



In Brief

- **Attacks on the security of your customer information can pose a real threat in these days of increasing identity theft.**
- **The law in this area is fast-developing, with different schemes evolving in California, other states, and throughout Europe.**
- **When your database is breached, the actions you need to take are dictated both by the law and by practical necessity. Learn more in this article.**

It begins with a small theft. Someone breaks a car window, grabs a laptop computer lying on the back seat, and disappears into the darkness with the machine. Unfortunately, that laptop belongs to the global sales manager of your company. And now you—and she—have some big problems, because that laptop contains the ID and password used to access your company's customer relationship management (CRM) system. This CRM system contains a lot of sensitive information, and none of it is encrypted. Among the sensitive information: a complete profile of your company's customers around the world, the customers' credit card numbers, and the customers' passwords for your company's ecommerce website.

Who STEALS My NAME

The US and EU Response to Data Security Breach

The manager discovered the theft Sunday morning. Early Sunday afternoon, she received an ominous phone call from the vendor who runs the CRM system: An unusually large amount of customer data had just been downloaded. The manager immediately told the CRM vendor to lock out her password and freeze system access. Then she called you.

So far, she says, none of the company's customers have complained about an identity theft. Neither she (nor anyone else in the company) has received a ransom demand. Still, she is shaken by what has happened and needs your guidance. What advice should you give her? What further actions should she take? Is there a difference between the practical business actions she should take and the legally required actions she must perform? This article attempts to offer some answers for companies doing business in the United States and Europe.

By Donald A. Cohn, Jonathan P. Armstrong, and Bruce J. Heiman

US Legal Standards California

If your company has customers in California, your client will probably have to notify those customers about the security breach, pursuant to S.B. 1386.¹ This statute requires anyone conducting business in the state to promptly notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, disclosed to an unauthorized person as a result of a breach of the business's computer system. Violators can be hit with civil damage awards and injunctions.

What businesses are covered? This law applies only to businesses that satisfy two criteria:

- The company must be “conducting business in California”—which encompasses far more than just California corporations or other entities registered with the state. A company can be “conducting business in California” if it has just a few employees in the state or even if it just makes sales to people in California.
- The company must “own or license” electronic personal information, defined as an individual's first name or first initial and last name, in combination with one or more of the following:
 - o social security number;
 - o driver's license number or California Identification Card number; and/or
 - o account number, or credit card or debit card number, in combination with any password that would permit access to an individual's financial account.

Note that it is irrelevant where the company keeps such personal information. The law applies even if the data is stored on servers outside California.

What triggers the notice requirement? Notice is required whenever there is a cybersecurity breach and the business knows or reasonably believes that *unencrypted* personal information was disclosed to an unauthorized person.² If a company's computer system is breached, but the business is confident that no information was disclosed, then no notification is required.

When and to whom must notification be made? After learning of a security breach, a business is supposed to notify affected individuals as quickly as possible, consistent with determining the scope of the breach, stopping further disclosures, and cooperating with any law



DONALD A. COHN is the lead technology lawyer at El DuPont de Nemours & Co. Inc., based in Wilmington, DE. Don is cochair of the ABA Business Law Section, Cyberspace Subcommittee, and has acted as legal counsel to the White House Chartered Chemical Industry Cyber Security Task Force.



JONATHAN P. ARMSTRONG is a London-based technology lawyer with the European law firm Eversheds LLP. Jonathan is a coauthor of the LexisNexis definitive work on technology law, *Managing Risk: Technology & Communications*. His practice is international and includes counselling multinational companies on electronic corporate governance and privacy policies.



BRUCE J. HEIMAN is a partner in the Washington DC law and lobbying firm of Preston Gates Ellis & Rouvelas Meeds LLP, where he chairs the firm's information technology practice group. He represents clients on cybersecurity and privacy matters and has been active in the area since 1990.

enforcement agency investigation. In our experience, this means days, perhaps a couple of weeks, but not longer. However, a service provider who merely maintains another company's data and suffers a breach need not contact all the affected individuals. The provider is required to notify only the company whose data was breached, and that company must in turn notify its customers.

How must notification be provided? Notice may be either written or electronic. Any electronic notice must be consistent with the federal Electronic Signatures in Global and National Commerce Act of 2000 (known as E-SIGN). However, if the cost of providing such notice would exceed \$250,000, or the company would have to notify over 500,000 individuals, or the company lacks sufficient contact information, then the business may provide “substitute notice.” A company provides such notice by doing all of the following:

- emailing notices to those affected people for whom the company has email addresses;
- conspicuously posting the notice on the company's website (if it maintains one); and
- notifying major statewide media.

There's one exception to all this. The statute states that a business which maintains notification procedures as part of its own information security policies may follow those procedures if they are consistent with the timing requirements of the new law.

What must the notice say? The statute is silent on this key point, but the notice should at least inform the customer that an unauthorized person has acquired (or is reasonably believed to have acquired) computerized unencrypted personal information about the customer.

Moreover, since the purpose of the law is to allow affected people to take protective actions, the notice should probably state what personal information was or may have been disclosed.

Other states

California was the first state to pass a breach notification law (in September 2002), and recently many others have followed suit. Following a widely publicized series of cybersecurity breaches in early 2005 (by ChoicePoint, Bank of America, Motorola, and many others), at least 40 states considered legislation involving breach notification and computer security, according to a report by the

If you are investigating a **data security breach** that touches on a **European** country, you should start with the **data protection legislation** in the country concerned.

National Conference of State Legislatures. By February 2006, 22 states had enacted breach notification laws.

These notification laws are generally similar to the California law. But each state law has its own particular requirements and specifications leading to potential compliance burdens.

Federal legislation

There is currently no federal law on breach notification, but five major bills on this topic were pending in Congress early in 2006. These bills all address the following key issues:

- *To what extent should federal law preempt state laws on breach notification?* Many large companies argue that they need to operate pursuant to a single set of rules, rather than a patchwork of inconsistent state laws. Therefore they are pushing for federal legislation that completely preempts state laws in this area. Three of the five bills clearly provide such preemption.
- *How serious must a breach be for the notification requirement to apply?* One bill would require notification whenever there is a breach of sensitive personally identifiable information. Another bill would require notice only when the breach results in a “reasonable risk” of harm. Two bills set the standard at a “significant risk” of harm. The final bill refers to “substantial harm or inconvenience.” Many businesses are pushing for one of the heightened standards, because they are concerned

about compliance costs and negative publicity.

- *Who is responsible for providing notice?* Three of the bills would impose notice requirements only on companies that own or license private data. The fourth bill would also impose such requirements on third-party service providers. The fifth makes the entity suffering the data breach “primarily responsible” for providing notice, unless there is an agreement between an entity and its third-party service providers to the contrary.
- *How should notice be given?* Many businesses are concerned about impractical dictates; they would like any federal law to permit a wide range of notification methods (email, phone). But the bills impose various restrictions and conditions on notification. Businesses also would like a safe harbor that protects companies from liability if they follow their own breach notification procedures, adopted pursuant to their own information security policies. Only one of the five bills provides such a safe harbor.
- *If the federal law is violated, who has the authority to sue the offender?* Businesses are adamant that any federal legislation should not be the basis for individual or class action lawsuits. Instead, the US Attorney General, the Federal Trade Commission, and perhaps state attorneys general should have exclusive authority to enforce the federal statute. Four of the five bills preclude private rights of action.

It remains to be seen whether, and in what form, federal breach notification legislation will be enacted. For one thing, the prospects for settling on a final bill are complicated by the fact that multiple committees are involved—the House and Senate Commerce Committees and the House Financial Services Committee, along with the Senate Judiciary Committee. Moreover, the second session of Congress is always shorter, and it becomes easier to delay and stop legislation. On the other hand, 2006 is an election year, and members of Congress may not want to admit they were unable to pass legislation to address voters’ concerns about identity theft and financial loss.

Legal Standards Outside the United States

The first myth about data protection law in Europe is that it starts and ends with the main European Community Directive, the Data Protection Directive (95/46/EC) (the Directive). Many countries in Europe had data

US States with Breach Notification Laws

Arkansas	Montana
California	North Carolina
Connecticut	North Dakota
Delaware	Nevada
Florida	New Jersey
Georgia	New York
Illinois	Ohio
Indiana	Rhode Island
Louisiana	Tennessee
Maine	Texas
Minnesota	Washington

protection law before the Directive came along; in the UK, for example, data protection legislation predates the Directive by a full 10 years. The second misconception is that every EU country adopts the Directive. First, the Directive only applies to countries that are in the EU (although others have used it as a template). Second, secondary in-country legislation is required to bring the Directive into force in each country. This secondary legislation often adds to the Directive, imposing country-specific requirements that go over and above those of the Directive. It is these country-specific requirements that generally impose additional data security obligations, including a reporting obligation where one exists.

Thus if you are investigating a data security breach that touches on a European country, you should start with the data protection legislation in the country concerned. Currently about 33 different European jurisdictions (including the 25 within the EU) have some form of privacy or data protection law in place. A full discussion of this law is beyond the scope of this article; we will simply note here that only a minority of these jurisdictions, as discussed below, explicitly require notification of data security breaches. (For more information on this topic,

see “ACC Resources on Data Security,” on p. 34.)

Notification standards

In Europe, there are as yet no direct equivalents of the Californian legislation, either at an EU or a domestic level. A minority of European states, however, have domestic laws that impose some notification standards when there is breach of personal data.

Italy

In Italy, for example, § 32 of the Italian Privacy Code states that:

Where there is a particular risk of a breach of network security, the provider of a publicly available communications service must inform subscribers and, if possible, users concerning that risk and, when the risk lies outside the scope of the [security] measures to be taken by the provider, the provider must give details of possible additional measures, including an indication of the likely costs involved.

This information must also be provided to the Italian Privacy Authority and the Italian Authority for Communications Safeguards.

Norway

In Norway, the unauthorized disclosure of personal data must be reported to the state data privacy office, Datatilsynet, but not to the individuals whose data has been compromised.³ No time limit is given for making the report, although the Datatilsynet has said it expects a report to be made within about a week of the breach.

Malta and Germany

Malta and Germany have complex legal provisions that could lead to mandatory reporting. Malta, for example, mandates that if a Personal Data Representative (PDR) has been appointed by a corporation to control data within that business, this PDR can be obliged under Article 31(2) of the Maltese Act to report to the Data Protection Commissioner in some circumstances, including after a security breach. In many respects the German system is similar. Most US corporations doing business in Germany will appoint an internal data protection officer (DPO) to police data handling, which can help the

company avoid the need to register with the local data protection authority. The DPO can be a company employee or an external person experienced in data protection law, and is responsible for the company's compliance with the German Data Protection Act (Bundesdatenschutzgesetz, or BDSG). If a security breach occurs, the DPO must act independently to stop the security breach. The DPO would determine whether the breach must be reported either to the relevant data protection authority or to the data subjects themselves.

Hungary

In Hungary, the Hungarian Data Protection Act⁴ contains a provision that is similar to those found in many other EU countries: It requires that data subjects (those on whom data is being kept) be informed about who is handling their data and how.⁵ Hungarian authorities have interpreted this as a requirement that data subjects be informed of any security breach (although no time limit has been set for providing such notice).

California's Cybersecurity Initiative

In 2004 the California legislature passed a law to impose a requirement for the protection of computerized personal information. This law was the first in the United States to establish an explicit, general, cybersecurity requirement. California Law A.B. 1950¹ requires businesses that own or license personal information about California residents to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." It also states that a business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party, require by contract that the third party implement and maintain reasonable security procedures and practices.

The statute explains that "it is the intent of the Legislature to ensure that personal information about California residents is protected" and to "encourage" (although the statute is mandatory) businesses to provide "reasonable security" for personal information (although the statute does not define reasonable security). Violation of A.B. 1950 is subject to a civil suit for damages as well as an injunction.²

The law retains the broad definition of "personal information" found in the breach notification law, with the addition of medical information. The statute also defines the phrase

"owns or licenses" broadly as "intended to include, but is not limited to, personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates."

The law is intended as a minimum, broadly applicable, baseline standard for the treatment of personal information by entities that are not covered by specific privacy statutes. A.B. 1950 specifically does not apply to any business that is regulated by a state or federal law providing greater protection to personal information than that provided by this law (e.g., medical and financial entities under HIPAA and GLBA).

Arkansas, Rhode Island, and Texas also affirmatively require reasonable security procedures and practices.³

NOTES

1. Assembly Bill No. 1950 adds and amends California Civil Code § 1798.81.5.
2. CA Civ Code § 1798.84. The California Senate Judiciary Committee staff also tried to address concerns about the new cause of action by explaining that "If reasonable procedures are maintained, a business would not be liable under the bill even if there were an unauthorized disclosure."
3. Although beyond the scope of this article, some of these laws also address "security freezes" on credit reports, requirements for data disposal, and limitations on the use of social security numbers.

Other EU countries

Other countries' data protection authorities have not followed Hungary's lead in explicitly interpreting their nations' data protection provisions to mandate notice of a security breach; however, it is likely that, in any investigation, the authorities will take into consideration whether notice has been given to data subjects. Given the wide-ranging powers of investigation and sanction in many European countries, this could lead to a civil or criminal investigation and—in extreme cases—punishments for individuals or corporations, ranging from administrative action or fines to imprisonment. In addition, the mere fact that a corporation is under investigation could cause severe difficulties. For example, some activities in Europe are subject to a prior license regime (e.g., to operate a wireless network, some forms of transportation, or certain types of plant), and licenses could be withdrawn or withheld.

Even when there is not a black-letter obligation to inform data subjects of a security breach, regulatory authorities often strongly encourage “voluntary” disclo-

sure. Such deals seem typically to be done behind closed doors, but a high-profile case in Spain is an exception. That case concerned the Spanish version of the popular reality TV show, *Big Brother*. In Spain, as in other parts of Europe, thousands of applicants sent their details to the TV company with the hope of taking part in the show. Some of the personal details of about 1,700 applicants appeared on a fan club website after an attack on the TV company's server. After regulatory activity, the breach was publicly reported. (And by the way, the Spanish data protection authority fined the production company behind the show the equivalent of about \$1.2 million for the security breach.)

Other reporting obligations

There's a second major way in which EU privacy law could result in mandatory notification: A data subject (perhaps suspecting a breach) could make a “subject access request.” A “subject access request” is a formal request directed to a corporation asking (for example) what data the corporation holds on an individual and who has seen it. Most EU jurisdictions would require that a data controller disclose who has seen the data. Pressure groups or business competitors could therefore use this mechanism to force disclosure of a suspected security breach. Moreover, such subject access requests must ordinarily be answered within a short space of time. (In the United States, by comparison, some disclosures have occurred months after the suspected breach.)

Other types of regulations can also impose disclosure requirements. In the UK, for instance, the Financial Services Authority (FSA) has said that it intends to keep a close eye on the security practices of ebanking sites and that it will call the operators to account for any breaches.

Criminal legislation could also have a role to play. Many countries in Europe criminalize hacking, and any resultant criminal prosecution might lead to significant publicity for the original attack.

Registration and security breach liability

In most European jurisdictions, a company must register with a specified state authority if the company intends to process any personal data. These authorities are increasingly using this registration process to require applicants to specify the precautions they will take against disclosures of personal data. It seems likely that a security breach in violation of such a security policy could prove actionable. Again, action by the data protection authorities is likely to include administrative action, civil penalties, fines, or in the very worst cases, possible imprisonment. Often the authorities will remind regis-

Some European Data Protection Authorities

- Austria—Büro der Datenschutzkommission und des Datenschutzrates
- Belgium—Commission de la Protection de la vie privée
- Denmark—Datatilsynet
- France—Commission Nationale de l'Informatique et des Libertés (often known as CNIL)
- Germany—Der Bundesbeauftragte für den Datenschutz
- Hungary—Adatvédelmi Biztos
- Iceland—Persónuvernd
- Ireland—Data Protection Commissioner
- Italy—Garante per la protezione dei dati personali
- Luxembourg—Commission à la Protection des Données Nominatives
- Monaco—Commission de contrôle des informations nominatives
- Netherlands—College Bescherming Persoonsgegevens (CBP)
- Norway—Datatilsynet
- Portugal—Comissão Nacional de Protecção de Dados
- Romania—Avocatul Poporului
- Spain—Agencia Española de Protección de Datos
- Sweden—Datainspektionen
- UK—Information Commissioner

trants of the likely penalties on registration—for example, the registration form of the Irish Data Protection Commissioner requires an individual to certify that all of the registration information submitted is “correct and complete” and warns signatories that:

1. *Knowingly to furnish false or misleading information is an offence.*
2. *It is also an offence knowingly (a) to keep personal data not specified on your applications, (b) to keep or use personal data for any purpose, or disclose personal data to any person or body, not described in those applications. . . .*

In Europe, as in California, individuals are generally allowed to commence civil actions for losses sustained as the result of a security breach. In the UK, for instance, individuals can seek to recover their monetary damages as well as damages for their emotional distress.⁶

Moreover, a contractual relationship will often exist between the parties—arising, for instance, from an employment contract or the privacy policy posted on a company’s website. This could give rise to an action for breach of contract. Civil actions in Europe are not common at present, but we know of at least one class action that currently seems to be planned.

Many countries in Europe **criminalize hacking**, and any resultant criminal prosecution **might lead to significant publicity** for the original attack.

What Steps Should You Take?

When you receive a call like the one from our hypothetical sales manager, you and your client should prepare to act quickly. In our example, you could certainly reasonably believe that personal information might have been disclosed to unauthorized persons. Now your company may need to meet tight deadlines in both Europe (in response to subject access requests) and the United States (in response to mandatory notification laws).

Consider notifying law enforcement. First, you and the sales manager should consider notifying appropriate
(continued on p. 36)

Data Security

ACC Committees:

More information about these ACC committees is available on ACC OnlineSM at www.acca.com/networks/committee.php, or you can contact Staff Attorney and Committees Manager Jacqueline Windley at 202.293.4103, ext. 314, or windley@acca.com.

- Corporate & Securities Law
- International Legal Affairs

Docket Articles:

- James R. Beyer and E. Johan Lubbe, "Clash of the Titans: Complying with US Whistleblowing Requirements While Respecting EU Privacy Rights," *ACC Docket* 24, no. 4 (April 2006): 22–36, available via www.acca.com/docket.
- Klara Burianova and Alice Turinas, "Avoiding the Latest EU Data Protection Pitfalls: Changes in European Privacy Laws That Restrict Emarketing," *ACCA Docket* 21, no. 6 (June 2003): 92–101. www.acca.com/protected/pubs/docket/jj03/eudata1.php.
- Michael Hintz and Michael Fekete, "Keeping Secrets: The Growing Challenge of Protecting Data in Outsourcing and Service Provider Arrangements," *ACC Docket* 22, no. 10 (November/December 2004): 44–59. www.acca.com/protected/pubs/docket/nd04/keeping-secrets.pdf.
- "Records Retention in Europe," *ACC Docket* 24, no. 2 (February 2006): 22–32. www.acca.com/protected/pubs/docket/feb06/retention-feb06.pdf.

Leading Practice Profiles:

- Leading Practices in Privacy and Data Protection: What Companies Are Doing (2006), www.acca.com/resource/v6679.

InfoPAK:

- Data Protection—A Practical Guide to Personal Data Transfer Laws in Europe, Canada and the U.S. (2005), www.acca.com/infopaks/data_protection.html.

Webcasts:

The following webcasts are available at www.acca.com/networks/webcast/:

- Data Privacy in Europe—The Essentials (June 15, 2006)
- "Whistleblower" Anonymous Hotlines and SOX—Dealing with the French and German Decisions (November 17, 2005).

Annual Meeting Course Materials:

Program material from these courses at ACC's 2005 Annual Meeting is available at www.acca.com/am/05/material.php.

- Jeffrey D. Adelman, Paula Barrett, Brent V. Bidjou, "Pitfalls and Landmines in Privacy and the Collection, Use, and Security of Personal Information," course 110.
- James R. Beyer, William Davis Harn, Larry L. Sharrar, "Workplace Privacy," course 306.

Virtual Library Sample Forms and Policies:

Sample forms and policies available via ACC's Virtual LibrarySM (www.acca.com/vl) include the following:

- Data Protection Surveys for EU Member States, an ACC Quick Reference. www.acca.com/resource/v6285.
- Flexsys' Retention Periods for Europe, an ACC Quick ReferenceSM. www.acca.com/protected/reference/retention/retentionperiod.html#1.
- Fact Sheet on European Union Privacy Directive (2005). www.acca.com/resource/v6163.
- Policy on Data Privacy (Finland, 2005). www.acca.com/resource/v6982.
- Privacy Due Diligence Checklist (2005). www.acca.com/resource/v6058.
- Privacy Policy (transfer of employee data, EU-US) (2006). www.acca.com/resource/v7097.

ACC-related Articles:

- "International data protection," a Global Counsel resource. Available via www.acca.com, at <http://ld.practicallaw.com/0-100-9542>.
- "Global Privacy Law: A Survey of 15 Major Jurisdictions" (2002), www.acca.com/protected/article/international/privacysurvey.pdf.

Don't forget to visit ACC's Compliance Portal, at www.acca.com/practice/compliance/index.php, which features topics that include privacy and international trade.

(continued from p. 33)

law enforcement agencies. While notifying these agencies is not required in the United States, they can help in recovering the stolen laptop and in apprehending the thief. In Europe, many regulators would consider notification necessary to guard against unauthorized or unlaw-

Articles, Books, and Websites on Data Breach Notification

Books and Reports:

Jonathan P. Armstrong, Mark Rhys-Jones, and Daniel Dresner, *Managing Risk: Technology and Communications* (Elsevier 2005).

“Corporate Governance and Information Assurance: What Every Director Must Know” (Report prepared by Eversheds and RAND Europe for IAAC, www.iaac.org.uk).

Raymond T. Nimmer and Holly K. Towle, *The Law of Electronic Commercial Transactions* (Sheshunoff 2006) at ch. 15.

Websites:

California Office of Privacy Protection: Recommended Practices on Notification of Security Breach Involving Personal Information, www.privacy.ca.gov/recommendations/secbreach.pdf.

Federal Trade Commission: Information Compromise and the Risk of Identity Theft: Guidance for Your Business, www.ftc.gov/bcp/online/pubs/buspubs/idthrespond.htm.

Information Warfare, www.iwar.org.uk.

Irish Data Protection Commissioner’s website, www.dataprotection.ie/.

Maltese data protection website (in English), www.dataprotection.gov.mt.

National Conference of State Legislatures: Security Breach Legislation, www.ncsl.org/programs/lis/cip/priv/breach.htm (a comprehensive list of state bills and laws related to data breach notification).

US Department of Justice Criminal Division (Computer Crime & Intellectual Property Section), www.cybercrime.gov.

ful processing of personal data. In Europe, if a company doesn’t contact the police, the data protection authority will probably require them to explain why not, and why the action they took was the better course.

Determine the notification method. You will have to determine which notification method (e.g., letter, email, phone) is both most efficient and best at complying with the law.

Notify your customers. You will need to work with the sales manager to notify your client’s customers, alerting them that there has been unauthorized access to the CRM system and that the security of their customer data may have been compromised. This notice must be carefully drafted, because it could be used as evidence in a prosecution or regulatory proceeding brought against the company. For example, in this case, the notice certainly should state that the company is not aware of any data that has actually been disclosed to date. The company could also note that is working with law enforcement. Notification must occur promptly, as soon as practicable; an obvious exception would be if law enforcement asks you not to do so because they believe it would jeopardize the capture of the criminal.

Notify all of your customers. Although the notice *must* be sent to customers in jurisdictions that have enacted a breach notification law, we believe it may also be prudent to send the notice to all customers potentially affected. Such incidents are invariably reported in the media, and from a customer relations perspective, your client simply cannot notify some customers and not others.

Work with regulators. In addition to sending notices to the individuals concerned, your client may need to engage with European regulators, as required by law. Even if strict reporting is not mandatory, you may still want to provide the information to regulators; this action may encourage the agency to act leniently in any subsequent investigation of your client.

Inform the sales force. Your client’s sales manager will also need to tell the company’s sales force about the situation as soon as possible—and certainly before the notice is transmitted. Working with the sales manager, you should provide background information as well as Q&As that are designed to address customer questions and complaints.

Consider additional help for customers. Some companies have felt the need to go the extra mile and offer additional help to potentially affected individuals. For example, a company could offer affected customers free insurance against credit card misuse, or offer them free credit reports and monitoring services to guard against identity theft. Taking such actions could help rehabilitate your client’s goodwill among customers and reduce the threat of

Being prepared with a quick, effective, and compliant response to a data breach is one of your best ways to ensure that it won't happen—and that if it does, you are prepared to protect your customers' identity and your company's reputation.

civil actions. And such offers may be less expensive than you think. By buying these services in bulk, your company could probably get a reduced price from third-party providers. We know of at least one case in which the offer of a free monitoring service was well received, particularly by individuals who had not been offered the service when other organizations had notified them of breaches. The result was that the corporation notifying customers of a security breach actually received thank-yous from the customers!

Establish or improve your policies and procedures. Your company should take this opportunity to establish a policy and procedure for handling any future data breach notifications. It should also review its existing administrative, physical, and technical safeguards for protecting personal information—as well as those of its CRM system vendor. (Thank the vendor for being diligent in monitoring and reporting the unusual account activity, and quickly shutting down access.)

- Does the company have in place recognized information security policies? What authentication measures are required for access to a system (e.g., certain mandatory password characteristics, such as those mandated in Italy, or a dynamic password logon system)?
- Are policies in place that prohibit employees from storing user IDs and passwords on portable computers?
- How burdensome would it be for the company to encrypt data, or at least the more sensitive data fields on the customer information template?

Review third-party contracts. Once the company reviews and updates its own policies and procedures and technology, you should review the company's standard contracts with third-party service providers to make sure that these agreements contain appropriate provisions concerning data security. The provisions should allocate the risk of a third-party vendor's failure of electronic or physical security; indicate who is responsible for the costs of notification; and specify who will pay the costs of defending third-party claims in the event of a data breach caused by the vendor.

Being Prepared

In the United States, we expect additional states will continue to enact data breach laws unless and until a federal law preempts them—and offers greater clarity. In the EU, given the power of public opinion, specific legislation

is also likely. Any in-house counsel responsible for data security matters should be up-to-date.

If you do suffer a security breach, take heart. While a breach of electronic security is never pleasant, you can use it to obtain at least some benefit for your company. It can help you secure resources for—and boost management's interest in—strengthening the client's electronic security and toughening its contracts with vendors who process your company's data. It can also help company personnel better understand some of the requirements of conducting electronic commerce in a multi-jurisdictional world. Being prepared with a quick, effective, and compliant response to a data breach is one of your best ways to ensure that it won't happen—and that if it does, you are prepared to protect your customers' identity and your company's reputation. ❏

The authors wish to thank the following people who provided invaluable contributions to this article. From Preston Gates Ellis & Rouvelas Meeds LLP: Paul Stimers (US). From Eversheds International: Paula Barrett (UK), Alvise Donà Dalle Rose (Italy), Florencia Grinberg (Spain), Bernadett Lastofka (Hungary), Arwid Mednis (Poland), Georg Röhsner (Austria), Rizwi Wun (Singapore), Kristine Karsten (France), and Christof Lamberts (Germany).

Have a comment on this article? Email editorinchief@acca.com.

NOTES

1. Senate Bill No. 1586 adds and amends California Civil Code §§ 1798.29, 1798.82, and 1798.84.
2. The statute does not define what is meant by "unencrypted." But the California Office of Privacy Protection called for use of the Advanced Encryption Standard adopted by the US National Institute of Standards and Technology.
3. Sections 2-6 of the Norwegian Personal Data Regulations.
4. Act LXIII of 1992 on the Protection of Personal Data and the Publicity of Data of Public Interest.
5. Section 6(2) of the Hungarian Act provides that a data subject "shall be notified of the purpose of data handling and of the identity of the persons who will handle the data. . . ."
6. Section 13 of the UK Data Protection Act 1998.

Donald A. Cohn, Jonathan P. Armstrong, and Bruce J. Heiman, "Who Steals My Name . . . The US and EU Response to Data Security Breach," *ACC Docket* 24, no. 6 (June 2006): 24–38. Copyright © 2006, the Association of Corporate Counsel. All rights reserved.