Gramm-Leach Bliley Act (GLBA) What You Need to Know and How to Ensure Compliance

1touch.io
Data Aware Security

While a lot of attention is paid to recently passed privacy laws, such as GDPR, CCPA, and LGDP, some older ones are still quite relevant and, as such, must be understood and adhered to, depending on the industry.

What is GLBA?

GLBA, or the Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, is a US federal law that regulates how financial institutions can use customer and consumer data (we'll explain the distinction between those two groups below).

GLBA didn't start life exclusively as a privacy regulation; until the law was passed under the Clinton Administration, different types of financial institutions were prohibited from merging, thanks to the Glass-Steagall Act of 1933. This law stipulated that commercial banks couldn't offer different financial services, such as insurance policies or financial advisory services, to their users. GLBA overturned this law to allow financial institutions to merge (truthfully, Citibank and Travelers Insurance had already taken the liberty of merging to create CitiCorp a year before the law was passed), which essentially gave rise to the modern banking ecosystem.

So How did GLBA Become a Privacy Regulation?

With the vast potential for mega-mergers, the FTC (Federal Trades Commission) understood that untold amounts of customer data would be passing through hands within the financial services industry. This meant that financial institutions would have access to all this data and could sell it to third parties or use it for their own data initiatives. Thus, the bill also included the requirement to protect their customers' and consumers' Non-Public Information (NPI; GLBA's version of PI). To be compliant with the regulations, financial institutions must ensure that all NPI is stored securely. Also, they must inform all customers and consumers on their data-sharing policies. In addition, they must provide users with the ability to opt-out of sharing NPI.

But wait, hold the horses, you say; what's the difference between customers and consumers? Under GLBA, a consumer is someone who has requested information, services, or a product from a financial institution, even if the individual did not follow through, or if their application was denied. This also includes someone who has withdrawn cash from an ATM at a bank where they don't have an account.

A customer is someone with whom the financial institution has an ongoing relationship, wherein the institution provides the individual with some form of service or product continually. There are some differences regarding how these two groups are viewed under the law, so it's essential to understand the nuances.

What is Considered NPI?

NPI, or Non-Personal Information, refers to any information that the customer or consumer discloses, which is not publicly available. This can include but is not limited to: names, addresses, phone numbers, SSN, bank account details, transaction details, purchasing history, income, and credit history. This information is limited in how it can be shared and with whom it can be shared--and if the proper measures are met, the NPI can be shared with third parties.

Who Must Comply With GLBA?

All companies that provide financial services must comply with GLBA, including:

Banks

Insurance brokers

Mortgage brokers

Real estate appraisers

Loan brokers

Financial advisers

CPAs and accounting firms

Also counted among entities that must comply are any businesses that are “significantly engaged” in financial matters. This means companies that extend credit or facilitate obtaining credit through banks, such as universities, colleges, and car dealerships, fall under the category of institutions that must comply with GLBA. Moreover, institutions must adhere to GLBA even if they don't disclose NPI.

How Does GLBA Ensure That Privacy is Upheld?

GLBA has set forth three rules that ensure that NPI is handled properly and securely:

Financial Privacy (Section 504(a))

This rule requires financial institutions to supply customers and, in some cases, consumers with notices upon signing up and every year thereafter, regarding the NPI they collect, how it is used, and with whom it is shared. Additionally, customers and consumers must be informed that they have the option to opt-out of sharing their data.

Pretexting Protection

This rule was established to ensure that financial institutions have a way to protect NPI from malicious actors. Phishing and fraud are common in banking and scammers employ myriad methods by which they try to trick banks into revealing sensitive customer or consumer data. The pretexting law was created to ensure these entities have the proper measures to prevent this from happening.

Safeguards Rule (Section 501 (b))

This rule makes sure institutions have written precautionary measures in place to keep customer data safe. Further, this section says that they must have a plan that specifies at least one employee to be in charge of managing the plan. They must also perform risk analysis across all departments that handle NPI, and the program must be monitored and tested to make sure it's effective. Additionally, they must reassess as needed when changes arise regarding how data is collected and stored.

What Happens if You Violate GLBA?

GLBA is one regulation you really don't want to mess up with, because; failure to comply can result in up to $100,000 in fines per company, per violation; $10,000 for the individual violator per violation, and up to five years jail time for the involved individuals. Violations often incur lawsuits and the inherent loss of customer trust and reputation.

GLBA and CCPA

When **GLBA** was established, it was one of the only federal privacy regulations in town. But today, the compliance regulation scene has grown considerably, with California's **CCPA** and new upcoming state regulations for New York, New Mexico, Hawaii, and others. There's bound to be some overlap between these newcomers and the established **GLBA** requirements.

When it comes to **CCPA**, the regulation applies to all businesses over a specific size that collect CA residents' data, including financial services. Therefore, **CCPA** has stipulated "that personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act, and implementing regulations" is exempt from **CCPA**.

Though it may sound like financial institutions that comply with **GLBA** are off the hook for CCPA, this isn't the case in actuality. In fact, as of this writing, the line of delineation between **CCPA** and **GLBA** is very murky at the moment and how exactly this overlap will be dealt with remains to be seen.

So How Can You Assure Compliance?

There's no room for playing around when it comes to GLBA; in order to stay continuously on the right side of this regulation, you need to get a complete, accurate, and always up-to-date picture of the data you hold on your customers and consumers. 1touch.io InventaTM

enables financial institutions to automatically locate all NPI types in their network – structured and unstructured, in motion and at rest, and known and unknown – to ensure sustainable compliance. With 1touch.io, you can ensure you steer clear of the massive fines and life-altering repercussions associated with failure to comply with GLBA.