# Actuaries, Data Security, and *Hill Street Blues*

Imagine sipping your Starbucks one morning and reading this headline: "Court Awards <*insert painfully large dollar amount*> for Privacy Violation. <*Insert your firm's name*> to Appeal."

It really could happen to you or your employer—or both. Many otherwise upstanding companies that never expected to be associated with that type of headline have been found guilty of violating customer privacy. A quick Internet search revealed the following recent U.S. privacy violations:

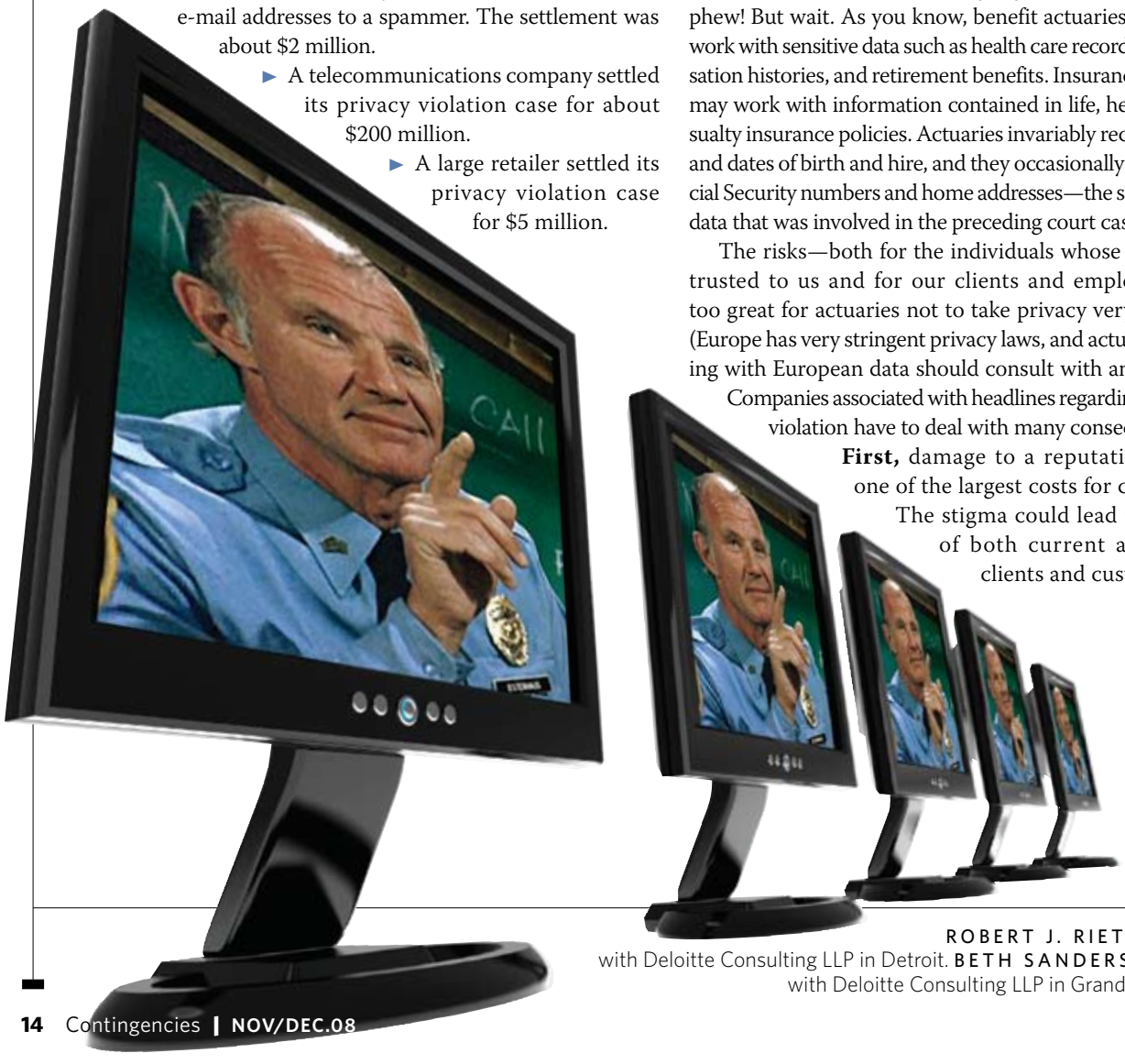
- A bank lost data regarding 4,500,000 customers, including names, birth dates, Social Security numbers, and bank account information, when a third-party storage company lost a backup tape. The settlement is yet to be determined.
- A financial services corporation lost almost 50,000 names, addresses, birth dates, and, in some cases, Social Security numbers, when a disk was stolen from a vendor. The settlement is yet to be determined.
- A web browser employee sold almost 100,000,000 e-mail addresses to a spammer. The settlement was about $2 million.
- A telecommunications company settled its privacy violation case for about $200 million.
- A large retailer settled its privacy violation case for $5 million.
- A large retailer lost data related to 45,000,000 credit card holders, which, in some cases, included driver's license numbers. The settlement amount is yet to be determined.
- A hacker broke into a credit card processor and obtained personal financial information on over 150,000 of its customers. The settlement was about $15 million.

Glancing through this list, we noticed that no insurance companies or benefit consulting organizations are listed—phew! But wait. As you know, benefit actuaries frequently work with sensitive data such as health care records, compensation histories, and retirement benefits. Insurance actuaries may work with information contained in life, health, or casualty insurance policies. Actuaries invariably receive names and dates of birth and hire, and they occasionally receive Social Security numbers and home addresses—the same type of data that was involved in the preceding court cases.

The risks—both for the individuals whose data is entrusted to us and for our clients and employers—are too great for actuaries not to take privacy very seriously. (Europe has very stringent privacy laws, and actuaries working with European data should consult with an attorney.)

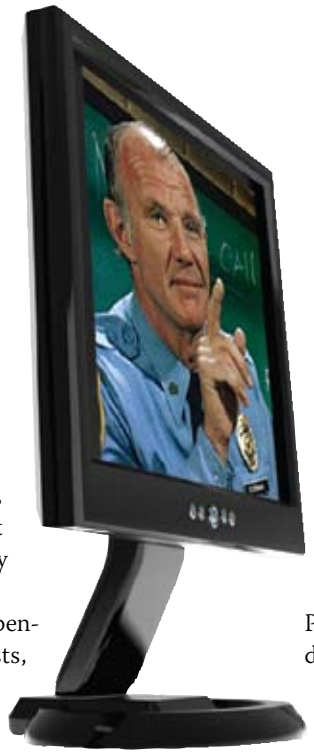
Companies associated with headlines regarding a privacy violation have to deal with many consequences.

**First,** damage to a reputation can be one of the largest costs for companies. The stigma could lead to the loss of both current and future clients and customers.



JOSH RESNICK / SHUTTERSTOCK, NEWS.HEREISTHECITY.COM, BONOTOM STUDIO

**ROBERT J. RIETZ** is a director with Deloitte Consulting LLP in Detroit. **BETH SANDERS** is a manager with Deloitte Consulting LLP in Grand Rapids, Mich.



**Second,** resources dedicated to gathering information about the privacy breach, communicating with those harmed, accommodating the inquiries of other customers, and addressing the failure that caused the breach, are only some of the internal costs.

**Third,** actual monetary expenditures include litigation costs, voluntary payments such as free credit monitoring to those affected, and damages awarded by a court due to class action lawsuits. Clients may attempt to seek damages from a consulting firm or insurance company if they were involved.

**Some readers may remember television's Sgt. Phil Esterhaus of *Hill Street Blues*. He was the duty officer on that program and closed every roll call with, "Hey, let's be careful out there." Actuaries would be wise to heed Esterhaus' warning.**

### Proactive Protection

How can we avoid making headlines regarding a privacy violation? Recognizing that the majority of security breaches occur from a virtual hacker or physical theft of personally identifiable information (PII), mitigation practices include the incorporation of policies, training, and regular monitoring in the following five areas.

**1. Collection:** Collect aggies, cats-eyes, steelies, or oxbloods, but don't collect personal data unless it's absolutely necessary. The actuary should address the collection of data with the data provider at the beginning of all engagements. Engagement letters should specify that the client agrees not to provide health information protected by the Health Insurance Portability and Accountability Act of 1996 or information protected by state laws that might otherwise apply, such as Michigan's Social Security Number Privacy Act or California's Privacy Act. Further, if the client does provide unnecessary private information, the actuary should return it and delete all traces of it from the employer's storage structure.

**2. Storage:** We store bagels in paper bags and money in the bank. Likewise, we should store PII appropriately. Proper storage of personal data can mitigate the risk that it will be stolen or lost. First, encryption, the conversion of data into ciphertext that cannot be easily viewed by unauthorized people, is a common approach. Second, given that network access is regulated and laptops all too frequently are stolen, it's generally more secure to store data on networks rather than on laptops. Third, older or internally developed software should be checked for its security.

**3. Usage:** Children love to pass on secrets, but we must think before we share private information. How many actuaries have disclosed participants' names and other personal information in a supplemental executive retirement plan or long-term disability report? Further, actuaries may utilize a subcontractor who needs access to PII from time to time. In this case, the actuary should ensure that there is a written privacy contract with the subcontractor and that the contractor has (and follows) a privacy policy. If, for example, an actuary provided benefit-statement information to a vendor responsible for producing the benefit communications and a privacy violation occurs, a court might find the actuary at fault if a written privacy contract didn't exist.

**4. Transportation:** It takes planning to transport your kids to soccer and T-ball games or yourself to a Caribbean island; similarly, personal information shouldn't be transported without proper planning. The majority of privacy breaches occur during the physical transportation of data. Devices, such as a password-protected thumb drive, can keep information secure when transportation is necessary. Rather than communicate private information in the text of an e-mail, put the information into a secure e-room or in a protected attachment with the password provided orally to your contact. Also, sending the information in a Zip file makes it very difficult for a scanner to intercept your e-mail, even without a password (which of course you would use anyway).

**5. Destruction:** While you wouldn't destroy your child's sand castle and you regret destroying your sister's Cabbage Patch doll, be sure to destroy PII as soon as possible. Every firm should have a record-retention policy specifying how long data must be kept to comply with legal and professional standards. But having a policy isn't enough; a system should be in place so that the PII is destroyed in conformance with the policy. Having a policy and not abiding by it may be worse than not having a policy at all.

Actuarial firms have been spared from large privacy damage awards so far. (We have been the targets of other types of litigation, but that's the subject of a different article.) Some readers may remember television's Sgt. Phil Esterhaus of *Hill Street Blues*. He was the duty officer on that program and closed every roll call with "Hey, let's be careful out there." Actuaries would be wise to heed Esterhaus' warning. ●

This article is solely the opinion of its authors. It does not express the official policy of the American Academy of Actuaries; nor does it necessarily reflect the opinions of the Academy's individual officers, members, or staff.