COMMONWEALTH OF PENNSYLVANIA
HOUSE OF REPRESENTATIVES COMMERCE COMMITTEE

NITTANY LION INN - BALLROOM C

TUESDAY, FEBRUARY 25, 2020
9:30 A.M.

PUBLIC HEARING ON
HOUSE BILL 1010

BEFORE: REPRESENTATIVE MARK K. KELLER
MAJORITY CHAIRMAN
REPRESENTATIVE MARCI MUSTELLO
REPRESENTATIVE BARRY JOZWIAK
REPRESENTATIVE MICHAEL J. DRISCOLL
MINORITY CHAIRMAN
REPRESENTATIVE MIKE ZABEL
REPRESENTATIVE JOE CIRESI
REPRESENTATIVE JARED SOLOMON

COMMITTEE STAFF PRESENT:
ELIZABETH HORNE BEACHY
COMMERCE COMMITTEE EXECUTIVE DIRECTOR
JENNIFER L. WEETER
REPUBLICAN CAUCUS EXECUTIVE DIRECTOR

I N D E X

I N D E X (cont.)

P R O C E E D I N G S

CHAIRMAN KELLER: It's 9:30. That's what time we are to get started with our comments. I want to say good morning. Thanks to the members for coming today. Thank you to the testifiers who will be sharing their expertise with data breaches and public security, as we explore the pros and cons of House Bill 1010, sponsored by Representative Solomon.

I'm Chairman Mark Keller from the 86th Legislative District, serving Perry County and Cumberland County. And I want to thank Representative Driscoll for standing in for Jeremy Galloway. And we can start with Representative Driscoll with introducing ourselves.

REPRESENTATIVE DRISCOLL: I'm Mike Driscoll from the 173rd District, Northeast Philadelphia.

MS. HORNE BEACHY:

Beth Horne Beachy, Executive Director of the House Commerce Committee.

REPRESENTATIVE ZABEL: Good morning, everyone. Mike Zabel, representing the 163rd District, which is in Delaware County.

REPRESENTATIVE JOZWIAK: Good morning,

everybody. Barry Kozwiak, Berks County.

REPRESENTATIVE CIRESI: Joe Ciresi, 146th, Montgomery County.

MS. WEETER: Jennifer Weeter, Executive Director for the Republic Caucus.

REPRESENTATIVE MUSTELLO: Marci Mustello, State Representative of the 11th District, which is in Butler County.

REPRESENTATIVE SOLOMON: Good morning, everyone. Jared Solomon, State Representative, Northeast Philadelphia, 202nd Legislative District.

CHAIRMAN KELLER: Chairman Driscoll, do you have any remarks before we start?

CHAIRMAN DRISCOLL: Just briefly, Chairman. And thank you for calling this hearing. I think this is a very important topic. We all know cyber security is a big deal in our lives. We take a lot of this stuff for granted, where we click a button and file our tax returns or we download something or, you know, we ordered something from Macy's, and it seems easy, pops into our home possibly even the next day.

But what we don't know is that the bad guys are out there, trying to get our personal information, and they're always a step ahead. I wish

those bad guys would channel their energy in a good way because they're very bright people. But be that as it may, we have to protect the citizens of the Commonwealth. And that's why I thank Representative Solomon for bringing this legislation to us, because we have to get the remedy right. And that's what today's about. So I look forward to the testimony from the experts and the gravity of this legislation makes sense for all of us.

CHAIRMAN KELLER: As I said, we're here this morning to explore the pros and cons of House Bill 1010, sponsored by Representative Solomon. This legislation creates the Breach of Personal Information Act to require certain entities to provide notification of a breach of personal information.

As we all know, the issue of cyber security is of great importance and we try to protect the citizens of this Commonwealth. As technology grows and changes, this issue becomes more and more prevalent. Today we will hear from various interest groups, all which I'm sure are making this a priority of protecting their clients and data.

Included in your packet today also is written testimony from the State Privacy and Security Coalition, the PA Institute of Certified Public

Accountants, the Pennsylvania Chamber, CompTIA, which is IP Trade Association. And at this time I'm going to turn the meeting over to Representative Solomon to discuss this Bill a little bit. So Representative Solomon?

REPRESENTATIVE SOLOMON: Thank you, Chairman Keller, thank you, Chairman Driscoll, for today's hearing on my Bill, House Bill 1010. Thank you to the members of the Committee and the assembled speakers and witnesses for the time and care they're giving to this important issue. Thank you also - a huge thanks to the Staff. Beth and Jen, thank you so much.

Across the street from my office in Northeast Philadelphia is a Wawa. Now, I know I shouldn't be talking about Wawa in Sheetz territory, but permit me just this once. My office staff and myself frequent this Wawa on Castor Avenue in my district all of the time, whether it's for lunch or to get supplies for my office or for various events. So when Wawa announced around Christmastime last year that there had been a massive breach in their system, it alarmed, of course, not only me but my whole team.

The question everyone asked was, was our personal information at risk? Sure enough, on February

7th of this year I got a letter from the bank we use for expenses at my office. Bryn Mawr Trust was notifying me that our card was at risk. Between March 4th, 2019 and December 12th, 2019, according to the letter, Wawa's system was compromised. So for nine months my credit card numbers and data and those of 30 million others were being passed around by cyber criminals eager to cash in from their heists.

These data breaches, and there are so many, from Wawa to Equifax to Facebook to our Federal Government, are all too common. No one is immune. We, as a legislature, therefore, have the duty to act in the face of this onslaught to ensure that the private information of our citizens are protected to the best degree possible from cyber criminals.

This is why we are here today, to have the discussion about House Bill 1010 and the issues related to it. In the Bill we require that companies that request or require sensitive personal information from customers to take reasonable steps to protect their data and we allow private citizens to file cases in Pennsylvania courts should their data be compromised.

My goal in this is to proactively enshrine in statute that which was stated in the PA

Supreme Court Decision. We, as legislators, do our constituents a disservice if we just let the courts do our work for us. Our constituents require and deserve clearly articulated policies and laws that are debated, amended and enacted in a public transparent process.

The cyber criminals after all of our information, they are tenacious, smart and determined. Whether as individuals, companies or as legislators, we must match them blow for blow. We cannot sit idly by while our citizens' private information is hacked and sold.

I am not by any means saying that House Bill 1010 is the perfect answer. It is a starting point. Let's all work together to perfect it. And in doing so protect the private information of the people who trust us to protect them.

Thank you so much, Mr. Chairman.

CHAIRMAN KELLER: Thank you, Representative. I appreciate that. Our very first testifier is the Office of Administration, Mr. MacMillan, Deputy Secretary of Information Technology and Chief Information Officer. Will you come to the front and give your testimony?

So everybody's aware of how this is going to work, you'll give your testimony and then

we'll have a chance to ask each testifier questions, if they so desire. And we'll take questions after your testimony. You may proceed.

MR. MACMILLAN: Again, I'm John MacMillan. I'm the Commonwealth Chief Information Officer. With me is Erik Avakian. He's our Chief Information Security Officer. I'm sure you read our testimony. Our background is included in the written document.

On behalf of the Governor and the Secretary of Administration, we appreciate the time to appear before the Committee this morning. We have four points to make this morning.

First is our support for the Bill.

Second is some small changes focused on the data rather than the systems.

Third, high-level review of some of the things that we're already doing to protect citizens' data.

And fourth, some opportunities to coordinate legislation that's already in front of various bodies in the Commonwealth.

Okay. So let's talk a little bit about where we are and where we're headed. When we look at the Bill, we think that there are a couple of tweaks

around the idea of the language that's in it that talks about security systems. And we think that that ought to focus on breach of personal information.

And the reason for that is that our systems that are implemented to protect data securely are built in layers. And there is a possibility that something could happen to the one layer but never get to the data. We want to make sure that we're dealing with the spirit of the legislation in terms of unauthorized access to acquisition of data, but perhaps not the penetration of the layers that protect it. When we look at those situations - and we'll present it in an analogy.

When we look at those situations where the layers are, indeed, penetrated, we can learn from those situations. We can learn the source of the threat and we can do more to protect the systems and the data that we're trying to protect.

So if you think of say your home and the data that's in it, let's say, personal photographs, think of that as the data. But you might have a fence, you might have locks, you might have an alarm system, and you might have a dog. Think of those as layers. And just because you jump a fence doesn't mean you get to the photographs. I hope I'm making sense. Okay.

So when we're focused on the data, then we need some time to determine how far through the layers that bad actors have gotten. We need time to make sure that there is - there has been unauthorized access and acquisition of data, not just jump the fence or ring the doorbell. Okay. I see heads nodding.

And so what we are trying to do today, in conformance with the existing law, is to take the time to determine - and Erik will talk more about the determination and what that means - I'm sure you read the testimony - is that it takes some time. Took a long time, nine months.

It takes some time to work through the layers to find the tracks. I think Equifax took three years. So when we look at this, we want to make sure that we're taking - or allowing time for due diligence to determine whether or not something bad has really happened.

It is in our best interest as our home, the Commonwealth, to protect our data, protect my data, Erik's data, your data. And we take it very seriously. So when we look at the Bill, we also work with CCAP and we see that there are other opportunities there.

In terms of what we're doing today in terms - in security, we have built this layered system,

again using the analogy of your home, to help protect against bad actors. And bad actors aren't interested in defense or the doorbell or the locks. They're interested in the data.

And so when we take the time to make sure that something bad has happened, it is our belief and our behavior today that getting the notice out in accordance with the law is something that we need to do and have done as quickly as possible. Although the law allows for a certain period of time, our job is to get the right information, follow the procedure and get the notice out quickly.

It's our data. We don't want it out there. We don't want our credit card out there. I know the Commonwealth does a pretty good job of avoiding collection of credit card information. It's all the other stuff.

I'm going to let Erik talk for a little bit. He will help you understand a little bit about what we mean by determination and the time it takes to go through those layers. Erik?

MR. AVAKIAN: Thanks, John. So as John mentioned, there's multiple layers of technology. With that we have policies - established policies and procedures. We really focus on and use our education

as well as - amongst the services that we have put into place. They're based on industry best practices. You want to think of this as some of the federal guidelines that are out there. We employ those multiple layers using that.

When I mention policies and procedures, back in 2018 we formalized the procedure for responding to an incident. When we think of an incident, that doesn't necessarily mean that a breach has occurred, but it could be any incident. For instance, somebody clicked on an email, they clicked on something bad, they get infected. We can usually get - we have those types of incidents a lot, but we can quickly get that user back up and running, remediate quickly.

So the vast majority of cyber incidents are remediated quickly. Where there's other types of incidents, where there's more - they might have gotten through a few layers, we need to do a deeper dive. And so through this process, which we call the incident response procedure, IRP, we formalize this process regardless of the type of incident from the most simple incident, as I mentioned earlier, to something more unique, where we need to do a deeper dive, where we will need to do a thorough investigation.

Oftentimes that involves forensic

analysis, a thorough log review. Because we need to take a look at, okay, where - what layers have they gotten through? And that takes times. Those processes take time, and no two incidents are alike because of the types of data, types of systems that are out there, and what the investigators are actually looking at.

But the process is formalized that throughout this life cycle of an incident, how we act technologically, how we act from a communications standpoint, so how we communicate with each other, how we communicate inward and outward is defined through each phase of that process, so that people are getting the facts during the investigation.

But investigations do take time. And so, therefore, it's vital to enable the team, the technical team, to perform that technical analysis to get to the facts. And once those facts are gathered, they're presented to a legal team, who then can use the terminology determination, can make the determination based on facts and evidence through a thorough investigation.

So that's why we formalized this process. And then through each incident we also have action after action, where we then learn from that. What can we take from this incident so that we can

prevent -? And John alluded to that earlier, so that we can prevent future occurrences?

Even in the Wawa example, we take a look at incidents that are happening out in the real world so that we can learn from those as well. What can we do internally to improve, even based on the incidents that we see outward in other organizations?

MR. MACMILLAN: One of the things that we're doing is working with actual organizations to look at how laws at different levels affect the way we design and built, implement and support some of the systems we have today. A couple of examples are federal laws, federal policies, federal regulations around protecting healthcare information.

And so those laws affect how we design and build the layers in our technical environment. And when there's some inconsistency in those laws and it's something that we have to look at by looking at all the legislation in front of us, how do we get a little more consistent with how those laws apply to those layers and technical environment?

Each layer costs some amount of money, whether it's the edged fence, the locks, the doorbells, the alarms and so on. When we can make that more consistent, we can design and build and, most

importantly, recruit staff for a consistent set of requirements. So we're working with the National Association of CIOs to look at federal legislation like HIPAA and other things for consistency.

Before I close my opening comments, one thing that we are really interested in is House Bill 2009. We think it complements what we're trying to do with 1010. The idea of creating a cyber security Coordination Board that would allow interest groups both from within state government and from without to talk about our opportunities for improving what we do and how we do it, so that these ideas can be shared and put in and prioritized into our systems is something that we're really interested in and really passionate about.

There is another Board that focuses on just spatial information that is designed and built very similarly, and we think that that is working. So I think that's -.

MR. AVAKIAN: In the spirit of collaboration - and we've really been focusing a lot on the collaboration aspects, working with CCAP, working with partners of cities, local governments. And it's a working model. We're working together. How do we improve together?

And we've done great things working with the county, bringing things like security training and exercises collaboratively with CCAP, using the model where we can achieve economies to scale and better services across state government. And doing more of that in collaboration is a winning approach.

MR. MACMILLAN: We're all trying to serve the same citizen. We tend to think of the government in layers. But from a citizen's perspective, it's all government. And so when we look at the opportunity to protect data and work collaboratively with other jurisdictions, we think that benefits all citizens.

CHAIRMAN KELLER: All right. Thank you very much for your testimony. I want to point something out you indicated on House Bill 2009. We haven't passed that out.

MR. MACMILLAN: That's terrific.

CHAIRMAN KELLER: Moving ahead, a question I have is, can you give examples of how you coordinate with the other agencies - other state agencies on other government entities on cyber security matters? And what plans do you have in respect to new projects and coordinating incentives for the collaboration or talking amongst -?

It's always been an issue of mine that we here in Government seem to falter in not having agencies speak with each other. I think it's very important that - especially with this, that, you know, that's something that we should be absolutely, you know, speaking to each department within the Commonwealth itself, the agency, about cyber security issues.

MR. MACMILLAN: Absolutely. I'm going to get started, then Erik, if you can take it from where I -.

So back in 2017 the Commonwealth went through a really important shared-services transformation, where all IT employees were aggregated into the Office of Administration. So in terms of those conversations about cyber security information, the layers in our technical environment, that is an ongoing conversation.

We also work with organizations outside of our jurisdiction. Erik and I both talked about CCAP. We also work with all branches of the House and the Senate.

Erik, do you want to take it from there?

MR. AVAKIAN: Sure. So you mentioned collaboration across the state agencies.

We also have an Enterprise Technology Security Council, where there is a member from each of the agencies on that, including the IT Legislative Caucuses, who also, back in 2018, were invited to that.

So we got this peer group of professionals where we talk about security policy, how do we improve, how do we collaborate for the benefit of security. How do we - and that group really provides direction on policy, strategy, how to make better investments when it comes to cyber security opportunities and capabilities and how to remain not at risk.

So it's really - it's collaborative. Bringing in the legislature as we've done, it now has brought that conversation to a wider audience. And doing more of that through this collaborative approach seems to work really well. Because when people are talking to each other, then they're more interested. Hey, what are you doing? What are we doing? And we learn from each other and improve collectively.

MR. MACMILLAN: And we focus on how things are being done. And through stronger coordination and awareness, then we can make that real impact. Because again, we're serving the same citizen.

MR. AVAKIAN: We also - you mentioned

CCAP. We also meet quarterly with the CCAP and we collaborate with their IT and their CIOs across all different counties. And that's been instrumental in forging partnerships and learning from each other and improving together as one Commonwealth.

MR. MACMILLAN: Some of that sensitive data flows from the federal level to the state level to a county level. And when we can protect it across the entire - interaction with a common set of technology, then we can make sure that we're doing the due diligence in getting the notifications out there to protect that data faster.

CHAIRMAN KELLER: Representative Jozwiak?

REPRESENTATIVE JOZWIAK: Thank you, Chairman.

It's quite - thinking about the layers of security, you forgot one, the armed guard. You have the homeowner. So I'm curious as to what is your ultimate - what is your ultimate guard in your system?

And what would you say - I'm assuming you're protecting the income tax records, HR information, people's personal stuff. What are you going to say to citizens to ensure them - give them confidence that you're doing everything you can do to

protect their data?

MR. MACMILLAN: Within the resources that we have, we believe that we're already doing many of these things and doing it very well. Could it be better? Yes, it could be better, because the environment is changing all the time. Personally, my data has been hacked five times. I take it very, very personal.

But the idea of building those layers and making sure we have the right protections also changes with time. New technology is introduced. New techniques that actors can use sometimes is as simple as what happens in between people's ears.

The fraudsters are really good at tricking people. You may have had that happen to you or a family member. Not everything is a technical solution. So when we have these ideas and these opportunities to work together, we can do more and we can see. And we know that there are examples. When we work across jurisdictions, we can also reduce the cost of sharing solutions.

So a couple things to think about. A common architecture. When we talk about security, we talk about those layers. It's built in a way that you might build a home. And if you were going to change

what's in your home, you would never start with pulling out the walls. You would go to your architect to figure out what's behind the walls. And so when we can look at this architecture across layers, across federal, across state, across county, across municipal, now we're dealing with the same citizens and the same data.

If we had the opportunity to do more, where would we start? Well, we have this architectural model. We know how we can make it better. We know that. I hope I answered your question.

REPRESENTATIVE JOZWIAK: Thank you.

MR. MACMILLAN: Erik, anything to add?

MR. AVAKIAN: I would just say in focusing on people, right, and working together and collaborating and learning from each other, again, go back to the CCAP example. Because there's an example of a service where we can improve security to the betterment of everyone in the state government, including the county governments.

Now we're - we're all utilizing a shared service, one unified service on an architecture that's common to all. And that includes everybody's security across this jurisdiction. And it also drives down cost, because in economies of scale we're utilizing

that unified service. So doing more of that, I think, is a great opportunity across all state governments.

MR. MACMILLAN: One of the things we're focused on is this idea of security awareness where we're educating users about what data is out there and how to better protect it. That helps.

And then we're going to exercise using the same solution to a test that people remember how they were trained. And we'll make that training better every year. We track data about security awareness, how many people have taken that education, and then we can see that, how to improve it year after year.

I think this year we're looking at 92 percent of us have gone through cyber security awareness training. And we make that better ever year.

CHAIRMAN KELLER: Representative Solomon?

REPRESENTATIVE SOLOMON: Thank you, Mr. Chairman. On 1010 you mentioned some tweaks. Do you - it seems like you're talking about the definitional section. Do you have specific -?

MR. MACMILLAN: Yes.

REPRESENTATIVE SOLOMON: Can you be as specific as you are prepared to today?

MR. MACMILLAN: Let me see if I can find

it. So in the definition section we talk about breach of system security. And we would like to focus on the unauthorized release of data within the system.

REPRESENTATIVE SOLOMON: Got it.

MR. MACMILLAN: Because, again, the systems are built in layers. We might get through one layer. Again, on the analogy of the home, we might be able to jump the fence, but we never get to the data.

And we were focused on unauthorized access and acquisition of data. We can determine that by following the instant process - procedure.

So that's one example. And I think from that point forward the legislation is very solid from -.

CHAIRMAN KELLER: Well, we understand you're working with CCAP to finalize it. But when you have it finalized, will you share that with our Executive Directors? It would be very much appreciated.

MR. MACMILLAN: I can. So this idea of - when you build those layers, part of the protection is to make sure that those that are authorized can get access to it.

It's a double-edged sword. You want to protect from unauthorized, but you still need to enable

the business sources that deliver value to citizens at the same time. And so by working through those layers and verifying that something good, which is fine, or bad has happened, then you can take the appropriate action. But it's not just the system. Right? Sometimes systems interact with each other.

So you might think of the Target situation. All right. Target wasn't an IT system. It came in through the building management environment. And then first a shared network to do something bad.

So when we look at all of those systems, right, we want to make sure that the right steps are taken so that the appropriate, correct monitoring and other protections are in place as quickly as possible. It's not our desire to go 30, 45 days. It's to get through that activity as quickly as possible.

REPRESENTATIVE SOLOMON: Thank you.

CHAIRMAN KELLER: Representative Ciresi?

REPRESENTATIVE CIRESI: So thank you both for being here. I know the testimony is beyond just what our own government's doing. It should be also to protect the consumer.

But I'm a little concerned, and I have been, that we're not consistent like you brought up, every agency in the government.

We have school districts out there that were just hacked and held for ransom and had to pay $600,000. And it showed that school districts are not consistent. They are government entities. We do legislate them.

So my question is, from your area, what are we doing that we're all consistent throughout the government in general? I don't understand the segmentation, siloing, it makes no sense to me. And again, it takes time. I'm not about time.

You know, let's get it done. What will it take? What will it take to do this across the state? This is what we need and then let us argue where the funding comes from.

MR. AVAKIAN: So if I can just answer in regards to some of the sources that I talked about earlier. So that security learning training, fishing exercises, that's a service, again, we've established within the state government for a number of years, working with the CCAP. Now we're doing that in the counties. Recently we had those discussions with the IUs.

We have to bring down the cost per license and having the school districts participate. And so there are many conversations that have occurred

over the past few months. And the goal is to bring the IUs on board with that service or in that same type of shared-service model.

And that's just one example of a common service, then, that will be established. But it does take collaboration, because that has actually occurred, but it's based on collaboration and us getting out there and building and forging relationships with the IU community to say, hey, look, here's a service. How can we work better together? I think it's going to take more of that across the entire service model.

REPRESENTATIVE CIRESI: Well, what will it include other than saying to the government here's what we're doing? Like we say to three kids, this is what's happening. You know what I mean?

MR. AVAKIAN: That is happening.

REPRESENTATIVE CIRESI: I know, I know, but I'm just saying - so good for you, but not you, but maybe you can have it. So I'm sorry to get off on that, but it escapes me that our school districts - if each district has to pay its own ransom for $500,000, we're in big trouble.

MR. MACMILLAN: We couldn't agree with you more. We have been promoting the idea of consistency of policy on legislation to enable us to

have those layers be more effective for everybody that we serve. I think we've said that more than once this morning.

Part of what we're talking about is going to take real courage. And I don't mean that in a bad way. Right? But when we look at all of the systems that are out there that support business transactions, whether it's HR or tax issues or transportation or unemployment compensation or vendors, all of those systems have some amount of sensitive data in them. And they're designed and built over about 60 years to meet policies and the technology that was available at the time.

It's easy to say we ought to burn it to the ground and start over. It's not the way we can do it. We have to work together. And I think that 1010 is the way that we proceed. We tighten the definitions, we focus on the data, and then we attack the broader problems of consistency.

We agree. We agree it ought to be done. We think - the real challenge is, we really don't know what that impact is. Could it cost less? It might. I don't know that. I can't tell you that today. If we had the same set of policies, the same set of laws protecting all of the data, all the data needs to be

encrypted at rest, encrypted at transit.

If we treated it all the same, would we raise the level of security? We have to align our protections and our layers with our policies. And one of those policies is privacy. And that's really outside our lane. We interpret what needs to be built and designed and implemented and operated for many years based on a decision that happened a long time ago, and we're trying to change that.

I am fully behind the idea of making it more consistent and faster. In the Commonwealth your child's data has to traverse the internet twice to get from the school to the Department of Education. That's just one example.

We should be far more consistent. I agree. And I applaud the idea of making it so.

CHAIRMAN KELLER: Thank you very much for your testimony. We appreciate you taking the time to up and give us that, and we'll move ahead. Thank you.

MR. MACMILLAN: On behalf of the Governor and the Secretary of Administration, we appreciate the opportunity this morning. Thank you very much.

CHAIRMAN KELLER: Our next testifier

will be the Pennsylvania Bankers Association. Mr. Hayes, he's the President and COO at Kish Bank right here in State College. And also we have with us Mr. McMinn, Executive Vice President, General Counsel for Kish Bank. Thank you both for participating and you may begin.

MR. HAYES: Thank you for having us. We appreciate the opportunity to speak on behalf of PA Bankers Association, as well as Kish Bank here locally.

Kish Bank is a $920 million community bank. We service three counties in Central Pennsylvania here, Mifflin County, Centre County and Huntingdon County, as well as some clients outside of those counties. And you know, our presence here today is on behalf of the PA Bankers, which is over 123 members, made up of banks, savings banks and trust companies of all sizes and their affiliates that are doing banking business, providing financial services in Pennsylvania, providing vital financial services to the communities and businesses and governments, the individuals.

We are an important part of our local communities. We volunteer a tremendous number of hours to local charities. We donate millions of dollars to local charities as well. And we feel strongly

community banking is a critical part of communities. It's a critical part of what makes Pennsylvania great, as well as many other communities outside of Pennsylvania.

We do want to thank you very much for this opportunity to share our views on data security, breach notifications on Bill HB 1010. And in particular, we welcome the opportunity to discuss how serious this is for our industry.

As the Chairman introduced, I'm Greg Hayes, President and Chief Operating Officer. Bob McMinn is our General Counsel, Executive Vice President of the bank. And we want to share a few things relative to our perspectives on this, but I first - just in reference to the Office of Administration's comments, I'm going to echo a few pieces of - to focus on data and the consistency that must exist. Specifically we'll talk about that as well as the collaboration that's needed as we move forward.

The background I want to just touch on is relative to banking history itself. And it's a bit different than some of the other folks you'll talk to today because of the massive amount of regulation. There is a ton of legislation out there and we can legislate - in Pennsylvania we can legislate changes

around notification and privacy. But as a financial institution we are regulated to the laws that we have to - that we have to follow. And that regulation is significant.

We are a state-chartered financial institution, so we have the Pennsylvania Department of Banking as our state regulator. But as a bank in the United States, we are federally regulated as well.

And one of the most significant federal laws that - and they've been in place for decades in the financial industry, that we have to comply with is the Gramm-Leach-Bliley Act. G-L-B-A, or GLBA as we call it in the industry, is a significant cornerstone of how we operate, how we keep our customer information and data security requirements in place.

In 1999 it was enacted and it contained very strict security confidentiality requirements on consumer data. Requires notification to the customers - or to the consumers if a breach of sensitive data occurs. A breach of a system is different than the breach of sensitive data, and so we'll talk a little bit about that.

But not only must banks properly notify our customers of a data breach, we must disclose our information, privacy, our collection of sharing

processes, our customers' rights, and we must limit the sharing of that information with nonaffiliated entities. We have a very strict set of rules in which we operate.

The financial market - the financial system in the United States is very complex and it does require that we share information. Credit card processing information must travel between certain entities. And that transfer of customer information is critical to the nature of providing those services to our clients.

And in some cases we're also required to report information to legal - based on legal regulatory mandates to law enforcement, child support, avoidance of terrorist and illegal trafficking activities. So we have to share certain information based on those rules.

GLBA, G-L-B-A, The Gramm-Leach-Bliley Act, is not the only financial protection statute that exists at the federal level. We also have the Fair Credit Reporting Act. We have the Right to Financial Privacy Act, which both date back to the '70s. We have the Health Insurance Affordability and Accountability Act, the Child Online Privacy Protection Act, the CAN-SPAM Act, Consumer Protection Act, the Electronic Communications Privacy Act, and the Drivers Privacy

Protection Act, among others. And when we get to the state level, we have our state requirements for information sharing in Pennsylvania.

We'll talk about this one again as well, but we have the PA Breach of Personal Information Notification Act as well that applies. And many states have - 47 states have something similar to what Pennsylvania has on the notification side.

But Congress has long taken the lead as our privacy - you know, the lead in privacy protection as well as information exchange. It doesn't stop at state borders. Obviously the financial system is a world - it's - the financial system is a United States system, but it's a world economy. It really isn't something that stops at the state borders.

So because of that we are and the banking industry is advocating for several things that connect to this Bill. And we'd like you to be aware of them. We're advocating for a national privacy standard, one that - like the one that's already in place for banks, is a national standard that's more clearly understood, so the consumers across 50 states can understand how their information can be shared.

You see even the - Mark Zuckerberg of Facebook is calling for this kind of national standard

for information privacy standards. But we also have strong advocacy and support for national data protection data breach notification requirements, similar to what exists in banking. So that if there were a breach of information outside of the financial industry, they would have the same levels of requirements that we have today.

We want robust enforcement of national standards by appropriate federal regulators. As I stated, it's one thing to have laws, it's another to be regulated. And we'll talk about that in a moment as well.

But then for financial institutions, the federal preemption of the patchwork of state and local security laws that ensure our national Consumer Protection Act - or national consumer protection model.

So since 2005, banks have been required and their affiliates have been required to place incident response programs in place to address security incidents involving unauthorized attacks as to consumer or customer information. And those - you know, for us, anything from someone's bank statement, the mail got put in the wrong mailbox and the person calls and says, hey, I got so-and-so's bank statement, that's an incident we have to track.

Was it a breach of information? At one level, yes, it was. Someone didn't - who wasn't intended to receive that information received it, and we have to track it and notify the customers. We're required to do that.

It happened because of something that was outside of our control, someone stuck it in the wrong mailbox, but it's still information that we have to share. And we are required at this time to share and make sure we communicate to our clients when that happens.

You know, and that's on one incident. You have all the way to the other set, where you have a Wawa or a - having lived in Philadelphia and now being in Sheetz country, I miss my Wawa. Don't tell Dave Sheetz that.

The other extent of Target breaches, where an organization that isn't required doesn't have notification standards, national notification standards, doesn't notify its customers, they get notified through their bank. Because through the credit card processing system we have understanding and communications around if information is breached, the bank takes on all the risk.

So when all of the credit cards from

Wawa or Target or Home Depot - and there are hundreds of breaches that have occurred, when those occurred, it was the banks that had to replace the cards. It was the banks who covered the cost of fraudulent transactions on those breached card owners.

Target didn't have any expense related to a fraudulent transaction that occurred on a card where they lost -. They had a fair amount of expenses, $240 million in communications and marketing, and things that helped protect their brand, but they didn't have any loss relative to the fraudulent activities that occurred on those cards.

And that's the kind of focus we want on a national standard for breach notification, so that we can be part of the solution to help our clients.

And so what happens when we get notification of our customers - maybe 360 of our clients had - were on the Target breach list, although we saw a lot more customers that came in and said, hey, I've got some fraud on my card. We weren't notified about it, so we know there are probably more.

We - if it was brought to my attention this is a loss, we replaced their card and we took care of it. And in the financial industry, that's - that's where the transaction accountability laws on the

financial industry, on banks - but it's important that we understand that as we - as we abide by all of these federal regulations and laws, we're also supported.

The Federal Financial Institution Examination Council, the FFIEC, has an Information Technology Examination Handbook. That Examination Handbook is over a thousand pages and it guides the Examiners on how to examine banks around cyber security and information protection, bank compliance, better management, information-technology governance and our security-program management.

That level of regulatory scrutiny is unique to the banking industry and is one of the reasons the banks are highly trusted by our customers and the incidences of data breach at our financial institutions is far less than any other sector.

At Kish we probably spend well over $2 million on our information security and data systems that protect our customers' information. And it is - a critical aspect of what we do as it is - as the banks we're in the risk management business of -. One of the things - one of the biggest risks for us is information security, cyber security threat. And we manage that with a very keen focus on what - due to our reputation, due to our ability to provide solutions to our local

communities, if that were - if that repetition - that trust were eroded.

So if banks fail to comply with the federal requirements, we have enforcement actions that are put upon us that recover significant penalties of up to a million dollars a day for consumer restitution and remediation actions. We don't feel that we need to expand the privacy enforcement authority over banks by other state agencies, state Attorney Generals or other state and local government authorities for good reason. The increase in state privacy data breach laws must simply be replaced by a federal standard.

The existence of new requirements have the potential to disrupt the financial system, preventing consumers from living their day-to-day lives across state borders. It's a national - they don't see the state border when they're buying stuff online or doing business or opening an account online these days or any of the aspects when they use their personal financial information.

And to reference some of the information included in our testimony, voters prefer a national privacy standard and they believe strongly in the banks' capacity - in the banking industry's capacity to keep the information safe.

So there are some aspects of HB 1010 that we are opposed to as drafted. And we appreciate that - your willingness to talk through where some of those things might need to change. But as a freestanding Act, it would conflict with the current PA Breach of Personal Information Act. It would conflict with a lot of the national standards that we have to abide by and create some concern over customer confusion.

As I noted, customers are already a national - you know, they expect things to be consistent across the nation. And there's a patchwork of state statutes that prevent customers throughout the nation from having the same rights and remedies applicable to maintenance and use of their personal sensitive information.

The other thing is the Bill has a bit of an incomplete definitional realm of financial institution. That definition is one we would need to see more clearly stated.

And then finally it adds an expanded authority to enforce violation for the Attorney General, including the overriding of arbitration agreement, providing a statutory private right of action, all of which unnecessarily impact the banking

industry and affiliates.

The provisions specifically, which would provide the state agency, any political subdivision or business or individual who maintains and stores computerized data, a customer's personal information-. If they fail to take reasonable measures consistent with their nature and size to secure information, the Commonwealth may issue a civil action to recover actual damages of $5,000 for each separate violation and then further authorize the Attorney General to recover civil penalties of $10,000 per violation.

You know, as the example in the previous testimony, the question about the school district, if 25 customers - 200 - I'm sorry, 2,500 students at that school district had their information hacked, not only would there be a $500,000 ransom, but there could be $12.5 million of costs and attorney's fee - plus attorney's fees for civil penalties -. Or I'm sorry, for the damages, civil action damages, as well as another $25 million in penalties from the Attorney General, who if they failed, in the words - reasonable measures consistent with their nature and size were not taken to secure the information.

And that's really hard in the face of the fact that when they got attacked, the school

district was the victim. And if we could come together - and this is the idea of collaboration, as much as with the Office of Administration brought up. If we could come together instead of punishing the victims of these crimes, the companies who are getting attacked, let's say create partnerships between government and private sectors to promote better measures to provide privacy - privacy consistence with what is being done in the banking industry and many other areas where the government - complex electronic - electronic data collection and storage systems are essential for the operation of our country.

So we suggest instead of the Commonwealth - instead, the Commonwealth build programs to help businesses effectively manage, distribute personal information and to aggressively pursue and prosecute actors who steal and misuse confidential information.

We devote a significant amount of resources toward protecting the customers' data and we offer a ton of guidance and education to them as well on how to keep their information safe.

We thank you for this opportunity to speak and share our concerns. We are happy to take any questions.

CHAIRMAN KELLER: Thank you very much. The question I have is I understand that JPMorgan had a data breach back in 2014 that affected 76 million people - households, 7 million small businesses. It was a significant breach. It came - it only came to light when the SEC did their filing.

Why aren't the individuals notified before that took place? Can you explain that for me?

MR. HAYES: I can. And just my recollection of that particular case, and actually it was their second breach.

The first one, a year earlier, occurred in their credit card system. And they, I believe, did replace all those cards and communicate with those customers.

When the second breach happened - and this is an example, again, for the gentleman from the Office of Administration. It was a breach of the system, but it was not an unauthorized access of data. So no data left JPMorgan's system in that case.

So while hackers got into the system and were able to view information, name, address, phone number, email, they didn't get - from my understanding, they didn't get any account numbers - they didn't get any account numbers or any information. And nothing

was extracted from the system. And under the same notification requirements for the roughly 47 states that have notification requirements, as well as federal notification requirements, since the breach was not material, there was no perceived malicious intent or use of the information, they were not required to provide notification. That is my understanding.

CHAIRMAN KELLER: Very good. Representative Ciresi?

REPRESENTATIVE CIRESI: Thank you very much. You guys are doing a lot of things. And as I'm sitting here thinking, you build walls, you have the security system and you have the armed guards, you have the dogs, and they're still getting in.

What are we doing? I mean, if that was the case and they're robbing money out of the vault every day and you have all those securities, we'd be in a room until we come up with a consistent plan.

When you mention the consumer themselves, my concern is this. It's become like an everyday occurrence. Yeah, we had a breach of security and you get a letter, a form letter, in the mail letting you know that your account was breached. And most people don't pay attention. It's more propaganda or whatever and back in the garbage.

So my thing is, how do we make a clear pathway to the consumer to let them understand what happened?

At this point, everybody's information has been breached somewhere along the way, somehow. We know that. Let's be realistic here. But how do we really let the consumer understand from your perspective - I'm not blaming the banking industry. Nobody's saying that, you know, I get a letter from Wells Fargo, your information has been breached, here's your new card. Okay, my new card.

What are we really, really doing for the consumer to understand? I don't think the consumers really get it a hundred percent.

MR. HAYES: Well, I certainly appreciate that. As we get notifications from our retailers of breach of card information, we have to reach out to our customers and explain their card number was breached through some of their activity somewhere and that we think it's in their best interest to replace their card.

That is hard. People don't understand it. And I'm not sure that - we do everything we can to explain to the customer how we protect their information.

As a community bank, we have more of a personal relationship with our customers. They're not just getting letters in the mail. They get a phone call from Jessie, the banker that they know at our branch. And our customers generally understand that the breach did not occur because of something we, the bank, did, but that we are there to protect them and help them because they trust us.

And they engage with us and they participate in the activities we have to help them keep their information more secure and more safe. Establishing trust for us is the only way we can work directly with our clients to help them be more safe and protect their information.

As we have seen, many people have become numb to it. And it's hard for us to - there are so many instances of fraud beyond the information breach - or well outside the information breach, where they're using one piece of information that they got on someone and they're trying to generate fraud. They're trying to send them that email to get them to click on something, to get them to do this or whatever.

They're sending them a check in the mail, getting them to deposit it into their bank, they wire money out to - they're using this information for

fraud and that relationship with your bank to help protect you when - not when you lose your information, not when your information's breached, when someone's trying to defraud you by using your information.

Because of the Fair Credit Reporting Act and the red flags and all of the federal regulations we have to abide by, if someone comes in for a loan and we pull their credit report and we see that their Social Security number has been tied to someone else's name or some other alias, we pay for services that collect that information.

We're required to make sure that when we're giving a loan to someone, when we're opening a new account for someone, they - the person in front of us is the person connected to that Social Security number and that we don't have fraudsters trying to open relationships with us under someone else's identity.

And so we have identity protection requirements that we work very hard to abide by, we are regulated by. Our regulators examine them when they come onsite. It's a big part of what we do.

Our concern is that there are nonfinancial institutions that - back to the definition of these nonfinancial institutions who are going to

collect this information or open relationships with the consumers who are not regulated and held to the same national standard that the banks are held to.

CHAIRMAN KELLER: Representative Solomon?

REPRESENTATIVE SOLOMON: Thank you, Mr. Chairman. On the freestanding Act piece, I - I think I can get with that because I signed an amendment of the 2005 breach law. So I'm happy to share that with you guys.

The incomplete definition of financial institutions, I think we can work together on that. The statement you made about that we don't need to expand private enforcement, I mean, what - isn't it, though, kind of the cat's out of the bag. Right?

I mean, the Dittman Decision in November of '18 says, yes, we do - individuals throughout Pennsylvania have a right - private right of action and it sounds in negligence. It's the first time the courts made a pronouncement on that.

So instead of just letting that percolate through our Court of Common Pleas and there's going to be now appeals to get the contours of what that negligence act looks like, why don't we in the legislature own that and work with stakeholders like

you to make it a law that reflects a lot of the feedback that you're giving us?

MR. MCMINN: Bob McMinn. The Dittman case did impact the way the courts look at the economic damages bar with regard to court actions. And I would suggest, however, that if we're concerned about Dittman, a different approach would be -. And one of the reasons to be concerned about Dittman with regard to this whole matter is that - and this goes to what Mr. MacMillan and Mr. Avakian said, we're looking for collaboration.

And we're also - as they discussed, layers of protection that are technologically-based. The remedies - civil remedy here is - put forward in this Bill would place, in our civil court systems, in the various courts across the Commonwealth, starting out with the Courts of Common Pleas, the determination as to whether or not reasonable measures consistent with nature and size have been taken. My suggestion would be that that eliminates any total consistency with regard to remedies.

The fact is that we are all very concerned about this topic, but using care to create the right remedy and not one that doesn't take the technology and the kinds of layers of security that

Greg is talking about and Mr. MacMillan and Mr. Avakian are talking about -. Placing decisions about that kind of technological expertise in a Court of Common Pleas before perhaps a jury instead of having a regulatory scheme where there is a layer of civil professionals, civil servants, who focus their professional lives on this, just doesn't seem to make sense to me.

And as we think as an industry, not just our industry, but businesses throughout the country who rely on a stream of revenue that suits their customers, we all do this. I know I'm on the phone or on my computer and I'm giving them my credit card number. All of our customers are doing this.

And to put us in a position that the discussions of that take place in a civil Court of Common Pleas seems to me to not be the standard by which, as government servants, we should be held. I think it's something we need to consider seriously.

I don't agree that Dittman calls for this specific type of legislation as a response. If it's a separate conversation - Dittman, of course, had to do with the University of Pittsburgh Medical Center, an issue with employee information. It wasn't a consumer-based case.

There was a variety of interpretations.

I'll just maybe cite to the Pennsylvania Bar Quarterly article on Dittman, which is much more eloquent than I can do. It's written by Thomas Martin, who is an expert Certified Information Privacy Professional and member of the Pennsylvania Bar. This was in the January of 2020 edition of that. Take a look at it. It's a pretty clear explanation of Dittman and scholarly work with regard to its impact.

REPRESENTATIVE SOLOMON: Can I respond? Yeah. I'm trying to - 62,000 people had information that was compromised in Dittman. Before the Dittman standard, Judges had no idea how to handle these type of breach cases. Right? It's like is this bailment? Is this unjust enrichment?

Like, what is a cyber breach? We don't know what to do with it. So at the most they dismissed it. Most of them were just tossed.

Now in Dittman there is a standard. I don't think it's clear at all, because negligence is sort of muddy, reasonable person standard. We in the legislature have the ability to reflect and clarify, so that folks like you know better when to anticipate litigation.

We are closer to the people that we represent who are dealing with these breaches. So I

can't really quite understand why you would rather allow the Supreme Court and now the many cases that are going to come from that Dittman Decision to define a right of action when we all can work together to get it right.

MR. MCMINN: The standard that is set forth in the proposed legislation is a reasonableness standard. It's the same negligence standard that would be referred to in any tort case.

My suggestion, though, is that civil tort litigation is not the place for this matter to be served. When we talk about the Act and its requirements, it has not been perfect. However, it has done an exceptional job of providing guidance to banks and management institutions across the country, holding them accountable. To add a layer that would involve civil court litigation, I think, takes resources away from that central focus and would impair our ability to continue to successfully respond to threats.

I acknowledge that there is this sense that the negligence standard ought to apply. However, the way that standard gets impacted in civil courts, the way it gets executed is designed primarily for individual cases, you know, we have auto cases as an example.

But to call for the civil courts to deal with this wide range of activities that are interrelated with nationally-based companies and state-based companies I think is a mistake.

CHAIRMAN KELLER: All right.

Thank you very much for your testimony. Appreciate it.

Our next testifier will be a retailer. We are running behind, as usual, so - just go ahead and introduce yourself.

MR. HOLUB: Good morning, Mr. Chairman and members of the Committee. I'm John Holub. I'm Executive Director of the Pennsylvania Retailers Association. If I may introduce these fine gentlemen this morning. To my immediate right is Dean Sheaffer, who is the Senior Vice President and Chief Compliance Officer for Boscov's. On the far right side is Paul Martino, who is the Vice President and Senior Policy Counsel for the National Retail Federation.

So we very much appreciate the opportunity to speak with you. I have submitted comments, so I will try and be very brief. And really I just want to turn it over to Dean and Paul, because they truly are the subject matter experts on this.

It's no surprise, this is a very

important issue to retailers. Obviously we want to - the protection of our customers' personal information is extremely important. If we were to lose the trust of our customers, they just might not shop with us. And right now, also I don't think this comes as a surprise, retail as an industry has gone through and continues to go through the most transformative periods that we've ever been through as to all technological advances we've had over the years.

I mean, just a few short years ago you wouldn't have thought you'd be sitting over the phone, that you could immediately break down and go on and shop at your favorite retailer. So thanks to those technological advances, things are just rapidly changing in our industry.

And one of the coolest aspects, too, of this technology is really the personalization that has occurred. And we really - retailers provide a seamless shining experience between your phone, between your computer, between your store visits. And it's really because of this personalization.

And obviously, we ask, if you talk to us, you know, should you advance any type of legislation, we really ask that you don't risk jeopardizing this relationship that we created for

customers through this technology, as well as any - you know, inhibit any future technology that might be developed to continue to enhance these relationships we have with those customers.

Just really quickly, there's a couple points. We do have some very significant concerns with this legislation. And a couple quick points that I just want to make. First and foremost, I think our biggest concern right now, which would be who this captures or more actually who it doesn't capture.

This Bill required notification requirements on consumer raising businesses like retail, but it does exempt a large array of entities, particularly financial institutions and credit card providers.

So there's instances where a retailer would be required to report a breach even though through no fault of their own that breach occurred. So that's quite troubling.

So if this legislation was to advance, every entity that is responsible for personal information, should they be - for reasons why that breach occurred, they should have an obligation to provide that notification.

Right now the way the legislation's

written, that currently doesn't occur. And I do just want to kind of point out -. And I think Paul really will add some more flavor to it, but we do - there's some inaccuracies - I'm trying to characterize it as nice as I can, by the previous testimony from the Bankers Association, as far as to the extent of the notification requirements, particularly one, retailers, all different states, including four federal territories, require retailers to provide notification.

The federal statute that they mentioned, GLBA, does not require a financial institution to provide notification.

And furthermore, there's some guidelines that say they should require notification, but it does not officially require it. So Paul, I think, will really touch on that a little bit more and kind of address some of those inaccuracies that you just heard in the earlier testimony.

The second issue that we're quite concerned with is these private actions, one issue where we can agree with our friends in the banking community, is with regards to private right of action.

We're quite concerned that obviously it will open the floodgates to lawsuits, and a lot of these occurrences need to be prosecuted, when there's

no harm to the consumer. So it's quite troubling and we really feel that any action -. And I believe the bankers might have mentioned it as well. Any enforcement activities really should be through the state Attorney General.

We think it's best suited for them to, you know, by a case-by-case basis, determine if there is any harm and then provide any kind of enforcement and penalties along that regard.

And then the last thing, one other big provision we're concerned with is the cost of government provisions. The retailers spend a certain amount of time and resources to combat this issue right now and they already are paying several different aspects for cost recoveries.

I will - I take great exception to a comment that was made earlier about one particular breach that said the retailer denied any cost associated with that breach. That, quite honestly, is absolutely absurd. And I'm trying to put that as nicely as possible.

And I think Dean will really touch on really the cost-recovery provisions and how sometimes retailers will be making three, four times more over what the costs are. So that's very troubling.

With that, I very much appreciate the opportunity to speak with you. There's several other provisions that we are very concerned with. The one that is quite glaring is the fact that law enforcement only has the ability to delay notification for three days. There should be no restrictions placed on law enforcement.

You know, if they're in the process of investigating, sometimes you don't want the other guys know that you're investigating it. So the fact that there's only a three-day - ability to delay notification is three days is quite troubling. There should be no restrictions on that.

So there's a whole host of other little smaller concerns that we have along those lines. We do appreciate the sponsor saying that it's kind of a starting point. We welcome the opportunity to continue the discussions. With that, I'll turn it over to the two experts on the situation.

MR. SHEAFFER: Thank you for the opportunity to be here. Again, my name is Dean Sheaffer. I'm the Senior Vice President of Financial Services for Boscov's Department Stores. I'm also that company's Chief Compliance Officer. I've been in payments literally my entire adult lift, starting as a

part-time collector trying to earn some money for pizza, beer at the University of Delaware.

By the way, it's great to see you here. It's great to have you show up in Berks County here.

Anyway, I'd like to - really two parts. One's to talk just a little bit about what department stores, retailers and merchants in general do to protect the consumer data.

And then secondarily I'd like to talk very specifically about some of the topics that have been brought up here with respect to breaches of payment data.

So Boscov's has a set of business-continuity programs. I'm responsible for maintaining those. One of those business-continuity plans is data breach. It is somewhere between 80 and 90 pages long. It is constantly reviewed. It's constantly updated, outlined.

It's essentially a playbook for our incident response team to understand how a company prepares for events in response to and remediates and recovers from data breaches.

It has significant players for banking partners. It has significant players like our cyber-security partners. We have an insurance broker from

whom we purchase a very substantial cyber-insurance policy. That policy allows us access to notification experts.

Why do we have policies such as this? Well, because our Information Security Officer - or Chief Information Security Officer, couldn't be here today. He's heads down implementing systems on which we spend millions of dollars to encrypt both in-flight and at-rest data and millions of dollars on systems to identify and prevent intrusions, millions of dollars on systems to identify data that's being - counted to be exfiltrated.

We have programs in place where every coworker that comes on board is trained in aspects of know your customer, what our banking partners talk about, any money laundering, what our banking friends talk about.

We have special training programs for our IT staff to teach them how to code programs so that they are less susceptible to attack. We have - we contract for external services for both external and internal breach attacks. So it's people that have white hats, we ask try to go breach our systems, and do so from the outside. But also come in, plug into our network internally and see if you can breach our

systems. What that does is allows us to identify areas to remediate that may be relatively minor or something that needs to be addressed right away.

Part of the concern that we have is that the process by which a merchant or any other protects data is constantly shifting. That business-continuity plan, the agreements with our cyber-security provider, the training programs that we run, the tabletop exercises where we pretend like we've had a data breach and figure out how we're going to communicate to our customers, how we're going to communicate to our banking partners, how we're going to communicate to our coworkers, how we're going to communicate to the media, all of that constantly changes.

Why does it change? Because the vectors under which we are constantly attacked change every single day.

Boscov's, every merchant in this Commonwealth, if they have an internet presence, I guarantee you it's under attack as we speak right now. It could be a relatively minor attack. It could be a fishing attack.

One of the things that we do is we teach every coworker that has an email account what fishing is, which is an attempt to have an email, take you to a

bad website or otherwise cause you to open a document that will open up your PC, where bad things happen, including data breach.

We don't just train them. We actually have exercises on an annual basis where our Chief Information Security Officer and I will craft a campaign where we send out fake emails that are what a fishing email will look like. And if the coworker makes a mistake and clicks on that link, we take them to remedial training, because it's that important.

Why is it important? Because we are - the one thing that makes retail different from every other industry is the relationship of trust we have with our customers. There is no other place where you go in and you buy clothes for your family and you buy candy for your mom or flowers for your mom for Valentine's Day, there's no other place that has that kind of relationship other than a merchant.

And in order to enable that we have to collect information, the customers' names and addresses if we want to deliver a mattress to them, write their name on a card, information. If you want to take a payment at Boscov's, 90-plus percent of our transactions are card-based.

So what do we do? So what do we do to

protect that payment? We have models where we not only encrypt data, use point-to-point encryptions.

A lot of people talked about the Target breach. We'll talk about that a little bit more as we get into the second section, but we have systems that protect consumer data generally and then additional protections when there is sensitive information - sensitive information, payment card information, employees' social Security numbers or other sensitive employee data, HIPAA data. Each one of those has a unique and specific requirement for protection. And those unique and specific requirements change on a regular basis.

So it's very, very hard to create a cage in which we want to try to operate. If there has to be a cage, it should be at the federal level so that the standard for what are data breaches, what reasonable protections are and what the notification requirements are should be consistent.

Why? Because if you're a merchant - guess what, I have customers in every one of the 50 states. Yet God forbid, I'm breached, that means I've got potentially 50 different types of responses I need to deal with. That's why our insurance broker has cyber-security experts and know the state notification

requirements.

That's also why I look at the National Retail Federation's state legislative tracker. The last time I looked there were 26 legislatures that had data breach and/or data privacy bills that were in-flight. So not only do we have to look at the existing legislations, we have to help inform and educate the legislators across the country as to what the reality of the situation is.

So I'm going to pause there. I'd like go on to payment systems. So I happen to sit on the Board of Directors of something called the Merchants Advisory Group. The Merchants Advisory Group is the merchant-payment experts in the United States. So it's Walmart, it's Target, it's Marriott, it's Microsoft, it's Amazon, it's McDonald's, it's Southwest Airlines. It's merchants that represent $4.4 trillion in transactions. And we talk a lot about payments and the unfairness for merchants as they exist today.

So you guys probably heard about swipe fess. When you buy something at Boscov's and you give your Visa or MasterCard, on average we pay about two percent in swipe fees. So we only get $98 from our bank. And that swipe fee is intended to cover a lot of things. And one aspect is the fraud.

So the United States has some of the highest swipe fees in the world. And part of what's built into those swipe fees is to cover fraud.

Secondarily, the banks have - because we have an allotment through Visa and MasterCard, they have the ability to write unilateral rules. So there are rules about when a bank can charge that merchant for a fraudulent transaction. And they do it all the time.

So - oh, by the way, swipe fees costs us 8, 9 million dollars. One of the highest expenses other than payroll and our rent. Charge us hundreds of thousands of dollars. Sometimes because of legitimate reasons. Sometimes not so legitimate.

Nonetheless, there are many, many, many cases where the rules require a merchant to accept the chargeback no matter what the circumstances, no matter whether it was a bad actor or the 16-year-old son or daughter taking mom or dad's credit card and buying something that they didn't tell mom or dad about. All right?

So we pay for fraud once in swipe fees. We pay for it a second time in chargebacks. We also spend millions of dollars to comply with PCI. So - and this is the standard that was promulgated by the card

associations and the underlying big banks. I've got a lot of respect for the small bankers. They do a stellar job of serving the community. So my testimony is really more targeted toward the large banks, if you will.

So they have promulgated a state security standard that requires every merchant to protect their fundamentally broken system. What do you mean? Why is it fundamentally broken?

Well, have you ever looked at the back of your card? It has a magnetic swipe on it. Right? So my dad, who would have been 87 this year, had a reel to reel to play music. It has a magnetic stripe. It preceded eight-track tapes, it preceded cassettes, CDs and DVDs. And that's still the technology that's used on the back of every single credit card. Okay?

Well, then the banks rolled out chip-based cards, the cards with the chips in them. Sure, they did. Unfortunately they rolled out EMV cards with chip and signature. The rest - most of the rest of the world, the vast majority, EU, Australia, the vast majority of the world rolled out EMV with PIN.

Why? Because I not only have the card, I also have to know that four-digit PIN. So if I find John's card laying on the carpet and he walks out of

here, I can still go use that card. There's nothing that stops me from using that card.

If I know that that card was issued by a European bank, I couldn't use it, because I don't know what his PIN his. I just happen to find the card, it's useless to me.

So we paid for it once, an interchange of fraud. We paid for it twice in chargebacks. We paid for it a third time in millions of dollars of technology to try to rule out - to try to protect the banks' fundamentally broken system.

And now this Bill asks us to pay a fourth time, to recover the banks' costs to reissue cards that are fundamentally broken.

MR. MARTINO: Thank you, Mr. Chairman, members of the Committee. My name's Paul Martino. I am the Vice President and Senior Policy Counsel for the National Retail Federation.

I appreciate the opportunity to be here. I'm a native Pennsylvanian from Delaware County, born and raised. I left for college and unfortunately I didn't come back. But I, too, am a fan of not only the retailer mentioned here today, Boscov's, but also Wawa. Wawa has made its way down to the D.C. metro area, so I can frequent those stores, too.

I want to leave you with a few things. I know time is short, but I want to give a little more detail.

John mentioned with respect to the three things that we heard some of the inaccuracies in the previous testimony. And then I want to leave you with sort of four high-level points. And my goal here is to help bring maybe some of the context from other states from the Federal Government handling this issue here, because it does impact what you do.

As John mentioned, all 50 states, including Pennsylvania, have breach laws. So does D.C. I believe Guam military base, has a breach law. So there is - back to the national standard. That happened because the Federal Government, as you know, has trouble passing anything these days and has been unable to pass a preemptive breach law that would create a uniform system.

So as he mentioned, if a breach does occur, the retail industry, we're all going to comply nationally with every law, that's 54 jurisdictions.

Second, the Gramm-Leach-Bliley Act that was mentioned, if you were to pull it up today on Google and read it, you will not find a single word that says breach notification. It's not required

because it's not in there. The law predates from 1999 and the first breach law in California, that was 2003. So from 2002 to 2003 - the breach notice was in 2004. The Gramm-Leach-Bliley Act is 1999.

What happened? After the first breach notice occurred, Congress started getting legislation for data breach. That was 2005. The Banking Committee had some proposals, as did the Commerce Committee. I was on staff of the Senate Commerce Committee at the time.

By the time we were done that year, ten committees in Congress had breach Bills. The way the Banking Committee and the Senate handled it was that the interagency guidance for FDIC, the Fed, OCC and - I believe there was one other, might have been OTS, but four agencies issued interagency guidelines for the financial institutions.

And if you'll allow me, because I think this is an important thing to understand what's in the Bill and what the guidance provides, I just want to read what the Bill says and what the guidance says, so you have some context for why you would say that they don't actually have a mandatory requirement to notify of breaches, which is why JPMorgan didn't in 2014.

So the Bill says in Section 7, notice

exemption, a financial institution complies with the notification requirements that are described by the federal interagency guidance on response programs for unauthorized access to customer information, customer notice - very long title - is deemed to be in compliance with this Act.

And as the gentleman from the Financial Association - Banking Association mentioned, it requires that you have a response program. That guidance came out in 2005. When the guidance came out, the Banking Committee decided not to get involved with legislation because this guidance was in place.

Well, what does the guidance say? When it comes to customer notification of a breach, the subject is - and I can send this to you so you can read it - when customer notice should be provided. I emphasize should.

Interpretive guidance believes the financial (sic) should provide notice to its customers whenever it becomes aware of an incident. It goes on to say that customer notice - customer notice should be given. Notice should be. You go through this and you go through the entire interagency guidance and there's prefatory language like that, it's should.

It's what you should consider. It's

what you should do. It's guidance. It's not a mandatory requirement.

To the sponsor's credit, if you look at the language in the middle where notice is required, it says shall because that's what we do in the statutes. We require, we mandate, we say shall. We don't say should, you know, and so I credit him for that.

The problem is it's shall for everyone that has to be covered by the Bill, but then in Section 7 it says banks are a lesser requirement. It doesn't require them to actually notify. So there is a significant concern with the Bill.

I do want to mention on the JPMorgan breach, some of the details of that is troubling. We're talking, just to give you context, the same year - the same 12-month period as the Target breach and the Home Depot breach. Target was around Thanksgiving 2013. Home Depot was later in 2014.

Well, in August of 2014, in the same 12-month period, JPMorgan had a breach, Mr. Chairman, that affected 83 million customers. It was their log-in dimensions, user name and password.

How do we know this? They didn't notify. They filed an investor report, an 8K, in October saying - they only had to require a significant

risk to the business. So they didn't tell any of the affected 83 million consumers or small businesses, but they notified investors that we have an event of such significance that we have to - required by the SEC to report this, and that's how we found out about it.

On December 24th of the same year, 2014, the New York Times did an investigative report that came out two days - or one day before Christmas and no one saw it. It basically said the JPMorgan breach was a result of a flaw - a simple flaw in the security server. It could have been patched. It should have been patched.

Where did we hear this again years later, Equibank breach. Flaws. Should have been patched. Is Equibank required to have security? Yes. Under what law? Gramm-Leach-Bliley Act.

So we don't have comprehensive laws at the financial - for financial institutions that work, and yet this Bill, again, exempts them. So I think - one question was asked, and we'll talk related to budgets and silos, but we have silos in - in our breach requirements, a lot of things that could be done. We require everyone who handles sensitive information to have the same requirements to use with reasonable data security and have the same obligations to notify

consumers.

Another area John mentioned, that the Bill fails to be comprehensive. As a consumer you would expect - you would expect that if the company that has your information has a breach, you would find out about it. We should have - create significant incentives for having - the threat of, you know, violating, not giving the public notice or having to give the public notice if you have a breach.

Retailers face that every day in 54 jurisdictions, but many other entities don't. Cloud companies, Broadband internet service providers, anyone that counsels a third-party service provider, marketing company. What if they have your data? What if they have a breach?

Well, the Bill says that they have to tell us and we have to make notice for them. That's a lot of cost for us to do notice for them and they don't have the incentive to have the best and most secure system.

So who would want and who would support the idea of reasonable data security support and the idea of consumer notification? I don't think you have trust without transparency. But if we're going to have transparency, everyone has to be covered the same for

handling sensitive data. As a consumer, I want that.

I guess - so I did want to leave you with four high-level points that I thought were extremely relative to this and put you in context.

So the threats that the Bill mentions are very real. They are. We hear it. We see it. We see the reports from the FBI, China, Russia, North Korea. Who's hacking us? So state-sponsored actors a lot of times, one of the most valuable data they have.

This is why the most sensitive information, your insurance information, your health - insurance fraud, which is far more lucrative than credit card fraud by a factor of about 40 times. And they're looking for the most sensitive - you know, they need your financial information, your Social Security number, your bank account numbers. That's far more lucrative than the card.

On the black market the credit card number will be bought probably for about a dollar. The consumer doesn't face any part of that, never charged for those fraudulent charges. The impact's not the same as if they suffered an ID theft from a stolen Social Security number or their bank account is hacked and they have a chance of losing their data, losing their financial assets or having their health insurance

account hacked and someone using - you know, putting thousands of dollars of healthcare charges on their health insurance without their knowledge.

Those are real, real harms, but they're not covered by this law. They're not covered by this Bill.

The second - so the threats are real and they should be addressed and it's important to address them.

Second, security is not 100 percent. The Chairman of the Federal Trade Commission - multiple chairpersons of the Federal Trade Commission have testified before Congress that security is not 100 percent.

One of the most troubling aspects of this Bill is that if you look at the liability section, and I'm telling you where it is. So it's Section 8, under civil relief.

But my point is this. What the Bill does is it requires you have reasonable security. But then it says if you suffer a breach of security. So your obligation is to do everything that's reasonable, transactions you have and things like that. But the fact of suffering a breach makes you liable to the tune of $5,000 for every violation.

If security is not 100 percent possible, if you can buy the state-of-the-art, but you can't prevent China from coming in and stealing your data, should you be subject to $5,000 for a violation for every breach? I think that's unfair. I think that informs us why - I think the Bill should say if you fail to provide reasonable security, you could be liable.

But there's also a reason why it should be an AG enforcement. We're looking at state-sponsored actors breaching our systems and that requires some prosecutorial discretion. It shouldn't be the fact of a breach, even if you did everything possible, becomes an automatic $5,000 for every person, every individual. That would bankrupt almost every company. So that was the second point of four.

Three, hackers don't discriminate. They go where they can get the data. So that's one reason why everyone should be covered.

And lastly, what do consumers expect? We're here to provide the transparency to consumers. We're here to meet their expectations with notification. Our laws should also be comprehensive. We should be trying to defend them everywhere. And we ought to create incentives in every industry sector to

prevent those losses.

I could go on, but I know time it short. The payment recovery, I just would say that that section entirely should be dropped, for the reasons stated in the attachment to the testimony. The letter to Congress, this has been an idea and it's been around since 2007. It's been rejected by every state. It has been rejected by Congress for the reason that Dean said, retailers already pay three times over for the cost of fraud on the system. Having us pay for 400 percent of the cost of fraud is not necessary.

So I'm happy to take any questions, but that's my testimony. Thank you.

CHAIRMAN KELLER: Thank you very much for all three of you testifying about this. I think you outlined a lot of the troubling pieces that are troubling for you as retailers.

Are there any -?

REPRESENTATIVE CIRESI: Just a brief question. I guess I'll show my age, but more for you, Dean, from Boscov's. A great store, by the way. I like that. You're out toward our region.

As I'm sitting here, I'm thinking I'm never going to use my credit card again. I don't know if my wife will be happy, but you know, but - but what

we were paying prior to - and Boscov's has been around a long time. A big family-owned businesses. Around a hundred years or whatever it was.

MR. SHEAFFER: Little over a hundred.

REPRESENTATIVE CIRESI: Right. So there was always security issues when we did cash and layaway.

MR. SHEAFFER: Sure.

REPRESENTATIVE CIRESI: Percentage-wise, how much of an increase for your institution when we went full basically cashless and everything was on credit? Did you see - I mean, the security with cash - how much difference did it make?

MR. SHEAFFER: So I've been with Boscov's for 30 years, so - so the cash handling, bad checks, gift card fraud or internal gift cards or value cards is maybe one basis point, something like that. And the total cost, all in, for swipe fees, for costs for data protection, for chargebacks is 200 times that.

REPRESENTATIVE CIRESI: Okay.

CHAIRMAN KELLER: Representative Solomon?

REPRESENTATIVE SOLOMON: Thank you, Mr. Chairman. So I understand the critique on who the Bill captures and the cost-recovery provision. I think we

just respectfully disagree on the need for a private right of action.

So you know, I understand theory. John, you mentioned about this is going to open up the floodgates and this idea of it's going to bankrupt companies. If you'd just talk about what, though, is happening on the ground.

Right now in Pennsylvania, in theory, if my banks breached, in light of the decision, I can bring a case. And the bankers brought up - they brought up this - the article that was written about Dittman. What that article tracks is after Dittman in Pennsylvania right now what's happening on the ground.

What the article says is, in light of Dittman, since November of 2018, three - three cases have been brought that cite Dittman and use negligence to try and establish breach. Three. And the three all relate to one breach, which is the Capital One breach, which was just egregious misconduct, 220,000,000 Americans suffered from that incident.

And arguably you could even say that that breach - that those cases began before Dittman and they just sort of added that on because the Supreme Court came out with the guidance.

So I'm just not - where's the data on

what's going on right now? Because anybody now - all of the millions that have been affected by this could bring suit today.

MR. MARTINO: Thank you for the opportunity to respond to the question. What you're talking about is litigation - I think it's going to be one reason why the financial institutions are opposed to it. That has to brought based on tort negligence, because there's no other remedy to federal law or state law to bring those actions against financial institutions. So that's why they're resorting to negligence.

With the Capital One breach as mentioned - Wells Fargo. Wells Fargo is opening new accounts in your name, so their associates could get better compensated by looking like they had generated more business.

So I think you have to - you have to look at it perhaps on the basis they're - as I mentioned before, we're subject to 54 laws, state and federal territories. Those laws are enforceable by the state Attorney Generals. In many cases they're enforceable in other ways. So I think that, you know, if there's a concern you have with respect to some certain types of breaches that perhaps where there are

gaps in the law, I would - I would look to that in terms of just to get a sense.

So Verizon does an incident report, a data breach report every year. If you go back into these reports, you'll find that at least in the retail industry we calculate perhaps about five percent, and it's going down every year as we were tracking. That's five percent of all breaches.

The vast majority of breaches are financial institutions. Why? There's a famous quote of why are the bank robbers running our banks? That's where the money is. And it's where the sensitive data is. And so I think there are reasons and would love to sit down with you and talk with you further about where there are gaps in the laws.

As I mentioned before, we're not shying away from our responsibilities. We think everyone should be covered. We think everyone should have security standards, reasonable security standards appropriate for their business. Joe's Pizza should not have the same security standards as a bank with a trillion dollars in assets. It's completely different.

The sensitivity of the data is different, what can be done with the data, the potential harm to the consumer. As I mentioned, Joe's

Pizza might have your card number, might. The consumer's not going to pay if there's a breach. The retailer's going to pay. And it's going to be covered by the damages as bad as it would be if, you know, your bank lost your Social Security number in a breach like Equifax did in their breach.

So I think - I think there are places where laws can be targeted. New York has realized this. The New York Financial Department, I forget their exact name, realized there were gaps in the law, realized there were gaps in the federal law. Put a 72-hour breach notification requirement on financial institutions.

Banks in Europe have a 72-hour breach notification requirement, as do anyone who's under the requirement, what's called the General Data Protection Regulation, GDPR, that's doing business in Europe subject to that breach notification law.

So there are ways to do this. I think the best way is we agree the banks are missed and have a federal law that sits down, you know, uniform standard for all entities across the country.

But politically, I'm not sure Congress is ever going to get there. I've been working in Washington, D.C. since 2001. I was on the Committee

for four years. I've been working as a lawyer outside that since 2005. I came to this from Silicon Valley, after seven years in Silicon Valley. I've been handling technology data security and things like that.

So I'm not sure Congress is equipped to actually get to a solution. So if states - and I think it's their right to protect their citizens, to want to find where there are places, where there are gaps in the law.

And as you know, here we contend the cost- recovery method was fully covered already, but there are - there are gaps in the law, such as Gramm-Leach-Bliley not having the notice requirement. I think that's the perfect place to look at - to look at ways that that can be addressed, as New York State.

CHAIRMAN KELLER: Thank you very much for your testimony. We appreciate it today.

MR. MARTINO: Thank you.

CHAIRMAN KELLER: Next up will be Professor of Information Sciences and Technology, Mr. Liu.

PROFESSOR LIU: So good morning. Thank you for the opportunity. So I'm a Professor of Information Science and Technology and Director of the Center for Cyber Security, Information Privacy and

Trust at Penn State University. We were nominated by National Security Agency, Department of Homeland Security as a National Center of Academic Excellence in Information Assurance Education.

So my goal here is to provide a few comments on the technical aspect of data breach since I am a researcher, so I just want to share a little bit of my understanding about how the cyber criminals use technology to steal data and data breach.

So first, technically speaking, I think the cyber-security problem is really caused by two basic characteristics of cyber systems, including your phone, your computer and internet.

So first is vulnerabilities in software platforms. The second is psychological weakness in human users.

So cyber criminals, they already know how to automatically exploit these vulnerabilities and steal personal data. By automatically I mean manually, so using the people to manually steal data. No, that's old-fashioned. They do it manually on malware. Today's malware isn't sophisticated and very powerful, from a scientific point of view. So I will give you an example to support my opinion why today's malware isn't sophisticated, automated and not very powerful.

So my example, a study shows that the Target 2013 data breach could be resulting from a widely used malware called Citadel. In case you are in the - in the cyber community this is a well-known name, okay. It's widely used malware. It's sophisticated type of malware. I'll give you a brief description how cyber criminals use Citadel in a step by step, resulting in a data breach in 2013, Target.

So step one, the cyber criminal needs a server that is hosted by a company to run malware. Such companies are called bulletproof hosting, bulletproof hosting. And some foreign countries allow such companies to exist. So probably not running in our nation but in some foreign countries.

Step two, the cyber criminal buys the Citadel key for about $3,000. That's the aftermarket price of this malware.

Step three, the cyber criminal installs and runs Citadel on this bulletproof hosting through the service from those companies. Next, the Citadel malware will automatically create a small piece of bot malware. So that's the sophistication. So after you install the malware software, you first automatically create a computer to launch smaller bot malware. By bot I mean Java the malware will automatically use and

run. And then the bot malware conceals - it's actually a way to avoid antivirus. So you can see why this breach is hard to handle here for many reasons. And then to make sure you have antivirus protection.

Step four, Citadel distributes the creation of malware to a large number of, malpacks.

As many as two million malpacks are used a year. Okay. So the real world malware attack, they are serious. And these websites were previously impacted either by Citadel, the malware itself or by other malware. So you know, there are some collaboration in the hacking community, of course is involved in some of the payment.

And why millions of websites could be compromised during this stage is due to the first high-risk system I mentioned to you, which is the vulnerability in software and hardware, okay, because today's software is too complex to even identify all those vulnerabilities, let alone verifying that your software, hardware do not have any vulnerabilities. That's just beyond today's science.

Okay. Step five, establish that employees of a contractor of Target, not really the Target company, it's a contractor of Target, which is an air-conditioning firm in Pennsylvania. I guess it

happens to be a firm in Pennsylvania.

The employees of this contractor had one of the malpacks. Given two million, including many popular websites, are used, so you cannot assess the likelihood that an employee - a criminal may access one of these websites. And due to drive by download, the bot malware was automatically installed on the employee's computer without consent.

In many cases, the malware does not need the employee. The drive by download vulnerability has the ability to enable the malware to automatically install a bot on the computer. So if there was a bot on my computer, I really am not very surprised. Okay. You don't have to be a researcher because today's software, some give you a little patch to make it up to date, then it's likely to have such vulnerabilities.

Then the next step is step six. The bot malware conceals credentials used by this employee of the contractor.

Step seven, a study shows that the malware used the stolen credential to log in onto a particular bank which is part of an external business system of Target. By external it is a system used by contractors to get payment from Target.

And importantly, this bank is also

accessible from the corporate network of Target. So there is evidence that a system of employees of Target can access this. So this problem with the malware is a stepping stone.

So next the malware is hypothesized that the malware is going to compromise the back end ability, of course, using the stolen credential from the contractor. After the back end is compromised the malware could move on and overtake the credential of a Target employee. So this - this employee could be a victim. Then using this credential, the malware could access the corporate network of Target because this is accessible from the corporate network.

And then next the malware could access many, many pulse devices used by the Target source. That could be many, many Target sources. As we know, today millions of credit and bank cards were stolen from those compromised pulse devices.

Then you have step nine, which is the last step. After those personal data are stolen, the malware usually goes to a global black market. So the black market, which is called underground economy, is being analyzed.

So what about today? The price tag for one type of credit card credentials ranges from $35 to

$135. So basically anybody can go to the black market and pay this amount of money for the credit card. We looked at the price influence from a recent data breach.

So I will stop here and will take any questions.

CHAIRMAN KELLER: Thank you very much for your testimony there. You brought up quite a few things to light that I didn't know. I'll say that, you know, and that you actually can go out and purchase a compromised credit card. I didn't realize that, you know.

Any other questions? Thank you very much for your testimony. Appreciate it.

PROFESSOR LIU: Yes. Thank you.

CHAIRMAN KELLER: All right.

Next up is our Pennsylvania Association for Justice. And you may begin.

ATTORNEY RIHN: Thank you very much. My name is Aaron Rihn. I'm an attorney from Pittsburgh, Pennsylvania, the firm of Peirce & Associates. I want to let you all know that I'm very excited and nervous to be here. I think this is a wonderful opportunity that you're giving me. Most of us don't get a chance to come and speak to the legislature about issues that

really impact them and are important to them. So I really thank you for giving us this opportunity. This is great.

Unlike my colleagues here and probably everybody else in the room, I'm not really an expert on data-breach legislation. I'm not an expert in data-breach litigation. I don't really handle data-breach cases. I'm just a personal injury attorney.

But what I am an expert in, I believe, is being a data-breach victim, which is kind of what I wanted to come in and talk to you about a little bit today.

Dan is a personal friend of mine and we were talking on the phone about another issue and he told me that he was doing this. And I said, you know what, Dan, I would like to come and speak for just a few minutes myself to kind of relay my story and give my thoughts.

Some of you might be a data-breach victim as well. And there are different types of breaches. But I can tell you it really stinks. What happened to me really stinks. If you haven't gone through it, sometimes you don't appreciate it.

I was a victim of the Equifax data breach. So as a result, my name, address, birth date

and Social Security number are out there in that - I don't know who has it. I don't know what they're going to do with it. I don't know what they can do with it. I'm not a cyber criminal.

But it doesn't make me feel very good. I know that every single year somebody tries to get my tax return from the IRS. Is that related to this? Probably. Now -.

CHAIRMAN KELLER: But we just heard I can buy that for $35.

ATTORNEY RIHN: I found out I was a victim because I received one of these letters in the mail. And along with that letter I think there was an offer of one year's free supply of LifeLock security.

Well, I knew what that was, so I looked it up and, you know, I ultimately decided that, you know, I better take advantage of this. Plus what other option did I have? You know, it was kind of a take-it-or-leave-it presentation, so I took the one year of free LifeLock.

And then, you know, the year ran out. It ran out. You know, I'm like what am I supposed to do now? My information's still out there. I mean, presumably it's going to be out there for the rest of my life. I think I got to continue this LifeLock. And

I think I'm paying $20 a month for this, you know, which is $240 a year. And presumably I'm going to keep paying that for the rest of my life.

Now, I'm kind of blessed in a sense that, you know, I'm an upper middle class guy. It's - I don't feel like spending $240 a year on security protection, but I can. You know, it's not going to keep me from making a mortgage payment or a car payment.

But you know, there are a lot of people out there who can't really afford $240. That's a lot of money to some people. There could be a single mother of three out there for whom that is her entire mortgage payment. She just flat out cannot make it. So she doesn't have an option. She not able to protect herself, because she doesn't have that $20 a month.

She's probably less able to take care of herself in other ways as well, due to the lack of resources or whatnot. So you know, those are the kind of people that I care most about with respect to these sorts of issues. And that's kind of why I asked Dan for some of his time.

So the first thing I did when Dan graciously agreed to give me some of his time was to take a look at the Bill that was - the Act that was in

place right now. And the first thing I noted was that, you know, it was enacted in 2005.

I don't really remember what I was thinking in 2005, but I wasn't very aware of data breaches at that time. I don't seem to recall them happening with nearly the frequency that they're happening today. And I think this area of law is probably more important than any area of the law to stay up-to-date.

So you know, my first thought was, well, this things probably needs to be looked at again, refreshed, tightened up. But then I also kind of looked at it and I'm like, okay, here's a section that says if my data is breached, they have to notify me within a certain period of time. And I thought, well, you know, that's great, because I'd want to be notified.

But I didn't see the section that says they have an obligation to keep my data safe. That's not in there. And I was really kind of surprised by that, because to me that's even more important than the notification provisions.

So you know, I've heard a lot of testimony today about various, you know, federal or other state provisions that might or might not govern

people who might have my data, but I would like to know for sure that the Commonwealth of Pennsylvania is doing something to require businesses that have my data to take reasonable measures to secure it. I don't think that that's too much to ask and I don't think that's really too much of an imposition upon these businesses.

You know, I heard a number of the other people this morning speak. And you know, basically what I was hearing from them is, we don't want to be sued. And I understand that. I don't want to be sued either.

And I don't want to have to sue somebody, but I also don't want you to be negligent with my personal data. And as Representative Solomon pointed out, you know, the genie is out of the bottle as far as the ability to bring litigation in these cases. The only thing that you all have to decide, in my opinion, is whether you are going to dictate under what circumstances somebody may be held simply liable for failing to properly secure data or if you're going to enforce it.

There's a lot of reasons why I think it's better for you to do it, okay, because we can go through this collaborative process. You know, you can, you know, iron out multiple versions of this Bill, work

on it, work on it, work on it, and try to get it as close to perfect as you can. That's not going to happen in the court system. I can tell you that right now.

You know, is the current version of the Bill perfect? No, I'm sure it isn't. But what I'm excited about is that we're here talking about it. You know, I kind of applaud you all for taking the initiative to do something here, because it's very important. I know today is not the end of the road. You know, today is kind of the beginning of the road. But I anxiously look forward to seeing where you're going to go from here.

Just a few more small points before I turn it over to Dan. I heard somebody earlier, I think it was with the retailers, talking about, well, you know, you shouldn't be able to just sue any time your data is compromised. You should only be able to, you know, bring action if you can show damages.

Now, I don't know what that means, you know, showing damages, because - does that mean I have to go and wait until somebody has stolen my identify and I have incurred some sort of cost associated with that before I have a cause of action against you? I just - I don't think that's the way we should go here

because, as I mentioned earlier, I incurred damages the second that my data is out there. And I've got to affirmatively spend money that I'm lucky enough to have, but some people don't, to go out there and take reasonable measures to protect myself.

And that's one reason why we need - some sort of statutory damage, whatever it might be, is a really important component to this legislation because then, you know, a single mother of three doesn't have to wait for her identity to be stolen to go out there and take the measures she needs to protect herself. You know, she can - it's - she can pursue some sort of recovery right off the bat and, you know, secure whatever she needs to help her go out there and do that, protect herself and her family.

So I think that's most of my points. Again, I really thank you for giving me the opportunity to speak. This is very important to me. You can tell I'm pretty passionate about it. So I'll turn it over to the other real expert, Dan.

ATTORNEY LEVIN: He knows how to put pressure on me. As Mr. Rihn introduced me, my name is Dan Levin. I work at Levin Sedran & Berman. We're a law firm located in Philadelphia. We do pharmaceutical drug liability work, class-action work. I don't know

that I'm an expert on data-breach security, but we have had handled data-breach litigation.

I'm an expert on litigation. And one thing I can tell you is nobody likes to be sued, and that includes lawyers. Lawyers are subject to liability under this Bill. When there is a data breach at a law firm, we hold medical records, we have Social Security - we're subject to exposure for wrongdoing if we don't provide reasonable measures to protect that data.

Not only are we exposed to liability, we have a potential ethics violation for allowing personal information of our clients to be disclosed. Does that make me feel good as a lawyer that I can be sued? No. Does that make it wrong that there should be a law in place that provides an avenue for someone who's been wronged by me to sue me? Absolutely not. That's why we have laws, to protect individuals who are wronged.

It doesn't mean that the person being sued is public enemy number one. It doesn't mean they should be tarred and feathered in the streets of Philadelphia. It means that they made a mistake. They were negligent and they allowed information to be disclosed. And that's why we have laws in place for regular people who've been wronged to be redressed,

whether it's from data breach, whether it's malpractice, whether it's any type of wrong that's done to you.

So we've heard from a lot of speakers today who talked about didn't like the fact that they were going to be sued. I can respect that. I don't like the fact that I can be sued. That doesn't mean it's wrong to have laws in place that hold people responsible who fail to act in accordance with the standard of care. And I think that's what this law does.

I want to also emphasize that data breaches don't just hurt the privacy of consumers. Aaron talked about that with this committee, that's personal to everyone here. You obviously want your personal information protected. But data breaches happen for businesses also in Pennsylvania.

You know, as a law firm, if we have a breach of data, that's going to affect our business. It's going to affect who's going to want to retain us as a lawyer if we don't put in proper standards and places to protect an individual's data. It's going to affect small businesses.

If you're a doctor, any type of entity that's protecting data, it's incumbent upon you to

protect that data. And I think that's where it's important for the Commonwealth of Pennsylvania, and I'm thankful for this committee for taking us this issue - to provide the standard - the ground rules in place to help law firms like myself, where I work, help small businesses and help big businesses understand what it is we need to do to protect information.

Now, I heard the bankers. They talked about, well, the Federal Government does this already. They even cited to a couple of federal regulations that regulate them. However, the Federal Government did not tell the states not to take action. In fact, the Federal Government - and they do that sometimes. The Federal Government will pass legislation, as you know, and they'll say, we're taking over this area of law, stay out of it.

They haven't done that in this case with data breach. And they specifically have allowed states to pass legislation that doesn't conflict with the federal regulation. In other words, they set the ground rules and the expectation is for the states to pass similar legislation so long as it doesn't make it impossible to comply with other legislations to be innovators of what is appropriate standards to protect individuals and their privacy.

So I don't think any of the federal regulations that were identified here by the bankers really is a reason for Pennsylvania not to consider legislation in this matter and consider ways to protect the residents of the Commonwealth of Pennsylvania.

In fact, Congress expects Pennsylvania to do that. They provide it in the Gramm Act that's cited by the banks. There's a section in that that specifically provides that they should. This does not restrict a state from regulating this area. And the reason is, is they want the states to confirm and pass legislation that allows for protection to consumers.

That's why we have a federalist government. We have a Federal Government and we have 50 states. And it's expected in most areas of legislation that the states are going to decide what's best for each state, for their consumers. Hopefully Pennsylvania, and I'm thankful for this committee for taking this up, will take that step and look into what is the most appropriate way to protect the privacy of individuals.

We do that all the time. We do it with minimum-wage laws. We do it with all types of legislation where states take it upon themselves to pass standards that they require upon businesses in the

Commonwealth. And businesses are able to comply with those state laws. It doesn't cause problems for businesses. I think it's appropriate in this circumstance that Pennsylvania protects the privacy interests of Pennsylvania citizens in conjunction with what the Federal Government is doing.

We know that the data breaches protect the - they hurt the economy. They hurt businesses when there's a data breach. They hurt their reputation. They hurt transactions with consumers. Consumers are afraid to perform transactions because they're worried about their privacy interests. So there are many reasons to pass legislation that helps protect privacy of consumers. And also it helps the interests of businesses.

What - Jared Solomon - State Representative Jared Solomon brought Dittman. There is now a cause of action, I would say. I would call it the Court - Supreme Court of Pennsylvania found that there was a duty for individuals who have sensitive information to take reasonable standards to protect.

That was unclear before this Supreme Court ruling. It was many District Courts and File Courts and even I think Federal Courts found that there wasn't a duty owed to the consumer to protect their

sensitive information. So therefore, you didn't have a claim under negligence.

The landscape has changed now. Now there is a duty, as pronounced by our Supreme Court, states a duty exists. What that duty is, I think that that is going to be determined by the courts. What is a reasonable standard of care, that's going to be determined in many ways by businesses, by the industry standards that they're going to incorporate to protect information.

But when the Supreme Court made that announcement, I think it would be helpful if the Commonwealth of Pennsylvania, this committee, and it would be helpful to consumers and to businesses to set - to now take our testimony, which you have, and set the parameters of the legislation. And that way you can protect businesses and consumers so everyone understands what the rules of engagement are and what's required of them. And that will help businesses and also ultimately help the privacy of individuals.

And I think one of the most - one of the things I want to address is the statutory damages. I just want to briefly discuss - go over this. I think that is something this committee should consider.

Mr. Rihn talked about how he - when he

had a data breach, he had to pay for services to protect his data. One of the problems, from my experience, with these cases is when you have your data stolen, you don't know when your damages are going to occur. It might occur one year from now. It might occur five years from now. It could occur ten years from now.

Once someone stole your data, you don't know when that damage is going to hit. And when that damage hits - let's say you suffer - you find out that your credit card was run up six years from now. It's going to be very difficult, if not impossible, to prove that that damage that occurred six years ago was a result of that breach that occurred.

That's what the courts would call causation. Your damages were the result of that breach. When you provide - I think it's incumbent upon the committee to find out - to come to a determination what's an appropriate value to provide for statutory damages and it's something for you to consider. But providing a causative action where it provides a damage, it gives notice to the business community as to what their exposure is going to be, but it also provides, in that case, for maybe that - as Mr. Rihn described, a single mother who is in their 20s who had

a data breach, who may not be able to prove that her damages were caused by that data breach, it provides what I would call an estimated damages as - as provided by this committee. It provides that individual with a causative action and gives them an opportunity to be redressed for the harm that occurred.

So in closing, I think this legislation is an important step in protecting the privacy of individuals in the Commonwealth and also protecting businesses. And I'm happy to answer any questions that the committee might have for both Mr. Rihn and I.

CHAIRMAN KELLER: Thanks. Thank you very much for your testimony. Representative?

REPRESENTATIVE ZABEL: Gentlemen, thank you for your testimony today. I'm thinking of a couple points that may not have been touched upon earlier.

First, on the federal standard, I think it's true, it'd probably be easier if we had a federal standard. But at the same time, my job as a state legislator and I think everybody here, we're interested in exploring solutions because we can't just sit back while all this is happening and cross our fingers and hope a Congress that's deeply polarized gives us direction. It's just not going to get us anywhere. So I think this is something we should be exploring and

I'm grateful that we're having this conversation and it's a productive one.

But I'm also thinking we need to put a human face on what's actually going on here today, because I heard something today that made my head spin, which described the banks as the victims in this case, which they are certainly not. The information that's being stolen is the consumers'. It's their data, their information. They're the ones - it's like calling the house a victim of burglary?. No, it's the people who live there. It's the people who are the victims. I think that's really important.

And one of the reasons I think we need to act on this, we also heard about this broken bank card system because they pay a lot of this - a lot of the costs involved. But they only pass the costs down to us when we buy things. So the consumers are ultimately also paying into the system that keeps getting breached. And it seems to me that a system for redress for them is entirely appropriate.

One thing I wanted to ask you about, because I see some parallels between litigators - some other types of litigation. Something I've said is that institutions should be help responsible for third parties and their service providers. But we know as a

matter of course that's not true in other aspects.

I won't use Boscov's, because Boscov's is a wonderful company. Let's say Kohls. Kohls provides bad security - they have some bad security guards and some bad people come in. They can't come back and say, well, what do you want us to do, we hired security guards, it's their fault. That doesn't work that way in litigation. Under the circumstances, yeah - you step up to the -. Just because you have a system in place doesn't absolve you of responsibility in virtually any other aspect in society.

ATTORNEY LEVIN: It pretty much comes down to your own duties, right. If you have a duty, then you're going to be responsible if harm comes from your failure to act reasonably with respect to that duty regardless of whether some third party came in here and initiated it.

And the security situation that you mentioned is probably the most - you know, that's something that we see all the time. I, as a personal-injury attorney, I see those cases all the time against, you know, hotels, bars. You know, if - if somebody goes into a bar, drinks 24 shots of whiskey, gets in their car, drives home, kills some - you know, kills some family of four, the bar doesn't get off the

hook just because the drunk driver, you know, committed a criminal act.

No, you know, the bar had a duty to me and everybody else out on the road to prevent that drunk driver from doing that. You know, I think that's kind of analogous.

ATTORNEY RIHN: I would just also add to that. I think Pennsylvania and nearly every other state has already decided that if there isn't a breach of privacy information that you're holding, regardless of whether it's your fault or not, you have a duty at that point to notify the individuals that had - had their information breached. That's not saying you were a bad person, just the standard of care is to notify the individual.

However, and I think this is important to emphasize, under this law, it doesn't - that doesn't mean that that company is going to be liable to every individual who had information stolen. Under this law that - in other words, once there's a breach they got to notify you. But in order for you to recover damages for there being a breach, you're going to have to demonstrate that that company did not provide the standard of care, the industry standard, whatever it may be, to hold that information properly.

And I think that's important and it was kind of missed a little bit in some of the testimony today, that this is not what I would call a strict liability statute, where if something bad happens, you get damages. You have to - if something bad happens, you have to be notified. But to get damages, you have to show wrongdoing.

I think that was a little confusing earlier, created some of confusion by that point.

CHAIRMAN KELLER: Do you have a question?

REPRESENTATIVE SOLOMON: Yes.

CHAIRMAN KELLER: Representative Solomon?

REPRESENTATIVE SOLOMON: Thank you, Mr. Chairman. To that point on damages, do you think that proving actual damages in a cyber breach is difficult?

ATTORNEY LEVIN: For a consumer, for an individual, yes. For a bank, not so much. Banks have card costs. They know how much it costs to replace the credit card. They can tabulate the damages that they have when there's a breach.

For an individual like you and I, it's going to be very difficult for us to prove what our damages is. I believe we have damages when it occurs,

but that damages may occur five years from now. Once your information is stolen, it's out there. And I think, as we heard today, the bad guys have the information then.

When they act on that information, I don't know. It could be three years from now, it could be five years from now, could be tomorrow. Then, once they act on that information and you suffer damages and you're alerted that someone signed over your mortgage or you have a credit card debt, then you're going to have to prove that those damages occurred because - maybe it was Wawa.

But a good defense attorney like - if it was Mr. Rihn - you can blame it on another company. You can't prove that it was Wawa. Look at all these breaches. It could have happened to someone else. And it's a good argument. And that's what makes it very difficult to prove damages in any case.

And that's why I alluded in my testimony, I think it's very important that there be some form of damages that are provided to the law. What that damage total is, I think that's for the committee to take testimony and - and discuss.

I think $5,000 is a fair amount. But reasonable minds can differ on that. So I think that -

but something needs to be provided to the consumer. Otherwise the law doesn't have the intended effect that I think we want it to.

CHAIRMAN KELLER: Thank you very much for your testimony. You did very well.

ATTORNEY RIHN: Thanks for having us.

CHAIRMAN KELLER: Our last testifier, a past colleague of mine from the PA Coalition for Civil Justice Reform, Curt Schroder. Curt, you can start whenever you wish.

MR. SCHRODER: Thank you, Chairman Keller.

Chairman Keller and members of the committee, good morning - I think it's good afternoon. My name is Curt Schroder. I'm the Executive Director of the Pennsylvania Coalition for Civil Justice Reform. The Pennsylvania Coalition for Civil Justice Reform is a statewide, nonpartisan alliance organization. It's dedicated for fairness to our courts by advocating awareness of civil-justice issues and advocating for legal reform in the legislature.

House Bill 1010 addresses a serious problem of data breaches. We hear much discussion of data breaches in the news today. The Associated Press recently reported that the Justice Department charged

four members of the Chinese military with breaking into networks of the Equifax credit reporting agency. And it's been discussed several times here today.

Tens of millions of Americans had their personal information stolen, making it one of the largest acts in the history - in history, targeting consumer data. But while individuals were victims of this breach and this crime, so, too, was Equifax the victim of a crime. And so, too, was every other entity, regardless whether it's a bank, regardless of whether it's a mom-and-pop store, regardless of whether it's a nonprofit.

They're all victims in the scenario, in this scenario, in the situation. Any business, large or small, for profit or nonprofit, is a victim of a crime when their security is breached.

Everyday businesses are under attack by bad actors seeking personal data for criminal purposes. The internet, smart phones, personal computers and other electronic devices have transformed the way commerce operates.

Every company in Pennsylvania, whether it's a small pizza shop, a multinational corporation or a nonprofit service organization stores data regarding its employees and customers. In our zeal to protect

consumers, I would urge that we not punish the other victims of these criminal acts by imposing burdensome and often unnecessary litigation.

In fact, the big issue that I have with this Bill is it's not so much a data-protection Bill as it is a litigation Bill.

House Bill 1010 encourages residents of Pennsylvania to file suit when their data is accessed through a breach. This is regardless of whether the individual suffers any actual monetary damage or loss. You'll recall earlier in the hearing when the Office of Administration talked about the breach, you know, it could be just getting over the fence and not actually getting on the wall of where the actual data might lie.

And while actually a common law exists for victims of a data breach, House Bill 1010 goes well beyond the common law and creates some reasonable litigation risks for entities that took no action themselves to harm consumers. This Bill creates a separate right to recover with a duty for an entity to take reasonable measures consistent with the nature and size of the entity.

Now, reasonableness is a concept, as we've heard today, associated with negligence claims and negligence lawsuits. It's also a case study in

victims. The standard offers no guidance to businesses of any particular size, whether nonprofit or for profit, as to what steps they are expected to take to prevent the data breach. And while lawyers might want to argue and wax eloquently about what constitutes reasonableness, there is no guidance in House Bill 1010 to help a business know whether it is in or out of compliance.

I will point out that there are other statutes in different states. We heard suggestions about a federal standard, which I, you know, think is also a good idea, but admittedly out of the control of this committee.

But there are other statutes out there, such as those found in Ohio and New York, which I believe also use a reasonableness standard, but they also provide actual data-protection standards to be met and provide a business entity with some certainty so that they know when they're living up to their responsibilities under the law. And I would urge that this legislation do the same, should it move forward.

House Bill 1010 contains a three-year statute of limitations, which is longer than that found under common law. We've heard much about House Bill 1010 allowing the minimum recovery of $5,000, even if

the individual has not suffered monetary damage. And I'll have more to say on that.

House Bill 1010 suggests victims of a crime recover damages, something that I don't know that we talked about today. That's three times the actual damages or three times the enumerated $5,000 minimum recovery. This creates a class action that only benefits the plaintiffs' attorneys who bring these lawsuits.

In addition to possibly three times the amount of damages, the crime victim must pay the plaintiffs' attorneys' fees and costs in addition. Arbitration agreements are voided, forcing the consumer and the business to endure the delays, inconvenience, conflict and uncertainty that goes along with adversarial litigation proceedings.

The committee should ask itself, do we want to solve this very real problem of preventing data breaches or do we want to create a litigation bonanza for attorneys through encouraging class-action litigation? And there's only one winner in class-action litigation, and that's not the plaintiff members of the class on whose behalf the suit is brought.

We heard from the previous panel about the necessity, they believe, for specified damages in

this. And they point to, you know, the possibility of not knowing whether, you know, you have actually monetary damages for quite some time down the road, seeing that as a reason why that provision should be in here.

But there's another reason why this is in here that has not been discussed and that is because it will allow class actions to be formed and provide huge pots of money in which these class-action plaintiffs will benefit very little, as individuals, but the attorneys bringing the suit will get quite a windfall.

Studies found the overwhelming majority of class-action members receive little or no benefit from class-action lawsuits. Even when class actions are settled, a percentage of class members who actually receive benefits are miniscule. Many do not know about litigation. Some never bother to collect the money that - money owed them.

The class-action litigation system labors under an inherent conflict between the interests of the lawyers who bring the cases and the interests of the class members. Too many cases are filed based on the ease with which the settlement may be extracted and too many cases are settled with illusory benefits to

class members and large fees for the attorneys.

Recent court challenges to proposed settlements have illuminated the prevalence of these abusive practices. And I want to turn your attention to a website, an organization called the Center for Class Action Fairness, if you want to learn more about the type of things I just talked about. It's headed by a brilliant attorney named Ted Frank, who, like I said, would be happy to provide this committee the important information on the impact of class actions.

Most class actions today are created not by injured consumers seeking redress but by plaintiff lawyers looking to recover substantial amounts in attorney's fees. Plaintiff lawyers have taken control of the consumer class action mechanism and turned it into a big business that uses the threat of litigation and potentially real damages to pry billions of dollars in settlements and hundreds of millions of dollars in legal fees from business each year.

And I submit that that's precisely the danger of this litigation. A company could be wiped out and financially ruined if the personal data of let's say thousands of individuals is criminally stolen.

Let's take the example of 10,000

individuals who have their data stolen and they become 10,000 members of a class. With a payment of $5,000 each pursuant to this Bill, that would result in $50 million in damages. And that is before traveling the courts, going to trial, which would bring the award to $150 million. And let's not forget the Bill also provides, on top of that, that the defendant pay the attorney fees and costs.

And who benefits in this? The plaintiff lawyers would get roughly one-third, or $50 million, of that trouble award while the consumer gets his $15,000 each. And that's if they collect it. Or the attorneys will get $151,515,152 of a nontroubled award under this example, while the consumer gets $5,000, once again, if they collect it.

Data breaches victimize the individual consumer and the entity that is broken into by the criminal actor. Both classes of crime victims deserve to be treated fairly. Is it reasonable to expect any business to be so secure that foreign military intelligence cannot penetrate? I don't know the answer to that, but it seems to me when Pennsylvania businesses are pivoted against perhaps foreign military intelligence, they're going to be at a big disadvantage every time.

And perhaps the best argument against the vague reasonableness standard obtained in House Bill 1010 has been raised by the attorneys themselves. As Mr. Levin, who just testified before me, points out, attorneys are subjected to standards for protecting against data breach in the rules of professional conduct. But just last week The Legal Intelligencer contained an article reporting more than 100 law firms had reported data breaches, and the picture is getting worse.

In the article, Attorney Kevin Baker pointed out that the rules of professional conduct require attorneys to take reasonable steps to protect their clients. In other words, the similar reasonableness standard to what's in this Bill. Attorney Baker, however, argued that because the rules contain no specific technical requirements, attorneys are placed in a difficult position of trying to determine what is sufficient to meet the reasonableness standard when it comes to cyber security.

Attorney Baker points out that what was considered reasonable yesterday is not reasonable today. And today's standards will be obsolete tomorrow. And what is reasonable for a large firm may not be reasonable for a small practice and vice versa.

So I would submit that if attorneys themselves are - you know, find themselves in a difficult position under a reasonableness standard, you know, the same is true for businesses in Pennsylvania. And I do believe that we need to remedy that by reviewing some of the other standards set forth and the technical standards and requirements set forth in some of the other state laws.

So I would ask that this legislation not be moved in its current configuration. I'm hoping you consider it using a standard with technical specifications with which businesses of all sizes can understand and comply and avoid incentives to bring litigation with little benefits to the individual, a windfall to the attorneys and possible bankruptcy to the businesses.

Thank you, Mr. Chairman, for this opportunity to present testimony.

CHAIRMAN KELLER: Thank you very much. We appreciate your testimony. I have a quick question for you. And that is, what would you think would - does your organization or you personally have any suggestion of what you would suggest should be part of the Bill as you alluded to in your testimony about the fact that small business will be put out of business

because of these suits? You know, how can we address this?

MR. SCHRODER: Well, I do believe - as I've said, I'm not an expert in what other states have done. I want to say that upfront. I have not had a chance to study their laws.

But there are other states, New York and Ohio, I believe, that have implemented data-breach security measures that impose duties on businesses, you know, in those states to provide protection against that. But they don't leave it at just the reasonableness standard. They insert things in their law which require steps to be taken, which require, you know, depending on the size of the business, the scope of the business, different protections to be put into place.

So I would just suggest and respectfully ask that the committee take a look at the matter and those measures to see what might work here in Pennsylvania in that regard.

CHAIRMAN KELLER: Representative Solomon?

REPRESENTATIVE SOLOMON: Thank you, Mr. Chairman. And I appreciate you bringing that up, because, Curt, I agree with now we have a

reasonableness standard. That's what the Dittman case came down on.

MR. SCHRODER: Right.

REPRESENTATIVE SOLOMON: And you are correct, not only in this country but in Europe they have specific ways to fill in what reasonableness is. So I hope that we can do that work, working with you, Chairman, and others to maybe better contour that standard.

The - your point on the - I mean, businesses, yeah, I would agree sometimes they're victims, right. So if a business hires a vendor, for instance, and they don't - that vendor does not properly encrypt their data or they don't provide requisite firewalls, certainly in that case they could be seen as a victim. But the Bill does allow them to recover damages from that - from that vendor.

You would agree with that, that's a possibility.

MR. SCHRODER: I think I'm aware of the section in that you're talking about.

REPRESENTATIVE SOLOMON: Right. Right. So I think we would agree on that.

I think that we need to provide some sort of certainty on reasonableness for folks that deal

with these breaches, the individual consumer.

So just for instance, I'm in the Army Reserves. So OPN had a huge, massive data breach, Federal Government. And an email went out to all service members saying your information has been compromised. Okay? So what they've done is continue to do is provide free credit checks. For me that's fine, right? I'm stateside.

Let's go and change the example and say that that individual is not Jared Solomon, who's drilling out of Horsham, Pennsylvania, but is someone knocking down doors, Special Forces or a Ranger in Iraq or Afghanistan. Don't we want to provide some sort of certainty to that individual, now that their career has been compromised, given the information that has been leaked, that they can pursue an action that provides some sort of redress for that individual?

MR. SCHRODER: I would just say my problem with the way this Bill is structured is that it relies too heavily on the litigation end of things and perhaps not as much thought given -. With all due respect, -

REPRESENTATIVE SOLOMON: Sure.

MR. SCHRODER: - not as much thought given to the preventative side of it and what we can

put in the statute to prevent these breaches and whatnot from occurring in the first place.

And it is one of - it is - something you said about just a couple moments ago, you know, in a store, you know, a criminal breaks in, you know, picks the lock or bashes the door down at night, you know, and takes something that belonged to, I don't know, maybe someone who had - getting a repair done on an item, you know, didn't belong to the store, belonged to the individual, you know, I would argue both of those situations.

You know, they're both victims of criminal - both criminal acts. And you know, I just think we should keep that in mind as we go through because none - you know, I think -. I hope we would all agree no business, you know, whether it's large, small, medium, nonprofit, for profit, wants to see anything like that happen to their customers, to their employees.

And if we could, you know, perhaps fashion a standard - tight standard that might need to be followed over time. I mean, these - I'm just thinking out loud here, perhaps regulatory aspect to it that would allow it to evolve over time as, you know, we noted that today's reasonable standard, today's

foolproof standard, probably isn't going to be tomorrow's foolproof standard. I think we can all agree on that. So perhaps some thought given to, you know, that type of mechanism moving forward.

CHAIRMAN KELLER: Thank you.

REPRESENTATIVE SOLOMON: Thank you, Mr. Schroder.

CHAIRMAN KELLER: Representative Zabel?

REPRESENTATIVE ZABEL: Just very briefly on reasonableness, which has been basically the standard for decades. The next thing about reasonableness, and I can make real good points in here, is exactly the reason that we have a reasonable standard is because, of course, what is reasonable today may not be reasonable the day before. What's right for a large firm is not necessarily the same thing for a small firm. So I think that's the point of the idea, is it's allowing those determinations to be made on a case-by-case basis.

To the extent businesses have a reasonable standard, every day that they're in operation with regards to potential liability, any certain number of threats. I'm not particularly concerned about the reasonableness standard. And I do think it's odd that an attorney, Kevin Baker, would be

complaining about it.

I just want to call your attention that he's not - Kevin Baker, he's not - the article doesn't mention - he's not an attorney. He sells security practices to law firms, but he himself is not an attorney. I just want to correct that, because that seemed odd.

MR. SCHRODER: I thought it had the name of his firm. If I'm incorrect, I apologize.

REPRESENTATIVE ZABEL: That's all right. I just thought it was odd to hear reasonableness standard -.

MR. SCHRODER: It was in The Legal Intelligencer.

REPRESENTATIVE ZABEL: Yes.

MR. SCHRODER: And if you want me to provide a copy of that article to the panel today, it was behind the pay wall and I didn't want to -.

REPRESENTATIVE ZABEL: That's fine.

MR. SCHRODER: I didn't want to breach the pay wall.

CHAIRMAN KELLER: Thank you very much for your testimony. We appreciate you hanging in there with us. We went over time, unfortunately, but that normally happens with these hearings.

Members, I want to thank each and every one of you. Chairman Driscoll, thank you for participating here also. And you know, we will move forward.

Representative Solomon, thanks for introducing the Bill. I think we've heard a lot of testimony that there will be some extra work that will take place on the piece of legislation. So thank you very much. This hearing is adjourned.

* * * * * * *

HEARING CONCLUDED AT 12:21 P.M.

* * * * * * *

CERTIFICATE

I hereby certify that the foregoing proceedings was reported by me on 02/25/2020 and that I, Amy N. Distefano, read this transcript, and that I attest that this transcript is a true and accurate record of the proceeding.

Dated the 20th day of April, 2020

Amy N. Distefano,

Court Reporter