STATEMENT FOR THE RECORD

ON BEHALF OF

THE NATIONAL ASSOCIATION OF CONVENIENCE STORES

AND

THE SOCIETY OF INDEPENDENT GASOLINE MARKETERS OF AMERICA

FOR THE

HEARING OF THE HOUSE ENERGY AND COMMERCE SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE

MARCH 18, 2015

"Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015"

Chairman Burgess, Ranking Member Schakowsky and members of the subcommittee, thank you for giving us the opportunity to submit this statement for the record on the topic of the elements of sound data breach legislation. We are submitting this statement on behalf of both the National Association of Convenience Stores (NACS) and the Society of Independent Gasoline Marketers of America (SIGMA).

NACS is an international trade association composed of more than 2,200 retail member companies and more than 1,600 supplier companies doing business in nearly 50 countries. The convenience and petroleum retailing industry has become a fixture in American society and a critical component of the nation's economy. In 2013, the convenience store industry generated almost $700 billion in total sales, representing approximately 2.5% of United States GDP.

SIGMA represents a diverse membership of approximately 270 independent chain retailers and marketers of motor fuel. Ninety-two percent of SIGMA's members are involved in gasoline retailing. Member retail outlets come in many forms, including travel plazas, traditional "gas stations," convenience stores with gas pumps, cardlocks, and unattended public fueling locations. Some members sell gasoline over the Internet, many are involved in fleet cards, and a few are leaders in mobile refueling.

Collectively, NACS and SIGMA represent an industry that accounts for about 80 percent of the motor fuel sales in the United States. And, this is truly an industry of small businesses. While many motor fuel outlets have agreements to use the brand names of major oil companies, those oil companies have largely exited the retail market. The vast majority of those branded outlets are locally owned. For example, more than 70 percent of the NACS' total membership is composed of companies that operate ten stores or less, and more than 60 percent of the membership operates a single store.

We submitted testimony for the subcommittee's January 27th hearing on the elements of sound data breach legislation which laid out the interest our members have in data breach legislation, noted how the payment card system impacts our data security efforts, provided background on data breaches, explained the current state of the law on data breach notification, and walked through the elements of data breach legislation that we consider to be most important.

This statement will focus on the draft "Data Security and Breach Notification Act of 2015" (Draft Bill).

A Central Concern with the Draft Bill

The Draft Bill sets a federal framework for data security standards for U.S. businesses and a system of notification requirements in the event that data breaches occur. The Draft Bill establishes a reasonableness standard that businesses must meet with respect to data security and, in our view, that makes sense given the wide diversity of businesses and circumstances that the Draft Bill aspires to cover. We do have concerns that this data security standard exempts some types of businesses from its coverage and that many of those businesses are not required by any

other laws to maintain a reasonable level of data security, but we will address that issue later in this statement.

Our overriding concern about the Draft Bill is that it creates fundamental problems that seem to undermine the intentions of its authors by taking large categories of U.S. businesses and foisting their notification obligations (with attendant threat of enforcement and fines) onto other U.S. businesses. The Draft Bill categorizes some businesses as "third parties" and others as "service providers." Third parties, as defined by the bill, store, process, maintain, transmit or route data on behalf of other businesses. These third parties include internet and other technology companies, cloud storage providers, payment card processors, payment card networks and many others. Companies that meet the definition of third party for much of the business they conduct include many corporate giants and household names such as Google, IBM, Oracle, Toshiba Samsung, Automatic Data Processing (ADP), Visa, MasterCard, and First Data.

Service providers are defined in the Draft Bill as businesses that transmit, route, or provide intermediate or transient storage of data for another business and are covered by the Telecommunications Act. Service providers also include corporate giants and household names such as Comcast, Verizon, and AT&T.

Under the Draft Bill, third parties and service providers do not need to notify affected consumers or the public when they have a data breach. In fact, in some situations, service providers do not need to notify anyone at all when they have a data breach. In other situations, the third parties and service providers are only required to notify the businesses whose data was taken in the breach. Then, according to the Draft Bill, once a business has been told by a third party or service provider that some of its data has been breached, all of the responsibility and cost of notifying affected consumers and the public along with the risk of enforcement by the Federal Trade Commission (FTC) and state attorneys general and attendant fines running into the millions of dollars fall on the business that was notified – not the business that suffered the data breach. That is fundamentally unfair. And, to the extent that requiring businesses to provide notification of their breaches incentivizes those businesses to try to protect against such breaches, that incentive is lost for third parties and service providers under the bill.

NACS and SIGMA, for example, collectively represent tens of thousands of single store operators whose pre-tax profits average about $47,000 per year. These businesses are not unique. There are many small businesses across the country in many different areas from restaurants to small shops, corner grocery stores, doctors' offices, and individual entrepreneurs that similarly work very hard just to make ends meet each year (or each pay period). But the service provider provisions of the Draft Bill mean that if Comcast, for example, suffers a breach of its data lines the most it has to do is notify businesses like a mom-and-pop convenience store whose data may have been carried when the breach occurred. Then, mom-and-pop convenience store is on the hook for complying with all the notification provisions of the Draft Bill and will face large fines if it doesn't do it right even though Comcast had the data breach. The same is true for third parties – just substitute Visa or Google for Comcast.

This is fundamentally unfair. Corporate titans should not be able to foist legal responsibility for notifying people of their own data breaches onto businesses that did not have a

data breach at all. The same would be true even if the third parties and service providers involved were universally small businesses. The cost and legal peril shifted onto other businesses simply does not make sense and those businesses have little if any ability to influence the data security practices of the third parties and service providers with which they deal.

Some have argued that third parties and service providers need to pass their notification responsibilities onto other businesses because consumers might not do business directly with those third parties/service providers and might otherwise be confused. First, we would note that consumers have a wealth of experience dealing directly with telecommunications companies (service providers), understand what services they provide, and likely would not be confused by receiving notices from them about their data breaches. Second, many third parties are equally recognizable (e.g., Visa/MasterCard) and would not engender any confusion by providing notices. Third, in situations for which there might be a genuine confusion problem, there is nothing in the Draft Bill or elsewhere that would prevent an explanation of how the data breach connects directly to the consumer involved (such as by noting that the business providing the notice handles data on behalf of a local business with which the consumer transacted). That explanation would be much less confusing in many instances coming from a business that actually suffered the data breach than coming from a business that did not suffer a breach (whose veracity may unfairly come into question simply because it provided the notice).

It is also worth pointing out that, during the subcommittee's hearing on January 27th on this topic, Representative Gus Bilirakis (R-FL) asked the panel which business should bear the notice responsibility in the event of a data breach. Jennifer Glasgow, Chief Privacy Officer of Acxiom, Brian Dodge, Senior Vice President of Communications and Strategic Initiatives for the Retail Industry Leaders Association (RILA), and Woodrow Hartzog, Associate Professor for the Cumberland School of Law, all answered that the business suffering the breach should bear the responsibility of providing notice to affected consumers. Only the witness representing a trade association for the information technology industry, whose members include many businesses defined as third parties and service providers by the Draft Bill, differed with the other witnesses on that point.

Having third parties and service providers pass their notification responsibility onto bystander companies creates many other problems – some of which do not make sense and were likely not intended by the bill's authors. We walk through just some of most glaring of those problems below, but we urge you to resist the strong temptation to simply try to patch over each of these problems individually. These issues are not the problem. They are symptoms of the underlying problem that many businesses which have a data breach are able to foist legal and financial responsibility for notification of that breach onto other businesses. New drafts of the bill cannot overcome these issues without creating new ones unless and until the treatment of third parties and service providers is fundamentally changed so that they remain responsible for notification in the event of their own breaches. Attempting to treat the individual issues pointed out below would be like building a hull of a ship with half of the necessary boards missing – and then trying to patch the gaps like they were individual small leaks. The job will never be completed to allow such a ship to float. The hull needs all of its boards to be sound.

And here, all businesses that suffer data breaches need to have responsibility for notifying affected consumers and/or the public or a federal data breach scheme will never work as well as it should.

Individual Problems Created by the Separate Treatment of Third Parties

As noted above, third parties only need to inform the business for which they store, process, maintain, transmit or route data of the information that was breached and then the notified business (that was not breached) has to provide notice to affected individuals. That leads to the following problems:

- **Individual notice may be impossible** – if the information that was breached does not include contact information for the affected individuals, the breached business has no responsibility to provide contact information so individual notice may be impossible. That means substitute notice (by posting on the website of the business that did not have a breach) may be the only possibility.
- **Notice may not be timely** – third parties are only required to provide notice to the non-breached business "promptly." But the non-breached business is required to provide notice to affected individuals within 30 days after the breached system has been restored.
    - But the non-breached business might not be aware of the breach within 30 days of the system being restored (it's not clear how long "promptly" is).
    - And, the non-breached business might not know when it is required to provide notice because the breached business has no obligation to tell it when the breached system has been restored (and might want to keep that information confidential).
    - Despite these problems, the business that did not even suffer a breach is subject to fines under the FTC Act and penalties from state Attorney General lawsuits of up to $2.5 million if it does not provide timely notice of a breach – even if it was not aware of the breach before the deadline and/or was not aware of what the notice deadline was.
- **Key information may never be known** – third parties are not required to perform any investigation if they have a breach (breached businesses other than those defined as third parties or service providers are required to do so). So, there is no way for the non-breached party to determine whether there is a risk to consumers that should lead to notice and important information about the causes and extent of the breach may never be known.

Individual Problems Created by the Separate Treatment of Service Providers

As noted previously, a business that transmits, routes, or provides intermediate or transient storage of data for another business and is covered by the Telecommunications Act is a "service provider" and does not need to notify individuals when it has a data breach. Service providers have fewer responsibilities than third parties.

- **No notice to anyone** – service providers do not need to notify anyone when they have a breach unless they can "reasonably identify" the business that was sending the

information that was breached. But service providers have no obligation to conduct any investigation or inquiry into their data breach in order to identify the business sending the information. The result is likely to be that no one is informed of anything in many instances when a service provider has a data breach.

- **Notice may not be timely** – there is no timing by which service providers must notify non-breached businesses of breaches (it doesn't even have to be "promptly" as with third parties). That exacerbates the problems with notice timing. Non-breached businesses may in many circumstances not be aware of a breach at a service provider until after they were required to provide notice of that breach. Non-breached businesses, however, will potentially be subject to fines under the FTC Act and state enforcement with penalties of up to $2.5 million for not providing notice of breaches they did not have and were not aware of until after the deadline for notice.
- **Key information may never be known** – service providers, like third parties, are not required to perform any investigation if they have a breach (other breached businesses are required to do so). So, there is no way for the non-breached party to determine whether there is a risk to consumers that should lead to notice and important information about the causes and extent of the breach may never be known.

Consumers Will Receive Multiple, Confusing Notices of Many Third Party and Service Provider Breaches

By making non-breached businesses provide notice when third parties or service providers have breaches, the draft bill will lead to individual consumers receiving multiple notices regarding the same data breaches. Those notices will include different contact information and risk both confusing and alarming consumers. The multiple notices will also lead to unnecessary, duplicative costs on businesses.

- **Multiple Notices of Telecommunications Breaches** – when a telecommunications provider has a breach, it is likely that the data of multiple businesses sending data over the telecommunications system are impacted. There will be many instances in which those businesses have some overlap in customers (those customers are likely, for example, to do business with multiple local businesses and not just one). The telecommunications company, however, may tell all of the multiple affected businesses of the information that was breached (if, as noted above, they tell anyone at all) and each of those non-breached businesses will be responsible for notifying their customers. So, it would not be surprising for an individual consumer to receive notices from the local restaurant, hardware store, grocer, drug store, and convenience stores regarding the same breach. And these notices will include some of the same along with some different contact numbers. They might also describe the information and circumstances differently leading to additional confusion.
- **Multiple Notices of Payment Processor/Network Breaches** – when payment processors (such as First Data) and networks (such as MasterCard) have breaches, it is highly likely that the data of multiple businesses sending payment card transactions over their systems are impacted. The results for these "third party" breaches will be much the same as for the telecommunications "service providers" noted above. Multiple affected

businesses may be notified and they, in turn, will each have to notify their customers – many of whom will be the same because they shop at multiple different businesses.

Third Parties, Service Providers and Others Will Have Non-Existent (or Reduced) Notice Obligations

Even though third parties and service providers are only required to notify the non-breached business(es) of their breaches, those third parties and service providers will no longer have to comply with state data breach notification laws under the pre-emption provision of the draft bill. This reduces the notice obligations of these companies under current law. And, for service providers, they will not have to investigate when they have a breach and will not need to notify anyone if they don't know who sent the data (which is likely without investigation).

- **The result of the draft bill for service providers, then, is that they could have a breach, not investigate at all, not notify anyone, and not have to comply with any of the 47 state data breach notification laws**.
- Similarly, banks and credit unions are not covered by the data breach notification provisions of the draft bill and will not be required to investigate breaches or notify anyone of their breaches under the Draft Bill. They do have guidelines under the Gramm Leach Bliley Act (GLBA) that say they "should" notify consumers when they have breaches, but that guidance is written in discretionary terms and is not required. The disparity in notice obligations between these financial institutions and the businesses with which they exchange data millions of times per day will lead to vulnerabilities that data thieves will exploit to steal data (and keep the thefts secret for as long as possible).

Many Businesses May Be Falsely Blamed for Breaches They Did Not Have

The Draft Bill allows businesses to contract with another business to provide notice. This makes sense because, especially in many large breaches, it is much more efficient and leads to more effective notice if a business that specializes in providing these types of notices is used. The problem comes when there are third party or service provider breaches.

- **Non-breached businesses must be blamed** – when a third party or service provider is breached, a non-breached business has the legal responsibility to provide notice (assuming the service provider notifies anyone at all). But the provision allowing a contractor to send the notice requires that the notice say that it is being provided on behalf of the business that contracted for the notice to be sent. That means the notice must blame the non-breached business for the breach, even though the breach was of a third party or service provider. So, the draft bill saddles the non-breached business with the legal obligation and costs of providing notice under the threat of fines and, if it uses a contractor to provide notice, requires the non-breached business to take the blame for the data breach.

Enforcement Will Unfairly Focus on the Wrong Businesses

As noted above, businesses that are informed by third parties and service providers of breaches at those third party and service provider businesses will be subject to enforcement even though they did not suffer a data breach.

- **Penalties without breaches** – Businesses that did not even have a breach will be subject to FTC enforcement and penalties under the FTC Act as well as state AG enforcement with penalties of up to $2.5 million.
- **Penalties without a chance to comply** – Businesses that receive notice from third parties or service providers close to or after 30 days from the time the third party or service provider's system is secured will have no way to comply with the draft bill, but will still be subject to enforcement by the FTC and state AGs and fines for non-compliance.

Financial Institutions Will Not Have Data Security or Data Breach Notification Obligations Under the Draft Bill

One other issue that bears attention is the exclusion of banks and credit unions from the Draft Bill. These institutions are certainly vulnerable to data breaches. In fact, according to the most recent Verizon Data Breach Investigations Report, financial institutions have about three times as many breaches as do retailers. Banks and credit unions exchange payment card information with businesses fully covered by the bill as well as third parties and service providers hundreds of millions of times per day. Those banks and credit unions do have guidelines under GLBA that say they "should" have data security processes and procedures in place, but that guidance is written in discretionary, not mandatory, terms.

Having banks and credit unions subject to permissive guidelines on data security and data breach notification while the other businesses with which they exchange data are subject to requirements backed by FTC and state AG enforcement invites differential standards and data vulnerabilities. Data thieves do not limit their activities to any one category of business. They go after everyone and are successful in every category. The Draft Bill should cover everyone if it is meant to improve our preparedness for and reactions to data thieves' activities.

* * *

We appreciate the subcommittee providing us with this opportunity to submit our views on the Draft Bill. We look forward to working with you as the committee continues to consider this topic.