlaw.com
ONLINE www.e-comlaw.com
POST Cecile Park Publishing 17 The Timber Yard, Drysdale Street, London N1 6ND

☐ Please enrol me as a subscriber to **e-commerce law & policy** at £390 (overseas £410)
☐ Please enrol me as a subscriber to **e-commerce law reports** at £380 (overseas £400)
☐ Please enrol me as a subscriber to **data protection law & policy** at £355 (public sector £255, overseas £375)
☐ Please enrol me as a subscriber to **world online gambling law report** at £485 (overseas £505)
☐ Please enrol me as a subscriber to **world sports law report** at £485 (overseas £505)

All subscriptions last for one year. You will be contacted at the end of that period to renew your subscription.

Name			
Job Title			
Department		Company	
Address			
Address			
City		State	
Country		Postcode	
Telephone		Fax	
Email			

1 Please **invoice me** Purchase order number
Signature Date

2 I enclose a **cheque** for the amount of
made payable to *'Cecile Park Publishing Limited'*

3 Please debit my **credit card** VISA ☐ MASTERCARD ☐
Card No. Expiry Date
Signature Date
VAT No. (if ordering from an EC country)

Periodically we may allow companies, whose products or services might be of interest, to send you information.
Please tick here if you would like to hear from other companies about products or services that may add value to your subscription. ☐