Customer Notice of Information Security Breaches

Much has been made recently of the "response program" expected of a financial institution as a part of its information security planning, and specifically whether customer notice is needed. The Gramm-Leach-Bliley Act (GLBA) contemplates that each financial institution will consider a response program. (The "Interagency Guidelines Establishing Standards for Safeguarding Customer Information," in section III.C.1.g., occur as appendixes to 12 CFR Parts 30, 208, 225, 364 and 570.) Also, in August 2003, the agencies released a proposed "Interagency Guidance on Response Programs" delineating some of the shape of these programs. Given this combination, it's safe to say everyone is interested in how a bank or other financial institution will deal with the question, "Should I inform my customers of a breach in security?" Let's take a look at how to answer that question.

COMPLIANCE

Need for a Response Program

As a supervisory matter, anecdotal evidence suggests that the banks' supervisory agencies are pushing harder and harder for a well-defined response program at financial institutions. Some of this may be a desire that management take advantage of the calm before a storm. Although no significant litigation currently appears on the horizon, it is fairly safe to say that soon one or another bank will be sued over a breach in security. Also, although it's still in proposed form, the 2003 interagency guidance mandates a customer notification and response program, which strongly suggests that this will soon be a rule we can't ignore.

Regardless of section 501(b) of the GLBA, many financial institutions are keenly aware that a disgruntled customer is both a lost opportunity and also a potential lawsuit. While the law is not perfectly clear, can we count on a court simply to dismiss an identify theft suit alleging damages suffered by a consumer? "Negligence" will likely be alleged as part of an effort to hold the bank responsible for breaching a duty to protect customer information against unauthorized access.

What Is a Response Program?

An information security response program looks much like any other type of a "disaster contingency" program. The difference is in the focus. An institution might begin, as an organizational matter, with designating a response team. Membership might be drawn from senior management and others who are otherwise closely involved in the information security program. The response program might also delineate and delegate responsibilities among the team. The goal is to empower the team and its members to deal effectively with difficult situations, on a real-time basis.

Once formed, the team might turn its attention to pre-planning. It could map various "what-if" scenarios, including contingency planning on the form and content of customer notices. At the least, preparation could entail a gathering together of various resources that would be useful reference materials if a customer notification becomes necessary.

Some Issues Already at the Forefront

The GLBA and its section 501(b) apply to "customer information" only. State laws, such as California's Computer Intrusion statutes (Civ. Code Section 1798.82 *et seq.*), also have limited scope. In California's case, they apply to "personal information." One issue currently at the forefront is how to deal with a breach that occurs at a party other than the institution but involves information about customers of the institution. **Example:** Imagine that your institution issues bank debit or credit cards. Imagine further that VISA or MasterCard informs you that specific and sensitive information regarding your cardholders has been compromised. The Association identifies the type of information, including the fact that the cardholder's name, card number, and expiration date have been compromised. To make the scenario somewhat more dire, assume that the cardholder's address and the cards' CVV numbers were part of the information taken. You are informed that this information was taken off of a processor handling card transactions on behalf of an on-line merchant.

Your initial reaction in this regard might be to notify cardholders. Certainly, nothing would bar an institution from providing that notice, and many would say that it is a good idea in any case, regardless of the legal requirements. However, technically it is not clear that either section 501(b) of the GLBA or laws like the California Computer Intrusion rules would mandate

Information Security Breaches

(continued from page 6)

customer notice in this case. Both these statutes impose a duty to notify customers, but in context they appear limited to notice of unauthorized access to information held by the institution (or, under section 501(b), provided by it to a service provider). In our scenario, the information was acquired from a merchant's processor, not from you or one of your service providers.

Courts may impose new duties on a bank, including somehow holding the financial institution responsible for the activities of distant third parties, such as a merchant's processor. This is a danger: Juries and courtrooms have not been favorable forums for financial institutions recently. Still, an expansion of a card issuer's duties to include notice of a breach involving third parties should give pause even to modern courts.

The Response

How would a card issuer "respond?" First things first. If losses are suffered by cardholders at the account level, the VISA and MasterCard chargeback rules may allow recovery against the merchant bank. Recovery of losses due to unauthorized use should be available through charge back if the thief were to use the stolen information in a "card not present" environment. If the thief were to use the information to create fraudulent cards, the situation becomes more complex. If CVV-2 (i.e., a new authentication scheme established by credit card companies to further efforts toward reducing fraud for Internet transactions) is properly used by the card issuer, the Associations may be responsible for card losses. This is a difficult and fact-specific analysis, requiring a close reading of the VISA or MasterCard rules. Nevertheless, it certainly is worth exploring.

There can be extraneous and supplementary costs. For example, if it were felt necessary to re-issue cards on a rush basis, the costs of card production can be high. Here, a compliance action against the merchant bank may still be available, alleging breach by the merchant of its duty to maintain a secure environment.

That may help on the monetary side. The issue remains, however: Should the customer be informed? Reputation risk becomes a legitimate factor in this equation. Some institutions are finding it appropriate to notify the customer, doing so in a letter that also makes clear the breach was not their fault. ■

— Mark A. Moore, Esq.
Adlrich & Bonnefin, PLC
Irvine, CA