NEW YORK STATE INFORMATION SECURITY BREACH AND NOTIFICATION ACT: STATE BREACH NOTIFICATION REQUIREMENTS

Thomas Smith

Thank you. Well, I'll give the introduction. Unfortunately, this is an agency, the New York State Office of Cyber Security & Critical Infrastructure Coordination, many of you may not have heard of. We have the unfortunate acronym of CSCIC. You know, it didn't occur to anybody after they established it in the statute to say, "Oh, my gosh, we're going to be . . . ." So we're thinking about changing it. In the meantime, what we're doing for the State is providing protection for all the data that the State processes and uses in the multitude of activities that the State undertakes. We're protecting the State's information from the bad guys on the internet. So that's intrusion detection and prevention.

We respond to incidents when State agencies have security incidents. We establish policies and standards to help the agencies protect the information that they use. We do awareness and training. We do advisories when, for instance, Microsoft comes out with its monthly advisories and we try to translate those into practical advice for the agencies on how to patch their systems. And we do vulnerability scanning for those applications that the agencies use on the internet.

So just to give you a little sense from our purposes: the current environment is no longer about the teenage hacker, Mountain Dew and Skittles in his bedroom all night trying to hack into your system. It's really turned into a big criminal enterprise. All over the world there are rooms full of people who are in the employ of criminals who work all day trying to get into our systems. They're working at this all day. They don't go home at five o'clock at night. So it's a challenging environment, there's a lot of risk.

People talk about cyber crime, cyber war, cyber terrorism; it's

all kind of blurring together. You may not know why the person is trying to penetrate your system and steal your data, whether it's purely from a monetary motive or they have some other motive. This slide shows five million new threats in the third quarter. People are turning this into a big business. Actually the U.S. Treasury Department came out and said that cyber crime is actually more profitable than illegal drug sales. And as we talked about a little bit before among the panelists, it's actually less risky for a lot of criminals because the penalties for cyber crime don't necessarily correspond to the harm that's being done.

It's a challenging environment. You can go out there and buy credit card numbers on the Internet. Hackers are now targeting public entities, which is a great concern to us because public entities are under a lot budget pressure, they may not have the resources to protect their information. But they do have information and information that can be used to steal money—there's a lot of cyber fraud relating to the banking.

In this environment there are all these cyber threats on government agencies and private companies that hold a lot of personal information. So we get into the area of the breach notification and we go back all the way into pre-history in 2003. As a result of a big breach of personal information of California state employees, California adopted a law requiring that victims of a security breach be notified when that happened, the premise being they need to know so they can respond, they can protect their identity, they can protect their financial accounts. It's an important public policy.

In 2004, ChoicePoint, which is a big data aggregator—they do background checks and they do a lot of credit check kind of work—had a very large breach. Now, the thirty five thousand people in California got a notice because of the California statute. Everybody outside of California was out of luck, they didn't get a notice, which brought this to light and a lot of people including the New York Attorney General said, "Look, you'd better notify everybody." And one of the things that the State did was hold the fact that ChoicePoint had a state contract over its head and said we'll terminate the contract unless you notify New York residents.

ChoicePoint, a very hot button issue, occurred in the same timeframe Designer Shoe Warehouse had a huge breach of one point four million people nationwide. The issue started to

percolate up and so in New York—it being New York—what we really wanted to do was develop a comprehensive, thoughtful approach to protecting people's information in this sophisticated threat environment. What we got was somebody who said that this is an important issue and instead of talking to experts in New York State about the right way to do it in New York State, the response was: let's copy off of California, let's take the California bill and essentially enact it whole, good, bad and indifferent provisions, whether or not they fit in New York.

People said, "Yes, this is an important issue." So the State agencies who were involved in these issues, like the Tax Department and Health Department who hold a lot of personal information—they're going to have to comply with these provisions—said, "Great, we're all for it, but, you know, these ten provisions are unclear, we don't understand what they mean and they're going to be difficult to implement." While the bill was passing in the Senate and the Assembly, the sponsors agreed to go back and make some technical changes, but it really wasn't enough. We ended up with a bill that was better, but it was very difficult for people to understand exactly what they were required to do.

The basic issue is if you have a breach and that's defined, you have to notify the individuals. But as you get into trying to implement practice both for private companies and for state agencies, who are subject to a very similar set of rules that are very difficult to apply and to understand.

New York's statute is only applicable to computerized data, not data on paper. So whether or not you agree that that's an appropriate distinction to be made that, well, if the Tax Department prints out a database and the guy leaves it on the loading dock to be stolen, well, that's not a breach, you don't technically have to notify anyone in New York State for that. That's a matter of public policy, that is, a bigger issue. The statute in New York only applies to computerized data.

In the phraseology of the statute, a distinction is made between "unauthorized acquisition" and "acquisition without valid authorization." Now, I'm not clear, and am still not clear, what the difference between those two things is.

There are some exceptions, but you get down to the core of it, private information in New York is defined as personal information. Basically, your name, your Social Security number, your driver's license or non-driver ID, or an account credit

card/debit card number in combination with a PIN or the password.

So we'll talk about a little bit later there's some holes in this current statue. There is an exception for encryption: if the data's encrypted, no notice to the individual is required. There is an exclusion for publicly available information. Now, again, that's an exception to the notification requirement, but there hasn't been a lot of clarity on what that means.

Now, for me I know that if I went down to the County Courthouse somewhere you could probably find a document that has my Social Security number in it and it would be publicly available. Does that mean somebody wouldn't have to notify me if they had a breach? I don't know. It's a very difficult thing to apply.

Notification is required to the individual whose information is, or is reasonably believed to have been, breached. The notice must occur in the most expedient time possible and without unreasonable delay. Now, some lawyer wrote that, who knows what that means. How fast is that? There are delays for certain purposes and in New York one of the things that's a little different is when an entity that suffers a breach has to notify three different state agencies: the New York State Attorney General, the Consumer Protection Board, and our office.

The statute also sets out what has to be in the notice. There's provision for substitute notice in very large breaches and breaches where the entity says it's going to be so expensive we're going to pursue substitute notice, which might be notice in the newspaper or on the internet. In the incidents where more than five thousand individuals are involved, there's a requirement that the major credit reporting agencies be notified.

A couple of other things, on the private side, which resides in the General Business Law, there's enforcement by the Attorney General who can bring an action if there's a determination that an entity has not complied with the statute. That does not apply to State agencies. There are civil penalties in the General Business Law, but New York State did not set up private cause of action for information security breaches.

So a problem, as I said, is that there's no definition of computerized data. There's no definition of encryption. There's no definition of unauthorized acquisition, a person without valid authorization. Unauthorized disclosure, major state-wide media, that's one of the substitute notice issues—you're supposed to put

the notice in major state-wide media. Now, in New York State does that mean putting it in the New York Times? Is somebody in Albany necessarily going to see it if it's in the New York Times?

Other issues: it's oddly written. It says that public entities other than state agencies are exempt from the statute, but those entities, although are exempt from the statute, had to adopt a policy that was consistent with the statute but in 120 days. So why exempt them if you're going to make them turn around and adopt a consistent policy? As I said, there are a lot of problems with the statute. They can't even decide whether they're talking about personal information or private information, they flip-flop. So it's very difficult.

Again, what constitutes encryption? If you talk to technical people, there's good encryption and there's bad encryption. So there's not really a standard. If you're going to exempt someone from providing the notice required under the statute, you'd think that you'd want to make sure that it was good encryption, that it wasn't easily broken.

So that's what we were left with. Where are we now in three plus years after the effective date of the statute? In 2008, we received 547 notices of breaches which encompassed over two million records of individuals and New York State residents. If you look out on the Internet for other information, there's the Identity Theft Resource Center. They tend to report breaches that are publicized. Some of that you may have seen, they troll the news and they listed 641 in 2008, which included more than thirty-five million individuals.

There's only been one instance of enforcement by the A.G. since the inception by the statute, and it related to a lost laptop. The company waited six weeks to file the notice and they ended up entering into a settlement with the A.G., talked about their privacy practices and they paid for the costs of the enforcement. The funny thing is that the day after they signed the settlement the laptop was recovered. So the question is, well, was it really a breach? But under the New York State Statute, the lost laptop is a reason to believe that the information has been breached.

So breach reporting. Ponemon Institute, which is a big research entity that does a lot of work in this area, they roll out an estimate of how much breaches cost and in the last year the private entities that they surveyed averaged $202 per person's record breached. So that includes a lot of things that go into it.

Doing the forensics to find out who you have to notify, notifying the consumers, whether or not they offer credit monitoring, those are all costs that go into responding to a breach. And it doesn't even go into the reputational costs when an entity has a breach: whether or not people go back and do business with them again.

So up here in Albany, Hannaford had a big breach of four point two million credit and debit cards. The interesting thing was, that for the purposes of the New York State statute, that was not a breach because Hannaford said, "We don't collect the names. We have the credit card numbers, but we don't have any way to connect them back to individuals." So under the New York State statute that wasn't a breach, it was a bad thing, but it wasn't a breach for purposes of the New York State statute. More recently, Heartland Credit Card Processing, a company that a lot of people probably never heard of, but they're the back-end processor for a lot of credit card transactions, was breached for a hundred million transactions a month. I don't think they've really determined quite what the scope of that breach is.

Not only did New York State follow California, forty-five other states, the District of Columbia, Puerto Rico, the Virgin Islands have all enacted breach notification. I don't envy anybody who does business in a number of different states because although most of them are very similar to the California statute, they all, like New York, have done little tweaks and changes. I can't imagine having to give notice in all 46 states.

So just some of the differences among the states: some of the states said it's only a limited universe of people who are subject to the statute if you're an information broker. Or is it everybody who maintains data? In some states they said this applied only to state agencies and in other states they said this only applies to everyone other than the state agency. Some of the states carved you out if you were governed by other requirements—you didn't have to do breach notifications if you were under HIPAA or Gramm-Leach-Bliley. Some of the states did go and say it makes all the sense in the world that this requirement would also apply to hard copies. A lot of these states are still saying it's only electronic or computerized data.

There are also a lot of variations in the definitions of private information. It's usually your name plus one of the big three, as in New York, such as Social Security number, driver's license ID, PIN account number plus a PIN. But in other states they've gone to it's an account number plus your name, we don't have to have

a PIN or a password. It might be your date of birth, your mother's maiden name, health information, biometric data, or digital signatures.

Again, encryption, some of the states have tried to define it.

When is it a breach? Some of the states have gone to a risk-based assessment to say we're going to let you decide whether there's really a risk to the people who have been subject to the breach. But then you have to get into a question of do you have to prove that to somebody. Do you have to file something with a state agency to say, "We've done our investigation and we don't think there's really a risk to people" and then have somebody evaluate that? Or is it something you can just do on your own? Which may be a conflict of interest.

There are carve-outs for good faith acquisition by people within your entity. That is, somebody who really didn't have authority to see this private information, but they weren't doing it for a nefarious purpose. They signed onto the wrong file or looked at the wrong database.

Timing the notice. Who knows what "the most expedient time possible" means. Some people short cut it "as soon as possible." Some of the states are going to: "Shall be no longer than 45 days" because they do want to give people an option if there's actually a crime. You want it to delay for the legitimate needs of law enforcement to figure out who's in these databases. A lot of companies don't know how many people are going to have to be notified. That takes time, the forensics takes time. So again, if the law enforcement says, "Wait, we're still investigating the crime," you can delay notice. Though there's some question about whether that needs to be documented.

States are starting, like Massachusetts, to impose broader requirements for maintaining security of information that you hold. And so, as time goes on, it's the states who've waited who are starting to add other things. I call South Carolina a "big-picture" state because their bill actually included a provision that criminalizes certain types of dumpster diving. So they're looking back.

When I did this slide it said that California was poised to update its statute. California's bill actually passed the state legislature and then Governor Schwarzenegger vetoed it because of what they perceived as additional burdens on business. He also cited the fact that it wasn't really clear it was necessary—that the current notices were not somehow insufficient. And that

may be a theme as we go forward.

I know we're going to talk about Federal law, so I'll just say right now that there is no single Federal requirement. A lot of people are looking for the Federal government to impose a preemptive statute. One bill actually moved out of the Senate Judiciary Committee yesterday, so there's some hope. I think it would make everyone's lives easier, assuming that the provisions of the bill that ultimately is enacted are reasonable and provide reasonable protection. So there's a lot of other things on the Federal side, which I'll skip through here.

A lot of people are looking to the PCI, which are the credit card rules.

I won't bore you with our proposed amendment to the statute. Needless to say though, there's a lot of push-back and I think it's similar to what went on in California. We have for two years had a bill in to sort of smooth out some of these technical issues with the New York State statute. There's a lot of push-back. People say, "I don't like this, I don't like that," and we haven't made much progress. We're hoping to bring it forward again this year, but really I'm banking more on the Federal statute to be enacted.

So we're trying to just do technical things, we're not proposing a very large overhaul of the statute. We're not saying that we go and make it applicable to paper. We're really just trying to smooth things out and make it easier for people to comply with the statute and maybe improve the quality of the information that those who get the notices they get. That's something that the Consumer Protection Board is big on is that the outreach piece. Are people getting useful actionable information when they get the notice in the mail?

And I think that's it. The breathless finish.