CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 159 years

THURSDAY, NOVEMBER 20, 2014

Chicago Daily Law Bulletin®

Volume 160, No. 229

Technology may reduce fraud but doesn't fix regulatory confusion

President Barack Obama recently announced the administration's BuySecure initiative. At a meeting at the Consumer Financial Protection Bureau Oct. 17, the president outlined the program, aimed at increasing the security of sensitive financial information and enhancing protections against fraud and identity theft.

As part of the BuySecure initiative, the president signed an executive order mandating the federal government's adoption of chip-and-PIN credit and debit cards beginning next year. Chip-and-PIN credit and debit cards are part of a payment system in which cards contain a computer chip and the user must enter a personal identification number when using the card.

The executive order will force the federal government to adopt chip-and-PIN technology for government payment cards and to outfit retail point-of-sale terminals at federal facilities — such as national parks and post offices — with the capacity to accept chip and PIN-enabled cards.

In addition to requiring that federal agencies use and accommodate chip-and-PIN cards, the order pledges support to the Federal Trade Commission in developing reporting and remediation resources for identity-theft victims and directs greater information sharing to improve how evidence of security breaches is reported. The administration also announced that it would be hosting a Cybersecurity and Consumer Protection Summit later this year, bringing together major stakeholders in the public and private sectors to discuss best practices and next-generation technologies.

The executive order appears designed to signal that the administration is sensitive and responsive to consumers' mounting concerns about data insecurity, but as those following privacy law know, the regulatory landscape is an ever-growing patchwork despite the near-constant news of breaches. Every few days, it seems, another company announces that customer information has been compromised in some way. Some of the most high-profile breaches have involved prominent national retailers such as Target, Neiman Marcus and Home Depot, but breaches occur across all sectors.

Financial giant JPMorgan Chase recently disclosed that hackers had accessed the contact information of 76 million households and 7 million small businesses. The information disclosed in these breaches varies — the JPMorgan Chase breach, for example, did not compromise financial information or result in the hackers gaining access to client accounts.

And even where credit card information is involved, the effect on most customers often may be the inconvenience of acquiring a new card. That said, the harm to identity-theft victims is real, and the costs to companies significant, even if the hacked information is never exploited for fraudulent purposes.

From a business perspective, breaches of customer information not only present the potential for reputational harm (and lost sales), they cost money and time notifying customers and governmental agencies of the breach.

All but three states have data-breach notification laws on the books, and 2014 has seen a flurry of bills in statehouses across the country as legislatures contemplate additions and amendments to existing consumer protection laws. State laws contain a wide variety of differing provisions on breach notifications, including which businesses are covered, what constitutes a breach, what personal information must be compromised to trigger the statute and when notification must be given. They also incorporate a variety of exemptions and exceptions.

California's statute, for example, specifies a lengthy list of information that must be included in any data-breach notification. Some states create private rights of action; others do not. Some exempt notifications for immaterial breaches; others do not. California recently enacted an amendment to its notification law requiring a notifying company that was "the source of the breach" to bear the costs of any identity theft and mitigation services it offers to affected customers. While the bill ultimately signed by Gov. Jerry Brown had less bite than earlier versions advanced by consumer groups, the law's enactment is expected to spur similar cost-shifting legislation elsewhere.

In this environment, what can — and should — businesses do? Although companies need to stay informed about requirements in the states where they do business, many larger companies are adopting best practices engineered to navigate the patchwork of state laws by complying with the strictest state provisions while anticipating how these laws are trending.

Plenty of federal privacy and data security bills have been proposed, but Congress has failed, somewhat conspicuously, to reach consensus and enact any federal legislation in this area. And while a federal blanket may seem to be a better solution than the existing patchwork quilt of state laws, a comprehensive federal plan will help only if preemption is broad and clear. Simply adding an extra layer of requirements, without assuring that divergent state laws will be pre-empted, will just make compliance more onerous.

The administration's BuySecure initiative doesn't propose a federal solution to the patchwork problem. It acknowledges public frustration with existing data security measures, focusing particularly on payment systems and identity-theft protection and remediation measures. By requiring that the federal government shift to chip-and-PIN cards (and systems enabled for those cards) in 2015, the executive order advances the public sector in the direction where the private sector is already moving.

Some of the country's retail giants, including Wal-Mart, Target, Walgreens and Home Depot, will activate chip-and-PIN support in their in-store credit card devices by January. (The devices are already installed but in many stores have not yet been activated.) This planned migration actually has been in the works for years, with MasterCard and Visa, as well as other larger retail companies, planning for the shift next year.

Although the credit card companies have pledged to support smaller businesses in adopting chip-and-PIN-enabled devices, the migration will be costly — and will not completely eradicate credit card fraud. Hackers are renowned for adapting their methods to shifting technology. But these cards do provide extra protection to users.

New secure payment systems are also being introduced — Apple Pay is one notable example — and it remains to be seen how those technologies will fare in practice, over time, as the field of users expands and hackers have more of an incentive and opportunity to detect vulnerabilities. Meanwhile, the administration's Cybersecurity and Consumer Protection Summit aims to provide a forum for private and public stakeholders to engage in productive dialogue on these issues.

PRIVACY, TECHNOLOGY AND LAW

NERISSA COYLE MCGINN

Nerissa Coyle McGinn is a partner in Loeb & Loeb's Chicago office. She focuses on matters involving the convergence of advertising and promotions, emerging media, technology and privacy law as well as intellectual property law. She can be reached on nmcginn@loeb.com.