CARLTON FIELDS

LOST OR STOLEN DATA: Minimizing Fallout

situation

Unfortunately, the theft or loss of private customer and/or employee information is becoming increasingly common. Since identity theft typically occurs within two weeks of a security breach, a company must have procedures in place to respond quickly.

in-house counsel challenge

Inside counsel must develop a process that will allow the company to quickly determine the extent of the breach, fulfill notification obligations under state law and mitigate the potential harm to customers and/or employees.

approach adopted

Your response process must be in place long before a laptop or any other data storage device is lost or stolen, because you will need to replicate its database to determine the information lost, the individuals impacted and the potential harm that might be caused if the information is misused. Some companies do not have a disaster recovery or emergency backup system in place to re-create lost data. Contact IT to determine whether your company can re-create data in the event of disaster (e.g., fire) or theft (e.g., stolen laptop).

Once the database is replicated, perform a risk assessment. If the lost or stolen data includes names, addresses and Social Security numbers or credit card numbers or other sensitive information, determine your notification obligations. Notification laws continue to evolve and vary depending on the state in which those affected reside. For example, if the data on a stolen laptop is encrypted, most states do not require you to notify the individual. If the computer is only password protected, most states do require notification. Even if your state does not have a data breach notification law, your company may wish to notify individuals if there is a significant chance of identity theft due to the type of data lost or stolen.

Draft a notification letter that explains what happened and provides instructions on how to file a fraud alert, which lasts 90 days, with any one of the three credit reporting agencies. In states with credit freeze laws, instruct individuals how to file. Also provide contact information for the Social Security Administration and other organizations, as necessary.

You may recommend a credit bureau's credit monitoring service, which typically includes identity theft insurance. If feasible, offer to pick up the tab, which not only mitigates liability exposure to the individual, but your company as well.

Work with media relations to prepare a public statement and press release explaining how you've mitigated the data loss and post it on your company Web site.

Identify and correct the security weakness to prevent future losses.

implementation steps

Make sure IT has a disaster recovery or emergency data backup system in place. If not, implement one immediately. Should data be lost or stolen:

- Have IT replicate the database to determine the type of data and the individuals involved.
- Establish your notification requirements, by state where those affected reside. In the absence of such laws, determine, based upon the type of information lost or stolen, if the company might reduce liability and benefit customers by sending notification of the breach.
- Send impacted individuals a notification letter with contact information for the big three credit bureaus, as well as the Social Security Administration and other applicable agencies.
- Include instructions on how to establish a fraud alert, credit monitoring, credit freeze and/or identity theft insurance through one of the agencies.
- Work with media relations to prepare a public statement.
- Implement new steps to prevent reoccurrence and future losses.

measuring success

Having procedures in place beforehand will result in a prompt, well-executed response. That, in turn, will significantly reduce the potential damages to the impacted individuals and the potential liability to your company.

future issues to consider

Every new convenience computers provide brings a corresponding security-related inconvenience. Annually review new technologies and their impact on your company's privacy/security policies. Since privacy and security law is a rapidly evolving field, regularly monitor the laws where customers are located.

CARLTON FIELDS
ATTORNEYS AT LAW

Phyllis F. Granade is a shareholder in Carlton Fields' Atlanta office, where she provides compliance assistance to clients confronted with privacy and security breaches. Phyllis is Peer Review Rated and can be reached at pgranade@carltonfields.com.