

BY WILLIAM A. MCCOMAS

Anyone who has been observing Congress' response to recent data-security breaches at U.S. corporations would never believe the era of big government ever ended.

After ChoicePoint revealed that data on 145,000 people had been effectively stolen, a sizable legislative snowball began rolling down Capitol Hill. The hundreds of pages in proposed bills now on the table suggest our legislators believe the federal government is capable of telling corporate information officers coast to coast how to do their jobs.

Certainly, the widespread breaches of computer security constitute a public problem meriting a federal response. When the personal data of millions are exposed by hackers, identity theft becomes a very real threat to potential victims. A 2003 Federal Trade Commission survey estimated that in a one-year period nearly 10 million people became victims of identity theft.

What is troubling, though, about the congressional response to the many high-profile break-ins of 2005 (in addition to ChoicePoint, targets have included Citibank, T-Mobile, LexisNexis, and Bank of America) is that it fails to recognize the true nature of the threat. To varying degrees, the bills now being considered reveal a naiveté about the current state of corporate data security and the government's capacity to regulate it.

## REGULATING SECURITY

Of the many bills proposed in the House and Senate, one appears to have gained traction, the Identity Theft Protection Act, co-sponsored by Senate Commerce Committee Chairman



To prevent identity theft,  
Congress should focus on  
banking and credit card industries.

## Weak Links

Ted Stevens (R-Alaska) and co-Chairman Daniel Inouye (D-Hawaii). With bipartisan backing, the act sailed through that committee in late July, and some form of it may well reach the president's desk in the coming months. This bill and other proposals similar to it set the stage for sweeping federal regulation of how companies secure sensitive data.

In particular, the Identity Theft Protection Act gives the FTC a year to promulgate regulations that would require any company or organization that stores sensitive personal data to "develop, implement, and maintain an effective information security program that contains administrative, technical, and physical safeguards for sensitive personal information."

That sentence alone is a red flag. Any proposed statute that tries to regulate security standards should die on the proverbial vine. Network security evolves faster than the FTC could promulgate and enforce its own dress code, much less information technology regulations for all of corporate America. But set that point aside and consider a fundamental tenet of computer security: A 100 percent secure network does not exist. As they say in the security industry, the only secure system is

one at the bottom of the ocean without any connections.

Our societal reliance on computer networks has given birth to two fiercely competing camps, one made of white-hat security experts, the other of their black-hat hacker twins. Unfortunately, the black hats are winning. Security breaches occur not once in a blue moon but daily, in all sorts of organizations—from large banks to universities to data brokers—and they are not always detected by the targets.

The consensus in the security industry is that in recent years hackers have become more sophisticated, mercenary, and skill-

ful at beating companies to the punch. Many white-hat IT professionals rely on daily warnings issued by security experts to alert them about specific system, encryption, and transmission vulnerabilities. IT departments rush to implement fixes, but often the hackers have the same information and can exploit the vulnerabilities before corporations can defend themselves.

Compounding the general problem is the prevalent use of remote-access connections. Mobile computing, essential for many organizations, multiplies the vulnerabilities found in a system. Hackers sitting in a wireless “hot spot” can gain access to an employee’s laptop or can hack a wireless provider’s servers, such as in the case of T-Mobile, where a black hat was able to download sensitive government documents. As always, the more useful our technologies become, the more vulnerable we are to digital trespass.

Into this fast-changing world of computer security marches the Senate Commerce Committee, demanding that any organization with personal information floating in its network take “reasonable steps” to protect such data. The result is predictable. Should the bill become law, the FTC will spend a year preparing regulations that will be difficult to understand and more difficult for the government to enforce, especially given that the bill allocates only \$1 million a year for the next four years to carry out the law.

Meanwhile, the very companies whose data is being hacked are already spending millions of dollars and taking countless steps, reasonable and unreasonable, to defend their digital citadels from assault.

## NOTIFICATION

But even if we foolishly assume that the FTC’s promulgations and enforcement measures could drastically improve corporate data security, there is little reason to believe the identity-theft epidemic would recede in equal measure.

Check and payroll fraud, stolen credit card numbers and PINs, e-mail “phishing” scams, spyware on home PCs, scanning computer monitors (with infrared readers or precision binoculars), and old-fashioned dumpster diving are examples of the varied means that identity thieves use to conduct business. None of these methods requires hacking a company network, nor are they even addressed in the proposed legislation.

Corporate data security is one piece in the puzzle, but many of the proposals go well beyond calling for IT standards. The Identity Theft Protection Act, for instance, states that a company made aware of a security breach putting 1,000 or more people at risk must notify the FTC, consumer reporting agencies, and the affected consumers.

This provision mirrors the California notification statute often credited for forcing ChoicePoint to confess its data-security sins. In that it provoked debate of this dire problem, the notification law proved valuable for its educational purposes. But as a federal statute applicable to all companies, a notification requirement would likely become ineffective. Its underlying premise—that companies know when they’ve been hacked—is simply not applicable to all network break-ins.

But give the proposal the benefit of the doubt and assume that all hacks were detectable, that the FTC would be able to enforce

the law, and that companies would obey it. In such a world, alarm bells of security breaches would be ringing so often the public would become desensitized to the threat.

Even if such alarm bells did raise general concern about identity theft, these notifications would not prevent data thieves from ripping people off. If a company has 90 days from the date of detection to report a break-in, as the bill stipulates, by the time the consumer hears word of it and takes protective action, the damage will likely have been done. The thief will have bought thousands of dollars worth of goods, flown to Cancun, or obtained several new credit cards.

In essence, a notification component would do little to stop identity theft. It would simply give consumers a false sense of security and require companies to waste money preparing and delivering notices to potential victims, rather than using financial resources to fight hackers.

## SOLUTIONS?

That said, Congress can take effective action if it directs its energies with precision, rather than with a broad brush.

To begin with, lawmakers should establish programs designed to educate consumers on how to mitigate the risk of identity theft and should grant consumers greater access to, and control of, their credit reports and financial information. The Identity Theft Protection Act takes a laudable step in this direction. It would allow a consumer to place a “security freeze” on his or her credit record, thus requiring reporting agencies to obtain the consumer’s authorization before releasing the record to a third party. It is just this kind of feasible, targeted measure that the identity-theft epidemic calls for.

Secondly, lawmakers should acknowledge that there is an elephant in the room: the banking and finance industry. Congress seems intent on shifting responsibility for identity theft to organizations nationwide while taking no action against the very industry whose practices most enable the problem.

Our culture’s thirst for easy access to credit has superseded all other considerations in the cutthroat financing industry, which has significantly reduced protections in the credit-approval process. Banks are able to reap fees for financing while pushing the risk of fraud upon their customers and merchants, which are often forced to eat losses resulting from identity theft. Today, if a credit card owner disputes a purchase made with his or her card, his or her liability is typically limited to a nominal amount. But the card issuer will then trigger a “chargeback,” by which the bank sticks the merchant with the cost of the purchase plus a chargeback fee. Thus, the financial institutions go unscathed.

Congress needs to bring some sane safeguards back into the process of approving credit—even if they add costs and inconvenience to the powerful banking and financial institutions.

Financiers should have to take greater care to confirm that applicants are who they purport to be at the time an account is opened as well as periodically during the life of the account. One means of confirmation would be requiring that applicants apply for credit in person with photo identification. Banks should also be required to audit each account regularly, monitoring it for patterns indicative of fraud. If given teeth, such steps

would indeed be troublesome to the financial industry, but they amount to more focused, effective, and enforceable regulatory prescriptions for the ailment Congress seeks to remediate.

In the same vein, Congress should consider mandating better communication and information sharing among financial institutions concerning fraudulent activity. Because banks don't always communicate with one another about problematic accounts and their associated addresses, an identity thief is able to rack up fraudulent charges with one bank and then quickly shift to another using the same victim's information. If banks shared these data with one another and with merchants, thieves couldn't get away with this ruse so easily.

Finally, Congress should consider curtailing the widespread use of Social Security numbers and introducing one or more new, unique identifiers. The Social Security number, as many of the proposed bills recognize, has become too ubiquitous and valuable to thieves. New, unique identifying numbers (i.e., one for use in financial transactions, another for driving information,

and so on) would make identity theft more difficult to pull off. They would allow industry and government to make data-security protections more sophisticated and harder to crack while preserving the ability to continue data mining.

Such steps may seem like radical reform, but they are minor compared with the enormous regulatory weight the Senate's Identity Theft Protection Act would place upon nearly every company in the nation. The act's attempt to regulate corporate security standards is overly ambitious, costly, and likely to reap little reward for the public.

Ultimately, the problem is not about data theft but fraudulent use of that data. Congress should train its sights on access to credit and consumer protections.

---

*William A. McComas, a former software engineer, is a partner in the Baltimore office of Shapiro Sher Guinot & Sandler. McComas concentrates on technology law and can be reached at [wam@shapirosher.com](mailto:wam@shapirosher.com).*