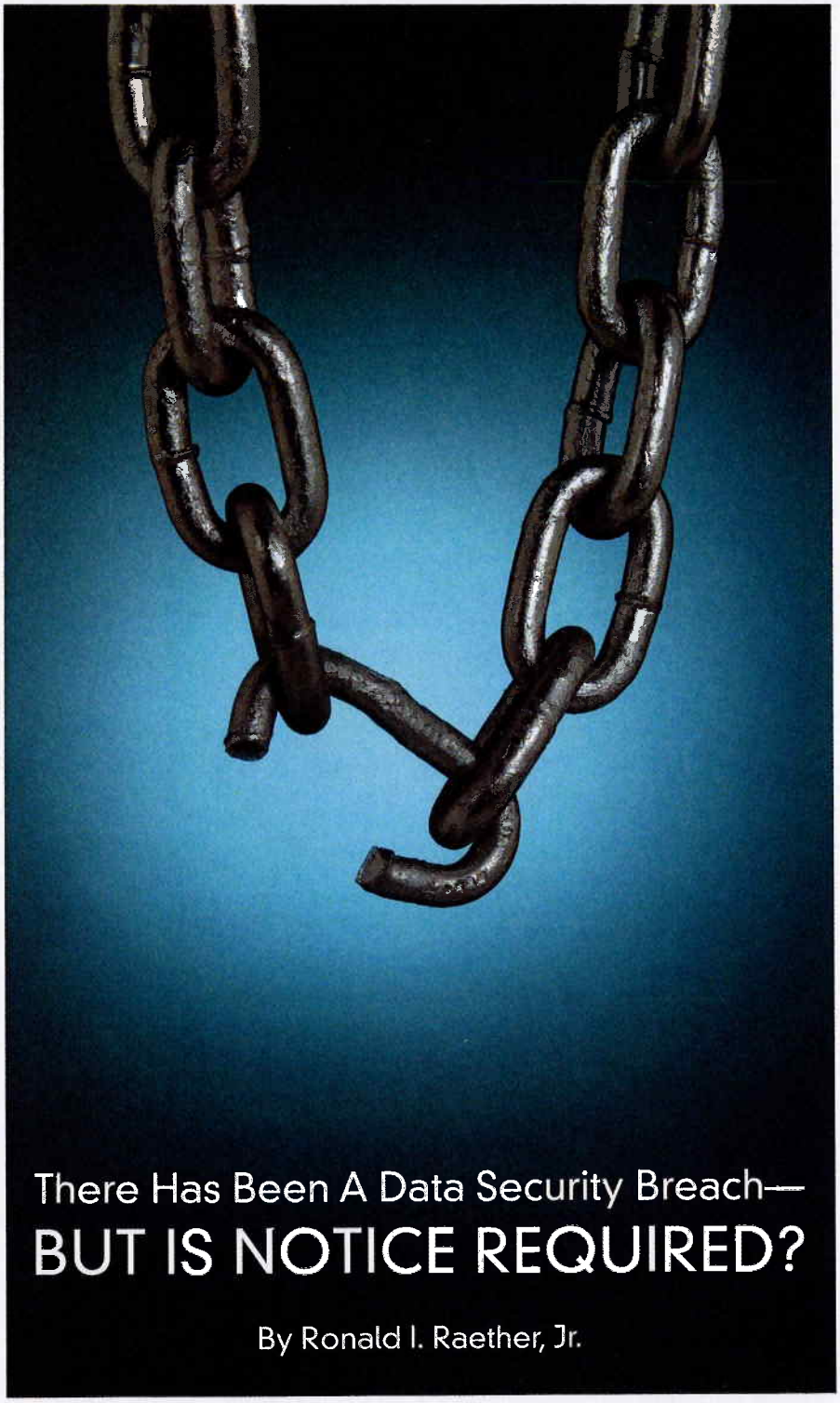

There Has Been A Data Security Breach— BUT IS NOTICE REQUIRED?

By Ronald I. Raether, Jr.

The emergence of Breach Notification statutes in 46 states places a clear responsibility on data stewards to understand the posture of PII in their custody. But with a range of statutory definitions and approaches, and still no "harmonizing" federal framework, questions quickly arise concerning the existence of a breach, and the remedial steps required in response.

It is Friday afternoon. You are looking forward to a relaxing weekend, spending time with your friends, and finally getting around to that list of activities that you have not had time for lately. Just a few more emails, and it is off to dinner at your favorite restaurant. At least that was the plan until just a few minutes ago, before Tom walked into your office.

Tom is from Human Resources, and he is reporting that an employee's bag was stolen from his gym locker. A company thumb drive was in the bag. Tom is coming to see you because the employee may have stored protected personal information on the thumb drive. You were recently named as the initial contact for potential data breaches in the company's incident response plan. To watch a video acting out this scenario, go to www.xtranormal.com/watch/11907723 (last visited June 30, 2011). So what should be the next step?

I have written before on developing an incident response plan and what should be included in the plan.[1] The basic concepts have not changed over the last few years. However, a few central questions have been developing, which still remain somewhat unclear today. How do you know if there has been a data breach that requires notice? Who should be notified?

The focus on data breach notification really began with the incident involving ChoicePoint in 2005. At that time, only California had a breach notification law. ChoicePoint decided initially to notify only California consumers. The backlash was swift and immediate. ChoicePoint quickly modified its decision and notified all affected consumers regardless of their state of residency.[2] The lesson for the industry? Err on the side of overnotification.

Even in the wake of the ChoicePoint incident and the passage of numerous other notification laws by several other states, a debate emerged and continues to this day. Will overnotification have an adverse effect on the purpose of the notice laws—namely, causing consumers to disregard the notices?[3] You may be able to answer this question based on your own experience from having received breach notices. Ask your neighbors, friends, and family. Most see the breach notice as another piece of junk mail and do little in response. Overnotification likely has not helped consumers better protect themselves.

Judging from these lessons, it is time to take a closer look at when a security breach results in the need for consumer notifications. The initial investigation and the legal analysis become critical to reaching the correct decision. The place to begin is with the legal standard for

providing notice. Admittedly, the states and regulators have not provided a clear picture on this point. As Sony can attest, making the wrong decision even today can have negative consequences.[4]

This article will discuss the little guidance available and suggest what should be the proper standard for when to provide consumer breach notifications. This article will then discuss the initial investigation and provide some guidance on conducting an investigation appropriate to the circumstances and geared towards addressing the legal questions. With this information in hand, a company is better positioned to decide whether a breach notice is required and who should be notified after a breach.

The need to comply with the law of multiple states presents an interesting challenge. While most states followed the lead of California, many states added slight modifications that make the analysis (and thus planning for compliance) more complex.[5] The same is true in deciding whether notice is required. However, there are some common questions in making this decision.

The obvious first question is whether the information at issue is covered by the governing statute, i.e., whether it concerns personally identifiable information (PII). Stated generally, breach notification laws concern data that includes some combination of PII (such as name and address) with confidential personal or financial information. The confidential information includes social security number, driver's license or state identification number, account number in combination with a password or security code, medical information, and the like. In the end, only if the incident involves data covered by the notice statute is further analysis even required.

Once it is determined that protected information is at risk, then the next step is to determine if the information was accessed or copied. The most basic place to begin is whether the information was encrypted. Most states do not require notice if the PII is encrypted. For example, under Nevada law, encryption means "the protection of data in electronic or optical form, in storage or in transit, using: (1) An encryption technology that has been adopted by an established standards setting body . . . which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and (2) Appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using guidelines promulgated by an established standards setting body. . . ."[6] Notwithstanding any encryption protection of data, many of these states still require notice if the hacker had access to the encryption keys, i.e., the hacker could view the data regardless of the encryption.

If the encryption exception does not apply, then is notice automatically required? Is this the end of the investigation? No. Many states require some level of potential harm. For example, Arizona requires that the breach "causes or is reasonably likely to cause substantial economic loss to an individual."[7] Other states take a slightly different perspective. For example, Florida does not require notice if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the entity determines that there is no reasonable likelihood of financial harm to the consumer.[8] Other states, such as Illinois, Georgia, and California, are silent on this point.

So what should be analyzed to decide if the harm element is met? The company should look at whether the information was accessed. If the company lacks records to determine definitively whether information was accessed, then a decision should be made as to the likelihood the information was accessed based on what data is available. Likewise, the company should determine whether the incident created a threat to the consumer. Was consumer PII the target of the unauthorized access?

An example helps illustrate the dynamics of this analysis. Suppose a criminal intends to steal money from the company. As part of the scheme, the criminal gains access to the company's computer system. The security breach could have given her access to PII. If there is evidence that (1) PII was not accessed or (2) consumer data was not the target of the scheme, then notice may not be required.

So why should notice not be required? Think of the computer system like your home with many rooms, closets, chests, drawers, boxes, and any number of other places to store things. A burglar comes into your home. The burglar may have the run of your house or may be limited to certain rooms. When you come home, you want to see what was taken. You confirm that your locked rooms and chests were not compromised. You look at the areas where the criminal had access. You look to see what was missing and you call the police and your insurer. On the loss report, you claim only the items that are missing. The same should be true with a data breach. Notice should be required for only the information that you reasonably believe was at risk.

So how do you determine the risk? You need to conduct a thorough and appropriate investigation. The obvious place to begin is interviewing the people involved. In our video scenario, you would interview the employee whose thumb drive went missing to learn such things as: what data can he access; what did he store on the thumb drive; and what equipment was used to store information on the drive. You also would interview the technical person supporting this employee to determine all of the locations in the company where copies of the data on the thumb drive are kept or where a footprint of what might be on the thumb drive might be located.

It is essential at the outset to identify and preserve all relevant records. Key sources that require immediate attention are log records and audit trails. If a third party handles any of the information or logs at issue, then a phone call and letter should be sent to secure these records. It is important to do this immediately as most systems allow such data to be writ-

continued on page 33

Ronald I. Raether, Jr. is a partner at Faruki Ireland & Cox P.L.L. in Dayton, Ohio.

Data Security Breach

continued from page 23

ten over within short periods of time (sometimes within 24 hours). These sources must be secured to avoid any spoliation issues, including any sources later identified by the entity conducting the forensic analysis.

You might ask loss prevention to speak with security at the gym where the bag was stolen. Likewise, if your employee has not done so already, then the employee should file a police report. Loss prevention should stay in contact with the police. These sources may be important to identifying the criminal and determining the target of the crime (although it is often too late to learn from the criminal what data was compromised).

Once you have a general understanding of the event, the next important step is to conduct a forensic analysis. I have written before on what issues should be considered in selecting the right party to conduct the study.[9] In sum, common issues include (1) what application or process will be tested; (2) what type of data may be exposed, and what is the source of that data (questions important in identifying applicable laws); (3) who will conduct the testing, and have they been properly screened and educated as to the limits imposed by law or contract; (4) what techniques will be used, and do these techniques raise contractual or other compliance issues; and (5) who will receive copies of any reports, and what controls are in place to prevent dissemination to improper persons or for forbidden purposes.

The forensic analysis should be done at the request of counsel so that the attorney-client privilege may be available to protect the results of the investigation from disclosure. That said, the analysis should be done under the assumption that third parties will have access to the work papers and the final report. For example, Iowa and many other states require that a decision to not notify must be documented in writing and maintained for five years.[10] Of course, if the decision is made to provide notice, then the company likely will want to claim privilege over this work.

The forensic analysis must be completed quickly. If notice is required, then the company must meet the timing obligations for such notice. For example, under Ohio law, notification must be made "in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system. . . ."[11] As a result, the focus of the study must be clear and controls must be put into place to prevent the investigation from losing sight of the main goals of the study. Indeed, the goals of the forensic analysis should be clear and direct: (1) determine if PII was accessed; (2) determine the target and mode of the attack; and (3) determine whose information may have been accessed. Regular meetings with the forensic team are essential. In my experience with system breaches, the answers to these questions often are complex, as data is stored in different places throughout a company's systems. In analyzing a laptop matter, the difficulty is in recreating what was on the lost laptop.

At the conclusion of the investigation, the team must consider all factors in deciding whether notice is required. Often there are close calls to be made. Although the standard is not clear or uniform, a reasonableness standard seems to have emerged. Ultimately, you want to give consumers notice so that they can protect themselves, or if they have already been victimized, then they can have some knowledge as to how it happened. Consumers can then take advantage of the assistance offered in the notice to protect them and remedy any potential harm. In the end, you should follow the Golden Rule—would you want to be notified if it was your information in the system?

The question of whether notice is required after a security breach should be given careful consideration. Over-notification likely has defeated the purpose of breach notices. Aligning the law with the proper investigation of the facts will allow you to make the correct decision. ◆

Endnotes

1. Ronald I. Raether, *Security Before and After a Data Breach*, Bus. L. Today (Nov./Dec. 2006).

2. Mike Hassell, *ChoicePoint: More ID Theft Warnings*, CNN.com, Feb. 17, 2005, *available at* http://money.cnn.com/2005/02/17/technology/personaltech/choicepoint/index.htm.

3. Bob Krenek, *Are We Suffering from Breach Notification Fatigue*, May 3, 2011, *available at* www.experian.com/blogs/data-breach/2011/05/03/are-we-suffering-from-breach-notification-fatigue/ (last visited June 30, 2011).

4. Ed Oswald, *Sony Sued Over PSN Data Breach, Failure to Disclose*, PCWorld.com, www.pcworld.com/article/226478/sony_sued_over_psn_data_breach_failure_to_disclose.html (last visited June 30, 2011).

5. G. Martin Bingisser, *Data Privacy and Breach Reporting: Compliance with Varying State Laws*, 4 Shidler J. L. Com. & Tech. 9 (Feb. 25, 2008), *available at* www.lctjournal.washington.edu/Vol4/a09Bingisser.html (last visited June 30, 2011).

6. Nev. Rev. Stat. § 603A.215(5)(b).

7. Ariz. Rev. Stat. § 44-7501.

8. Fla. Stat. § 817.5681.

9. Ronald I. Raether, *Data Security and Ethical Hacking: Points to Consider for Eliminating Avoidable Exposure*, Bus. L. Today (Sept./Oct. 2008).

10. Iowa Code § 715C.1-2.

11. Ohio Rev. Code § 1349.19(B)(2).