

**THIS MONTH'S TOPIC ...**

## Massachusetts' Battleground for Consumer Protection

### Tough data breach law finds tough opposition

In August 2007, Massachusetts Governor Deval Patrick approved the toughest data breach legislation in the United States. It was an apt response on the heels of the TJX breach, in which hackers reportedly compromised nearly 100 million consumer financial records. Consumer advocates extolled the new law and encouraged other states to take heed and confront the obvious threat that, to this day, has only shown signs of worsening.

Unfortunately, the Massachusetts law hasn't had a clear path to its realization. In the face of protests from business owners claiming they could not afford or were otherwise unprepared to comply with the law, the January 1, 2009 effective date was pushed back—twice—to January 1, 2010. Some business leaders are still fighting the implementation of the law. This month, we cover the [dispute between business leaders and consumer advocates](#), examine the [salient points of this landmark law](#), and propose exactly [why businesses can't afford to ignore it any longer](#).

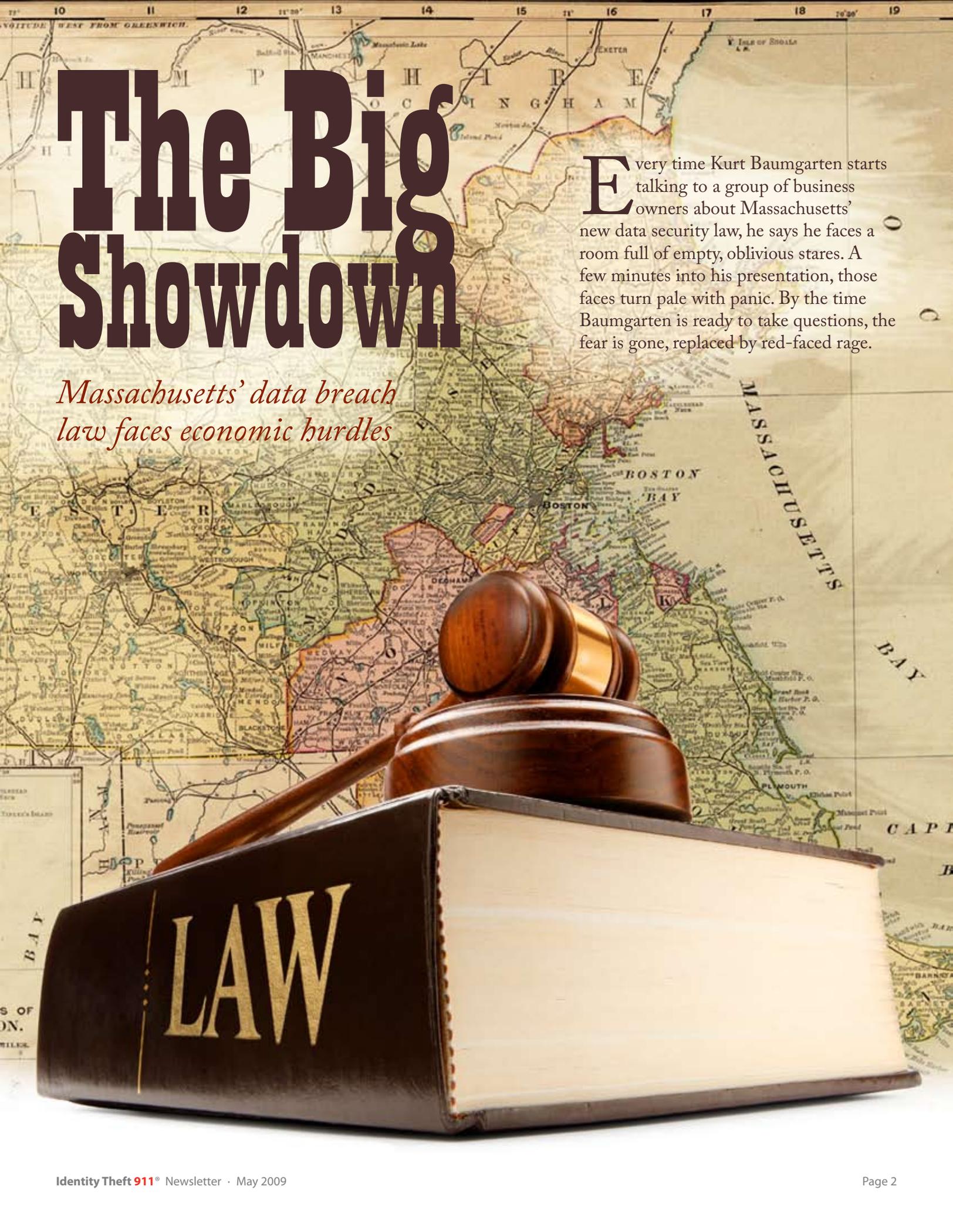
For a complete newsletter archive, visit: [www.identitytheft911.org/newsletters](http://www.identitytheft911.org/newsletters)

To learn about the latest scams on identity theft, visit: [www.identitytheft911.org](http://www.identitytheft911.org)

Comments, questions? Contact us: [media@identitytheft911.com](mailto:media@identitytheft911.com)

**Another first for  
Massachusetts!**



A vintage map of Massachusetts serves as the background. In the foreground, a wooden gavel rests on a dark brown book with the word "LAW" embossed in gold letters on its cover. The map shows various towns and geographical features, with "BOSTON" and "BAY" clearly visible.

# The Big Showdown

*Massachusetts' data breach law faces economic hurdles*

Every time Kurt Baumgarten starts talking to a group of business owners about Massachusetts' new data security law, he says he faces a room full of empty, oblivious stares. A few minutes into his presentation, those faces turn pale with panic. By the time Baumgarten is ready to take questions, the fear is gone, replaced by red-faced rage.

"To business people in Massachusetts, it's a double-barreled shotgun," says Baumgarten, who travels the state giving lectures about the new law as vice president of information for Peritus Security, a consulting company in the Springfield area. "The legislation is gobbledygook to them. And they don't know where to begin."

## State law, national impact

In August 2007, Massachusetts Governor Deval Patrick signed the nation's most comprehensive data privacy law. The legislation requires companies to secure consumers' private information and prevent it from being lost accidentally or stolen by identity thieves. The rules apply to any company that gathers information about Massachusetts residents, no matter where the company is located.

"This law impacts the entire United States," said Agnes Bundy Scanlan, a Boston attorney and a board member of the International Association of Privacy Professionals.

For American companies, the law's potential impact is enormous. Sprawling computer networks must be encrypted and secured, and heavy fines await companies that fail to comply. Still, many business owners inside Massachusetts have never heard of the new law. The rules originally were scheduled to take effect Jan. 1, 2009. But after intense lobbying by business groups, the Massachusetts Office of Consumer Affairs and Business Regulation postponed the deadline twice, originally to May 1. The law is now scheduled to take effect Jan. 1, 2010.

Massachusetts officials say the delay was needed to reduce the financial impact on companies already hurting from a deep recession.

"We have to bear in mind that businesses are under economic stress as we speak," says David Murray, general counsel for the consumer affairs office. "So to do this balancing of burdening businesses and protecting consumers, we had to give a little."

But people who study the rising threat of identity theft worry that waiting more than three years since the bill's passage may simply be too long.

"Of course there's concern," Baumgarten says. "Because every minute you allow best practices to be ignored for the sake of making a buck, you put more consumers at risk of identity theft and fraud."

## A State Comes of Age

As a consumer advocate for MASSPIRG, a consumer watchdog group, Eric Bourassa started working to help Massachusetts residents safeguard their private information 15 years ago when he lobbied for what was then an innovative idea: Free credit reports for consumers. Next he helped the state pass a law requiring companies to notify customers whose private data is compromised by a security breach.

*"Legislators started saying to me, 'Well gee, breach notification and credit freezes only work after your information has been lost or stolen,'" Bourassa says. "What about preventing it from being stolen in the first place?"*

Then, in late 2006, Massachusetts played host to one of the worst data breaches in history. Identity thieves hacked into TJX, the parent company of clothing retailer TJ Maxx, headquartered outside Boston. The hackers stole tens of millions of customer records. A leader of the theft ring, Maksym

Yastremskiy, ran up \$11 million worth of fraudulent charges on the stolen credit accounts, according to a federal indictment.

Lax security at TJX was partly responsible for the breach. The company transferred millions of customers' names and credit account

numbers over unsecured wireless networks, without encrypting the data. The failure was stunning, but not illegal. "When TJX happened, the state could do nothing," Baumgarten says. "The attorney general found himself [unable to act] because we didn't have any laws in place to cover something like this."

The scale of the attack fundamentally changed the privacy debate in Massachusetts.

"Legislators started saying to me, 'Well gee, breach notification and credit freezes only work after your information has been lost or stolen,'" Bourassa says. "What about preventing it from being stolen in the first place?"

So Bourassa helped the legislature write a privacy law that is the first of its kind in the United States (though similar policies are now commonplace across Europe). The idea was simple: if companies want to collect large amounts of our private data, the onus rests with them to protect it.

"The business community wants it both ways," Bourassa says. "They want to collect all this information on us, but they don't want the liability if something goes wrong."

## Few details lacking

That basic insight led to the most comprehensive data security law in the country. The law defines private data as a resident's name plus either a Social Security number; driver's license number; credit, debit or financial account number; or PIN access code. Companies that gather such a combination must designate at least one employee to implement a data security program.

"If you're a small business owner, sorry, that's probably you," says Randy George, a columnist for InformationWeek magazine.

The law's major components require companies to identify the internal and external risks to their paper and electronic records. They must restrict

employee access to those documents on a need-to-know basis, encrypt private data whenever it is transferred or stored on laptops or PDAs, train employees about secure record management, discipline people who break the rules, and audit the program annually.

All of this leaves some business leaders feeling overwhelmed.

"[M]any employers are frustrated with the confusing regulatory wording and the complexity of technological and legal issues," Bradley MacDougall, lobbyist for the Associated Industries of Massachusetts, a trade group, said in testimony before the state consumer affairs office in January. The industries organization did not respond to calls seeking comment for this article.

The reaction among technical experts has been quite the opposite.

"This isn't rocket science," says Nagraj Seshadri, marketing manager at Utimaco, an encryption firm based in Foxboro, Massachusetts. "When you ask a technical guy about this law, it absolutely makes sense."

## Sticky wickets

When it finally does take effect, the data security law will differ from the version originally signed by Governor Patrick. The original version required companies to encrypt all sensitive data with at least 128-bit encryption. Business leaders worried the rule would require them to spend big on technology that soon will be out of date, because encryption standards grow higher as criminals become more sophisticated.

"This is an arms race with the bad guys," Seshadri says.

The consumer affairs office agreed to loosen the wording, instead requiring that companies encrypt data enough to render it unreadable.

Another area of concern was subcontractors. Legislators and state regulators worried that companies

might avoid the new law by hiring third-party companies to manage their data, Murray says. So the original law required businesses to certify that their subcontractors comply with the law, too.

Business leaders howled at the idea. "This is one of the most troubling aspects of the regulations," MacDougall said. "[M]any firms outside of Massachusetts or globally are completely unaware of these rules. Regulated parties under these rules will face a significant economic disadvantage." Here the regulators compromised again, requiring only that companies take reasonable steps to assure that vendors are able to comply with the law.

But the biggest concern was the deadline. In near unanimity, business leaders said they simply could not make all the required changes by January 1, 2009. The consumer affairs office first moved the deadline back five months, then by a full year. Still, MacDougall said, the deadline "does not provide sufficient time for public and private entities to become aware of the new regulations, to know what compliance really means and then to locate appropriate resources for the necessary investments required by these regulations."

Though the law's supporters worry that postponing enforcement could leave Massachusetts residents exposed, they fear more that forcing the pace could cause additional problems.

"If you do this in a cavalier fashion, you drive up the number of people who will simply ignore the law," Murray says. By moving the deadline back, "you're not diminishing the protections, you're increasing them."

Of course, the business community also raised another important issue, one that remains unsolved after months of wrangling: the government itself. The

state of Massachusetts is exempt from its own tough law.

"The regulations do not equally apply to the public sector," MacDougall said. "Therefore, can a firm continue to conduct business with the State of Massachusetts if several of the agencies do not accept encrypted data?"

## Broad reach

Even after the compromises and delays, the data security law will have nationwide reach because it affects any company in the U.S. with customers in Massachusetts. Another factor broadening its likely impact: states have a history of following the leader on privacy laws. California's move in 2003 to enact the first breach notification law was followed quickly by 44 other states. Legislators and consumer affairs officers in California, New Jersey and New York have discussed or introduced legislation similar to that in Massachusetts.

"Other states are paying close attention to this legislation," says Bundy Scanlan, who recently spoke about the law at a convention of resort developers in Orlando, Florida.

In the long run, however, data security experts believe that calls for change may come less from state governments than from the private sector, which is beginning to realize that protecting customers' private data protects the bottom line.

"Companies should be doing this stuff anyway because these are best practices for preventing identity theft, which is a booming, billion-dollar business," Baumgarten says. "There's no reason not to follow best practices because otherwise your reputation and your business will suffer." ■

*"This isn't rocket science," says Nagraj Seshadri, marketing manager at Utimaco, an encryption firm based in Foxboro, Massachusetts. "When you ask a technical guy about this law, it absolutely makes sense."*

# Major Components of the Massachusetts Data Security Law

The new data security law in Massachusetts is unique for its broad scope and specific detail about what companies must do to protect consumers' private data. Here are some of the key aspects of the law. Any U.S.-based company that collects its customers' personal data and has a least one Massachusetts customer must:

- ✓ Designate *at least one employee* to manage data security
- ✓ Identify all the data that the company collects, and *limit the amount of data collected* to that which is reasonably necessary to accomplish a business need
- ✓ Identify all the *internal and external risks* to data security
- ✓ *Encrypt all sensitive data* that is sent electronically or stored on laptops or other portable devices
- ✓ Install and regularly update *computer firewall and security software*
- ✓ Create a *Written Information Security Program* (WISP), which lays out:
  - What sensitive data the company collects
  - Describes controls that limit employee access to sensitive data on a need-to-know basis
  - System of individualized passwords or other devices that track users of computer or paper records
  - Training for employees on security procedures, and disciplinary measures for employees who break the rules
- ✓ Take reasonable steps to ensure that all *third-party service providers* with access to the company's sensitive records comply with the Massachusetts law
- ✓ *Audit* the system at least annually

# No Rest *for the* Wicked

## *Businesses can't afford to push back landmark law*

Consumers and privacy advocates rejoiced in August 2007, when Massachusetts Governor Deval Patrick signed the toughest data security law this country has ever seen. Finally, a state had looked into the belly of the beast—a rising tide of data breaches, increasingly sophisticated identity thieves, more consumers victimized—and decided: No more. If Congress and the other 49 states failed to take this problem seriously, Massachusetts would lead by example.

And then we waited. And waited. Now we're waiting some more. The law originally was supposed to take effect on January 1, 2009. The business community objected, saying that Massachusetts companies were simply incapable of meeting the deadline.

So regulators compromised, moving the deadline back to May 1. Companies claimed it still wasn't enough time, so enforcement now is scheduled to begin on Jan. 1, 2010. As for whether that date will stick, consider this: For most companies, complying with the state's data security law will require some new capital investments at a time when businesses, like everyone else, are

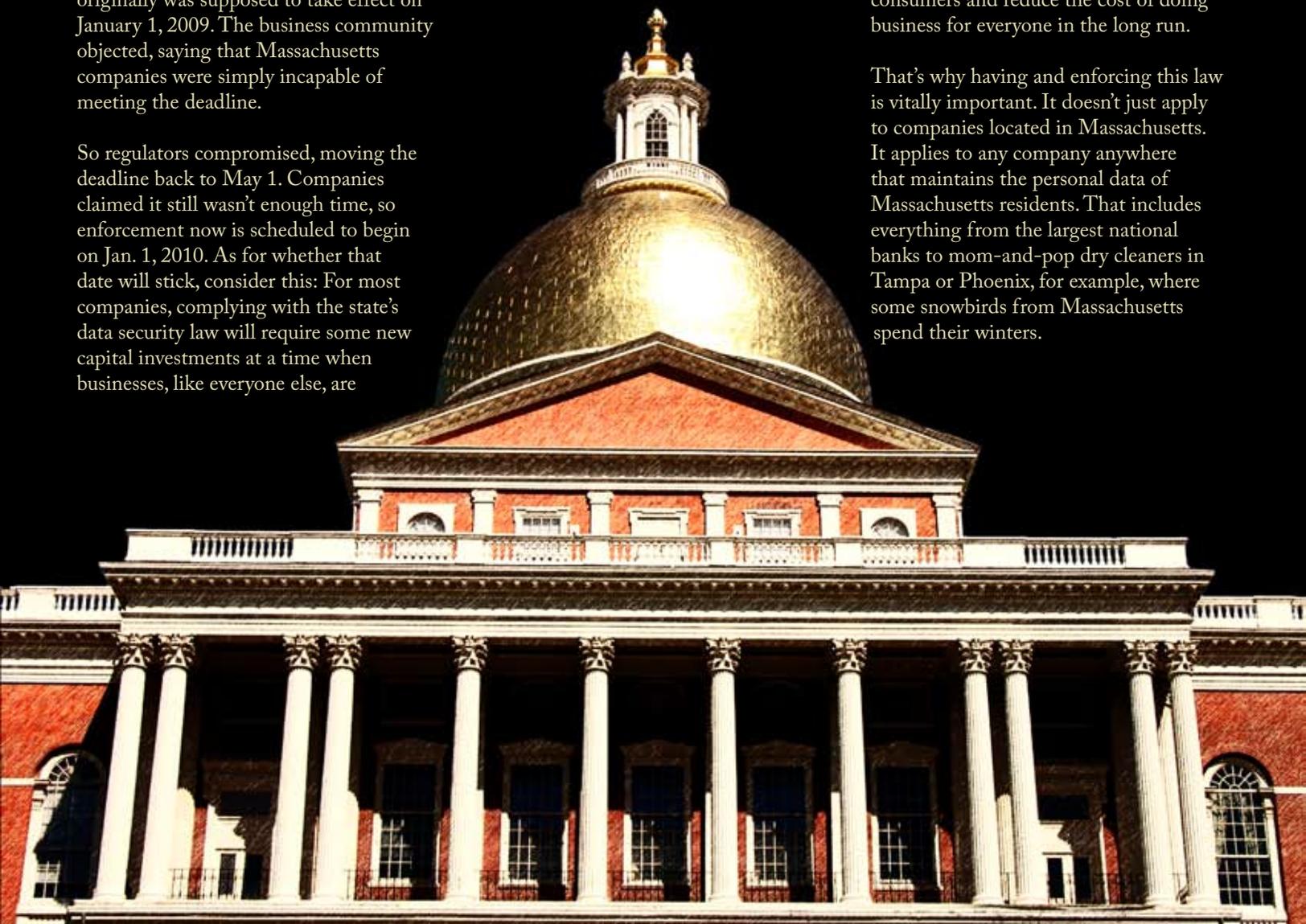
struggling to survive in the current recession. So companies in Massachusetts are lobbying hard for yet another extension.

This must not happen, as it is precisely during the depths of a recession that consumers are most at risk of identity theft. As businesses across America shed jobs, disgruntled or even desperate former employees (many of whom are facing potentially indefinite unemployment) have unprecedented incentive to exploit access to internal computer systems and steal consumers' private data for the sake of personal financial gain.

As consumers reach the limits of their credit and begin to default, foreclose, or go bankrupt, some may grasp at any solution to salvage their finances. Such desperation makes them more susceptible than ever to fraudulent refinance options offered by identity scammers who are mining for every scrap of consumers' personal financial data.

As business lobbyists attest, truthfully, to the pain this recession, more state legislatures around the country may back away from writing new data security regulations that cost businesses money in the short term, even if those laws protect consumers and reduce the cost of doing business for everyone in the long run.

That's why having and enforcing this law is vitally important. It doesn't just apply to companies located in Massachusetts. It applies to any company anywhere that maintains the personal data of Massachusetts residents. That includes everything from the largest national banks to mom-and-pop dry cleaners in Tampa or Phoenix, for example, where some snowbirds from Massachusetts spend their winters.



The law also is important because it shows other states the way. Instead of a broad and generic mandate, the legislation is specific and comprehensive. It goes deep, laying out exactly which steps companies must take to evaluate the risks to their stores of personal data and create a detailed plan for keeping data safe.

Trade association lobbyists may complain now about how onerous it is to comply with such a law. But in the coming years, other states are likely to try to improve data security while giving companies more flexibility. In those cases, businesses will find themselves financially liable for failing to secure private data but they will have no roadmap to follow, no documents to hold up in court and show how they tried to comply. If that happens, defendants may pine for the safety of Massachusetts' proscriptive law.

And besides, Massachusetts' new safety measures are not so outlandish as the lobbyists would have us believe. Any information technology professional worth the title knows that the law merely follows best practices for data security, which have been used by many companies for years. These rules include such basic concepts as knowing what data you collect in the first place. Encrypt that data, and make sure that only employees who need it to perform their jobs have access to it. As Nagraj Seshadri of the

Foxboro, Massachusetts encryption company Utimaco says in this newsletter, this is not rocket science. It's simply good business.

The business community does make some valid points, however, which are important for privacy and consumer advocates to remember. Perhaps the lobbyists were correct that the original deadline was too soon. Rushing into enforcement before many companies had time to comply might have rendered the law useless, since business owners might have simply ignored it. But postponing the deadline cannot be allowed to happen again. If the law takes effect as planned, on the first day of 2010, it will have been four years since

millions of consumers whose sensitive financial data was compromised in the catastrophic TJX breach, and three years since the law was originally passed. Companies have seen this law coming for a long time. By next January 1, they must be ready.

Business groups also are correct about a major flaw in the Massachusetts law: the state itself is exempt. The government's alphabet soup of bureaucratic agencies collects mountains of personal information every week. Yet those agencies are not required to encrypt

that data, secure its movement, or limit which employees have access to it. For all businesses are required to do to shore up data security, this still leaves consumers wide open to the risk of data breach. It also puts companies in an interesting position. Businesses must assure that third-party subcontractors manage data in accordance with the law. Does that mean companies are now barred from handing data over to the state? Obviously, this is more of a hypothetical question. But it points to the thorny issues that arise when lawmakers open such a huge loophole. Their next priority should be to close it.

To celebrate Massachusetts' historic step, we originally planned to publish this newsletter in May. When we heard the law would be postponed, we considered doing the same. But we decided to move ahead anyway, hoping to highlight the importance of the law, and to raise awareness that come January, it must take effect. Especially during a recession, identity thieves never rest. Neither can we. ■

*Massachusetts' new safety measures are not so outlandish as the lobbyists would have us believe. Any information technology professional worth the title knows that the law merely follows best practices for data security, which have been used by many companies for years.*

By Adam Levin