


**A National Data Breach Notification  
Legislation Framework**

Bipartisan Recommendations for  
Legislators and Policymakers



**NTSC**  
NATIONAL TECHNOLOGY  
SECURITY COALITION

[ntsc.org](http://ntsc.org)



**D**espite bipartisan support, the United States lacks a national data breach notification law. In the event of a data breach, CISOs must individually report to all 50 states, the Virgin Islands, Guam, Puerto Rico, and the District of Columbia. As a result, consumers unfairly and arbitrarily experience disparate data breach notification laws from state to state. Consumers are not protected equally in all states, so it's reasonable to challenge why so many different and varied laws exist that seem to focus more on pleasing regulators rather than following a nationally agreed upon set of data breach notification standards.

For example, 47 states require disclosing the cause of a breach, but Massachusetts explicitly prohibits declaring what caused the breach. Both of these contradictory laws must be followed by organizations experiencing a breach. That means a company operating in one state or industry may be legally required to file a report that explicitly violates the laws of another.

Legislation and guidelines tend to differ from state to state in many aspects, including:

- The definition of a breach
- The amount of time before an organization must notify regulators after a breach is uncovered
- Actual or potential financial harm to the consumer
- The consumer notification process
- The organization's responsibility for supporting the consumer post-breach (such as credit monitoring for some period)

Companies are thus required to make multiple investments to achieve full compliance with each state. Are these investments helping protect consumers? No.

These investments do not directly compensate any impacted consumers or improve the company's cybersecurity posture. Instead, these investments go toward a notification industry that arose to take advantage of a complex, muddled legislative environment—an industry only existing because we allowed a national issue to be regulated at the state level.

**According to IBM Security**, data breach costs increased by 5.5 percent over the last year. Currently, the average cost of a data breach in the United States is \$3.86 million. Data breach notification is an expensive process, and the

IBM Security study explains that "direct expenses include engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates."

It is the primary job of a CISO to develop and implement an information security strategy to defend against known threats from known adversaries. Secondly, they must devise a comprehensive security approach to anticipate new threats from a seemingly endless list of state and non-state actors. In addition to securing consumer data from continual cyberattacks, CISOs are also responsible for the regulatory compliance that accompanies the business. Instead of focusing on the latest technologies to safeguard against a cyberattack, emphasis is misplaced on trying to meet the varying and often conflicting standards set forth in the myriad state regulations. Simply stated, CISOs are more often forced to focus on regulatory compliance and not necessarily cybersecurity.

This whitepaper will:

- Examine the history of Congressional attempts to implement national data breach notification legislation in order to understand why Congress hasn't passed such a law despite overwhelming bipartisan consensus.
- Outline the current obstacles that must be overcome to successfully pass a national data breach notification law.
- Provide recommendations on how to overcome these obstacles and move forward.

# A Brief History of National Data Breach Notification Legislation

Beginning in 2002, when California enacted the first state data breach notification law, and concluding in 2018, when South Dakota became the 50th state to enact a state data breach notification law, the United States saw states, one after another, act on this issue. Federal inaction led to states taking on this job for themselves, leaving us with a patchwork of conflicting, contradictory laws that add compliance burdens and costs to many companies with customers throughout the United States.

Congress began to introduce national data breach notification bills as early as 2003. Various attempts continued throughout the 2000s, without success. [In a 2010 Senate report](#), Senator Patrick Leahy (D-VT) noted, “Multiple Federal entities, including the Secret Service, the Federal Trade Commission, and President George W. Bush’s Identity Theft Task Force, have urged Congress to pass such legislation.” Summarizing the obstacles in 2011, [law firm Wiley said](#) the sticking points included “disagreements between the House and Senate as to the proper approach, opposition to preemption from privacy advocates and states that might believe that the federal law provides insufficient protection, and disagreement as to the appropriate ‘risk’ threshold for when businesses should be required to provide notice to affected persons.”

As time progressed, data breaches became larger, more prominent, and more devastating. While industries such as financial services and healthcare experienced significant breaches, [retail began to experience some of the largest data breaches](#). For example, on December 19, 2013, Target Corporation announced they discovered a data breach that ultimately impacted 70 million consumers by exposing their names, credit and debit card numbers, card expiration dates, CVV (card verification value) numbers, mailing addresses, phone numbers, and email addresses.

In response to a spate of such larger breaches, Senator Tom Carper (D-Delaware) and Roy Blunt (R-Missouri) put forth the [Data Security Act in 2015](#), President Barack Obama took the unusual step of recommending [The](#)



[Personal Data Notification & Protection Act](#) in 2015, and Representative Marsha Blackburn (R-TN-07) introduced

the [Data Security and Breach Notification Act of 2015](#). [When privacy groups pushed back](#), pointing out that the bill would be less stringent than 38 state laws and weaken enforcement, the legislative efforts once again stalled.

The increasing number and breadth of data breaches led to more consumer awareness about data security and privacy.

**The increasing number and breadth of data breaches led to more consumer awareness about data security and privacy.**

One of the major watershed moments for the public came in the form of something incredibly personal to consumers—Facebook. The Facebook–Cambridge Analytica data scandal and a July 2017 Facebook data breach that was not revealed to the public until September 2018 both made US consumers viscerally aware of their data security in ways that EU consumers have contemplated for decades..

In 2017, Senator Bill Nelson introduced S.2179, the [Data Security and Breach Notification Act](#)—a bill filed in the wake of the 2016 Uber data breach. It was perceived to be overly punitive. In 2018, the [Data Accountability and Trust Act](#), introduced by Representative Bobby Rush (D-IL),

concerned some groups because of its heavy reliance on FTC enforcement. In the wake of the Equifax data breach, Senator Elizabeth Warren (D-MA) introduced S. 2289, the [Data Breach Prevention and Compensation Act of 2018](#). It prompted the NTSC to send a letter of public opposition to the bill due to its punitive nature.

During this time, states' rights became a sticking point as many of these proposals would indeed weaken some existing state data breach notification laws. However, legislators including Senators [Mark Warner](#) (D-VA) and [Ron Wyden](#) (D-OR), along with Representatives Kevin McCarthy (R-CA), Michael McCaul (R-TX), Maxine Waters (D-CA), [Jim Langevin](#) (D-RI), and Ted Lieu (D-CA), all released public statements in support of national data breach notification legislation.

Another sticking point became objections by the retail industry. In response, Representative Blaine Luetkemeyer (R-MS) introduced a financial services-only federal data breach notification bill that would preempt state notification requirements. This bill, H.R. 6743, the [Consumer Information Notification Requirement Act](#), passed the House Financial Services Committee in September 2017. In February 2018, Representatives Luetkemeyer and Carolyn Maloney introduced a draft bill, the [Data Acquisition and Technology Accountability and Security Act](#) which also tried to tackle national data breach notification. While the NTSC worked with Representative Luetkemeyer on

## This decades-long inaction by Congress is not helping businesses or consumers.

national data breach notification legislation, offered language recommendations to his legislative text, and directly supported his legislation, even this narrowly-tailored attempt failed to gain traction.

Data breach notification legislation fell apart in the 115th Congress around liability and jurisdictional issues. Meanwhile, states [such as New York](#) continued to frequently update their data breach notification laws, making compliance stricter and more difficult. And the pace at the state level is not slowing: a growing number of states like New York and Colorado are currently pushing new cybersecurity standards for the financial services industry, possibly setting a precedent for other states to implement with their own new standards that will add even more complexity, cost and confusion to the existing patchwork of data breach notification regulations.

This decades-plus-long inaction by Congress is not helping businesses or consumers. We are excited for Senators Rob Portman's (R-OH) and Senator Tom Carper's (D-DE) draft Data Security & Breach Notification Act of 2020, which we will discuss later in this whitepaper. But first we want to take a step back, analyze this history, and examine why these Congressional efforts keep failing.



# Obstacles Preventing the Passing of National Data Breach Notification Legislation

National data breach notification legislation is still a no-brainer for many in the House and Senate, but the various stakeholders cannot seem to agree on specifics. While several obstacles have shifted in importance over the years, the following obstacles tend to linger as sticking points:

## States' rights, enforcement, and preemption

While this issue has lessened somewhat in recent years, it remains historically one of the greatest sticking points to a national data breach notification bill. States have noted correctly that many past attempts at federal bills were not as strong as many existing state laws. It is rational for those states to maintain their high data privacy standards. Thus, if a proposed federal bill preempts and weakens state law while removing the ability for state attorneys general to enforce their laws, then states will not support it—including Members of Congress representing those states.

Many GOP representatives are reluctant to preempt state data breach laws for fear of making data breach notification a states' rights issue. States will actively lobby against such a law because it takes away regulatory power. When lawmakers say they will take the strictest state standard (such as California) and use it as the basis for a national data breach notification law, resistance remains.

Typically, preemption is a hard-fought battle for any law. In this case, attorneys general will want to retain their states' data breach notification laws and fight against a federal law that may be perceived as unnecessarily strengthening or weakening cybersecurity protections.

## Different perspectives from different industries

Strict laws, regulations, and guidance bodies oversee industries such as financial services and healthcare, so a national data breach notification law will have less of an impact on them. However, sectors like retail often take issue with proposed data breach notification bills because such a law would put too much burden on mom-and-pop businesses. The retail industry's opposition to recent attempts at a national data breach notification law currently ranks alongside states' rights as one of the biggest legislative obstacles.

It's important to note that the retail industry's concerns about data security are valid. As the National Retail Federation (NRF) noted in a [February 2018](#)

**Many GOP representatives are afraid to preempt state data breach laws in fear of making data breach notification a states' rights issue.**

# 11

## Obstacles Preventing the Passing of National Legislation

- States' rights, enforcement, and preemption
- Different perspectives from different industries
- Privacy group concerns
- A punitive mentality
- Incentivizing speed-to-market and consumer convenience
- Definitions
- Customer notice methods and timing
- Who must comply?
- Co-existence with industry laws
- Priority
- "Another regulation" perception



Consumer convenience makes constituents largely apathetic to data protection laws.

[blog post](#), they want consumers to be notified, all industries to be held accountable for breaches, no breaches kept secret from a lack of notification requirements, and fair standards that don't treat one industry differently than another industry.

### Privacy group concerns

Similar to concerns from states, privacy groups grow wary when existing laws to protect consumers are weakened in any way.

Consumers experience different data breach notification laws state-by-state, regulations vary wildly by industry, and punishing companies helps the consumer too little, too late, without examining smarter ways to strengthen companies' security posture.

### A punitive mentality

We are so used to blaming companies for data breaches that we often forget a simple fact: these companies are victims of a crime. Often, various industry experts and federal and state government lawmakers call for stricter privacy legislation and tougher penalties for breached companies. After the Marriott data breach, there were even calls for executives in these companies to be **"locked up."** While extreme negligence may be considered a crime, punishing corporate executives as a rule of thumb will not stop cyber criminals or address the root cause of data breaches. Unsurprisingly, excessively punitive bills do not get much Congressional support.

### Incentivizing speed-to-market and consumer convenience

Most companies pay close attention to profits and market drivers, with a focus on increasing shareholder value. Security teams are often beholden to a vast ecosystem of business stakeholders, shareholders, and customers who may consider security a lesser priority. However, brand trust and cybersecurity are themselves rapidly becoming market drivers. Companies are beginning to realize that a balance must be struck between speed-to-market and security.

Additionally, consumers often demand products and desire conveniences that pressure companies to move quickly. Consumers want the convenience of not entering a credit card number every time they purchase something from Amazon or iTunes, or the convenience of walking into a rental car parking lot and driving away with the car of their choice because that rental agency has everything they need in their file. But consumers are not cybersecurity experts and companies may not be fully transparent about their processes. As a result, it's often difficult for people to understand—as with the GDPR in the EU—how companies use their information. A demand for consumer convenience, without an awareness of what's really happening to their information, can make constituents largely apathetic to data protection laws; that is, until the breach affects them and their personal information.



## Definitions

What is a “breach?” What constitutes “harm?” Definitions of terms often become sticking points as lawmakers struggle to define breach notification, cybersecurity standards, and unauthorized access in ways that please all interested parties. But differing and inconsistent definitions only add to the confusion, inconsistencies and compliance costs.

## Customer notice methods and timing

How are customers notified? When should they be notified? What’s the trigger for a notification? How do organizations let them know? What happens next? Many questions surround customer notice methods, and various industry groups argue for different forms of strictness.

## Who must comply?

How big must the business be before they are required to comply? Many industries argue for varying levels of enforcement depending on the size of a business. For example, how should a Fortune 500 financial services company get treated differently than a dry cleaning shop with two employees? But what if the small business is handling extremely sensitive personal health data. Shouldn’t they be held to the same standard of security and privacy controls?

## Co-existence with industry laws

How would a national data breach notification law coexist with existing industry security laws such as those found in the healthcare (HIPAA, HITECH) or financial services (the Gramm-Leach-Bliley Act) sectors? Stringent regulations make healthcare and financial services data breaches more expensive than other industries, so a bill cannot add more burden to these industries. It’s important for any national data breach notification law to harmonize with existing industry laws that already apply stringent requirements.

## Priority

Lawmakers have focused on the urgency of cybersecurity incidents related to Russia, national security, and ransomware—along with spending time on plenty of other non-cybersecurity Congressional demands during a pandemic. National data breach notification often falls to the bottom of the list of priorities. Because such a law requires bipartisanship, a divisive political climate also doesn’t help.

Even if the arguments make sense, many lawmakers are reluctant to go to bat for a national data breach notification law if it only seems to impact business with little benefit for consumers. In other words, why should the public care?



**Many lawmakers are reluctant to go to bat for a national data breach notification law if it only seems to impact business with little benefit for consumers.**

## “Another regulation” perception

On the surface, it appears as if a sweeping federal law would serve up bloated, unneeded regulation that infringes upon states’ rights. Yet, a national data breach notification law lessens regulations—especially when organizations only report once rather than dozens of times to separate entities.

It’s important to note CISOs are not opposed to legal and regulatory oversight. In fact, comprehensive oversight is welcome when the emphasis is properly placed on consumer protection and notification.

**Now that we’ve examined the obstacles, let’s make the case for what a national data breach notification law needs and why it needs to be passed.**

# 6

## Elements of a National Data Breach Notification Law

- **Preempt all state, district, and territorial data breach notification laws by picking the strongest state law as the standard.**
- **Work with the retail industry on a bill that removes their objections.**
- **Agree upon a set of widely accepted security standards, and adjust those standards to the size of an organization.**
- **Agree upon basic definitions.**
- **Use a complementary system of enforcement, shared between the FTC and state attorneys general.**
- **Ensure harmony with existing federal regulations.**

## What a Law Needs

Based on the input of the NTSC Board of Directors, the NTSC Advisory Council, and the NTSC Policy Council, we have narrowed down the components that a national data breach notification law needs to contain in order to work effectively and navigate the political waters to ensure its passage.

### **Preempt all state, district, and territorial data breach notification laws by picking the strongest state law as the standard.**

In the event of a data breach, we need to ensure that all United States consumers are entitled to the same level of protection instead of varied state-by-state protection. At the very least, we must provide organizations a single place to file a data breach instead of dealing with multiple state agencies. By providing for uniform protection, we ensure that consumer rights are properly guarded.

To eliminate any perception that a federal law would weaken state laws, we recommend reviewing existing state laws to find the right balance for a national standard. In other words, we need preemption to make this law work—to give businesses one set of requirements and consumers a consistent law throughout the nation. Setting the standard high will alleviate the concerns of states and privacy groups. Additionally, having one law and one place to which to report a data breach makes compliance easier for CISOs.

### **Work with the retail industry on a bill that removes their objections.**

As we noted earlier, the retail industry has brought up reasonable objections to past national data breach notification bills. These objections must be overcome, or a reasonable compromise must be reached to circumnavigate this impasse. Otherwise, doing absolutely nothing hurts retail—and all other industries—from the plethora of existing state laws with which they must comply.

It's time for the retail industry to come to the table when all other industries agree that a national data breach notification law would help businesses, consumers, and national security. We need something that encompasses all industries because not all consumers are protected equally by state legislation governing data breaches.

For example, many of the retail industry's concerns about financial services need not worry them. It's easy to trip up on the term "guidance" when used by federal banking regulators. The [FDIC](#) provides "guidance for financial institutions to develop and implement a response program designed to address incidents of unauthorized access to sensitive customer information maintained by the financial institution or its service provider." This guidance



includes how customers are to be notified after a data breach.

Financial services CISOs do not ever view this “guidance” as optional. To them, it’s mandatory. **Interagency guidance issued by federal banking regulators** applies to customer information defined as “any record containing nonpublic personal information ... about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of” a financial institution. These guidelines provide that, when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been, or will be, misused. If the institution determines that misuse has occurred or is reasonably possible to occur, it should notify the affected customer as soon as possible.

We understand why groups like the National Retail Federation lobby against current national data breach notification bills. They want financial institutions to adhere to the same notification requirements as the retail industry. But the idea that financial institutions don’t have notification requirements is false. While it is true that under the Gramm–Leach–Bliley Act (GLBA) they technically do not, other banking regulators do provide strong guidelines to which these institutions must adhere.

Meanwhile, financial institutions often say they will adhere to



national data breach notification requirements if retailers adhere to the same data protection requirements to which they are subjected. Of course, the retail industry is never going to agree to those requirements because those protections cost money, and smaller retailers will never be able to afford them. That’s a legitimate point.

That is the circular argument that perennially torpedoes the advancement of national data breach legislation. This argument needs resolved as soon as possible before more state laws are enacted that complicate, frustrate, and financially impact both the financial services and retail industries. Despite valid arguments on both sides, failing to compromise on a few points now leads to everyone losing more later.

### **Agree upon a set of widely accepted security standards, and adjust those standards to the size of an organization.**

A uniform national data breach notification law would eliminate a multitude of different laws by creating one law and one set of standards. By agreeing upon one set of standards, the law will be clear and uncontradictory.

Currently, a variety of federal and state laws conflict and focus more on reporting requirements after a data breach instead of preventative security measures that would improve cybersecurity standards. Laws, regulations, and policies can better define authentication standards, cyber hygiene requirements, more secure business processes, and a focus on protecting valuable non-PII information.

With the agreement of the security practitioners who must implement any data breach notification requirements and the industries that understand the nuances of their businesses, all definitions and parameters must make practical sense—such as following existing NIST standards familiar to security practitioners.

Standards could also include better incentives and penalties tied to business metrics. Boards, executive leadership, and legal teams are less prone to care about cybersecurity if it is solely the CISO's concern. But if cybersecurity laws, regulations, and policies were tied to revenue and brand reputation, then organizations would be more incentivized to change.

For example:

- What percentage of budget is an organization spending on cybersecurity? Is it appropriate?
- What does governance look like?
- Is cybersecurity at the table and talked about at every board meeting?
- Should there be real consequences for executive leadership and shareholders in the wake of a data breach or cybersecurity attack?

We must mandate a cyber investment standard designed to improve the security posture of American businesses. This means requiring companies to achieve a specific standard of cyber protection with an appropriate investment, guided by the NIST Cybersecurity Framework or something similar.

We must also ensure that the security standards for consumer

data make sense based on company size and type of data held. Applying the same standards to all businesses is impractical—there is no reason to treat a small dry-cleaning company the same as a Fortune 500 financial services company.

Standards must also be clear about third parties and define personal responsibility. Currently, **states vary on how they hold third parties accountable as part of data breach notification requirements**—ranging from requiring the organization to train third parties to simply contractually obligating them to follow a set of best practices.

### **Agree upon basic definitions.**

A law needs to provide clarity around what constitutes a breach. Legislators should continue to work with cybersecurity practitioners to create reasonable definitions and parameters. Challenges to a uniform data breach notification bill include agreement upon:

- **Definitions of key terms:** For example, what is defined as personal data? What is a breach? What is the threshold for reporting a data breach? How many users?
- **Definition of access:** What constitutes accessing data? This can be tricky, especially in cases where someone accesses encrypted data.
- **Definition of personal responsibility:** This issue is complicated by the use of third parties, vendors that host confidential customer data but may not know about the content, or bots that use servers and workstations at innocent companies to carry out attacks.

- **Definition of reporting:** How is the breach to be reported? How will consumers be notified? What credit monitoring protection would be required given a certain scenario?

### **Use a complementary system of enforcement, shared between the FTC and state attorneys general.**

Oversight is an important part of any national data breach notification process. To avoid conflicts of interest and abuse of power, the agency overseeing the law will not be the agency that regulates it.

We recommend giving state attorneys general specific powers that complement the FTC's authority with appropriate civil penalties in cases of gross negligence. This complementary system of enforcement ensures that state attorneys general maintain certain enforcement standards while allowing the FTC to regulate companies more broadly with a national footprint.

Therefore, standards are deeply important as part of this law. We don't want a situation where the FTC has the authority to punish companies for data security violations without providing standards or guidance.

### **Ensure harmony with existing federal regulations.**

As most past bills have proposed, we recommend complementing existing industry legislation where appropriate. Financial services, healthcare, communications, and other industries already operate under stringent requirements. If

those requirements are sufficient or exceed the requirements of a national data breach notification law, then those industry laws should preempt and/or complement the national law.



### **Senator Rob Portman's Data Security & Breach Notification Act of 2020**

As a path forward, we are optimistic about a bill drafted by U.S. Senators Rob Portman (R-OH) and Tom Carper (D-DE) that is likely to be introduced in 2021. During 2020, the NTSC Board and the Policy Council members provided extensive input on the senators' data security and breach legislation throughout multiple drafts by reviewing drafts and going over their comments with Senate staff. We're excited to see some traction on this priority in Congress after many unsuccessful attempts.



## **The Path Forward**

If we continue on a path of patchwork of disparate state laws, a punishment mentality, and a reactive strategy to data breaches that never solves the root causes, then it will only lead to greater vulnerability. The NTSC endorses reasonable data collection, especially if that data is collected without the consumer's knowledge. But we also believe that creating security standards based on the size of a company and the type of data held is critically important to ensure the protection of consumer data.

Is that an easy task? Absolutely not. It requires bipartisan and industry-agnostic discussion to craft a law that helps businesses, consumers, and national security while reducing bureaucracy, unnecessary compliance requirements, and a fixation on punishing companies. The NTSC supports federal legislation that gives businesses one place to file, ensures a standard of security for consumer data based on company size and data held, and supports appropriate civil penalties in cases of gross negligence.

From our conversations with CISOs, we see agreement between financial services, retail, and other industries that we need a national data breach notification law. We want consumers to have the same level of protection nationwide. Lastly, we want more cybersecurity dollars going toward protecting consumers and better securing companies rather than spending about 60% of data breach costs on the notification industry.

The National Technology Security Coalition is confident that, if the financial services and retail industries keep their eye on these goals as they discuss sensible compromises, we will soon see a national data breach notification law passed that finally moves our industry forward.

The National Technology Security Coalition (NTSC) is a non-profit, non-partisan organization that serves as the preeminent advocacy voice for Chief Information Security Officers (CISOs) across the United States. Through dialogue, education, and government relations, we unite both public and private sector stakeholders around policies that improve national cybersecurity standards and awareness.



4400 North Point Parkway  
Suite 155  
Alpharetta, GA 30022  
**[ntsc.org](http://ntsc.org)**