




# **How to Achieve GLBA Compliance: A Guide for Financial Services**

---





**Everything financial institutions need to know for GLBA compliance, including the provisions of the law itself, what data you need to safeguard and disclose to consumers, penalties you could face as an organization — and possibly individual — for noncompliance, new exemptions and challenges the CCPA presents, and how BigID can help you ensure the confidentiality and security of your consumers' data.**

# Table of Contents

Introduction	04
What Is the Gramm-Leach-Bliley Act (GLBA)?	05
Defining Nonpublic Personal Information (NPI)	06
What Is a “Financial Institution” Under GLBA?	07
“Consumers” vs. “Customers”	08
Maintaining GLBA Compliance: The 3 Sections of the GLBA	09
a. The Financial Privacy Rule	09
b. The Safeguards Rule	10
c. The Pretexting Prohibition	11
GLBA Fines, Violation Penalties, and Compliance Benefits	12
CCPA For Financial Institutions: Exemptions for Data Protected Under GLBA	13
How BigID’s Data Intelligence Platform Helps With GLBA Compliance	14

# Introduction

---

Financial institutions and their affiliated companies who collect data from consumers and customers have a responsibility to keep that data safe.

The federal Gramm-Leach-Bliley Act (GLBA) regulates how businesses that are significantly engaged in providing financial products or services handle customers' and prospective customers' personal information.

Financial institutions and their affiliates who collect data from consumers often find it difficult to:

- capture siloed and hard-to-find data from many data sources
- find difficult-to-identify critical data
- locate dark data that has a way of hiding
- consolidate visibility into their data
- eliminate redundant, duplicate, or similar data
- solve for other issues that can affect business value and company reputation, from improving data quality to classifying critical data

All of this can make it hard for organizations to discover, manage, and protect all types of sensitive data for regulatory compliance.

We'll take you through everything you need to know for GLBA compliance, including the provisions of the law itself, what data you need to safeguard and disclose to consumers, penalties you could face as an organization — and possibly individual — for noncompliance, new exemptions and challenges the [California Consumer Privacy Act \(CCPA\) presents](#), and how BigID can help you ensure the confidentiality and security of your consumers' data.

# What Is the Gramm-Leach-Bliley Act (GLBA)?

---

Enacted on November 12, 1999, the GLBA — also known as the GLB Act or the Financial Modernization Act of 1999 — is a U.S. federal law that requires financial institutions “to explain their information-sharing practices to their customers and to safeguard sensitive data.”

The law aimed to modernize the financial industry and tighten consumer data privacy safeguards by ensuring the confidentiality of customers’ private and financial information.

Broadly speaking, the GLBA requires that companies acting as “financial institutions” take steps to ensure the confidentiality and security of their customers’ “nonpublic personal information” (NPI). The regulation additionally limits the disclosure of NPI to nonaffiliated third parties.

This means that financial institutions must notify customers about their information-sharing practices and inform customers of their right to “opt out” of having their data shared.

**Financial institutions must inform customers of their right to “opt out” of having their data shared.**

The Federal Trade Commission (FTC) is the main agency that enforces the GLBA. State laws can require greater compliance, but not less than what’s required by the GLBA.

# Defining Nonpublic Personal Information (NPI)

---

The GLBA protects nonpublic personal information, which is any personally identifiable financial information that is not otherwise publicly available.

NPI may include names, addresses, phone numbers, social security numbers, bank and credit card account numbers, credit or debit card purchases, court records from a consumer report, or any other consumer financial information that:

- a consumer provides to a financial institution
- results from a transaction or service performed for the consumer
- is otherwise obtained by the financial institutions

NPI does not include information that has been made publicly available or widely distributed in the media or public government records.

To determine that a piece of information is not NPI, an organization needs to ensure it's something that's made lawfully available to the public generally, and that the individual has not opted to keep the information private, given the choice.

Companies can share NPI with affiliated and non-affiliated third parties, provided customers and consumers have been informed according to the provisions of the regulation.

# What Is a “Financial Institution” Under GLBA?

---

The GLBA defines “financial institutions” as companies that are “significantly engaged” in providing financial products or services — such as loans, financial or investment advice, insurance, etc. — to individual consumers or customers.

GLBA applies to both these organizations and their “affiliates,” defined as any entity that receives consumer financial information from a financial institution.

A broad range of businesses of all shapes and sizes fall under this category, including, but not limited to:

- banks
- non-bank mortgage lenders
- loan brokers
- some financial or investment advisers
- debt collectors
- tax return preparers
- real estate settlement service providers and appraisers

In addition to straightforward financial institutions and those that directly collect NPI from customers or consumers, entities that receive consumer financial information from a financial institution may also face restrictions under the Financial Privacy Rule — one section of the three-part GLBA.



# “Consumers” vs. “Customers”

---

Under GLBA, “customer” and “consumer” are not used interchangeably. “Consumer” is a broader category, encompassing “customers.” So, all customers are consumers, but not all consumers are customers. This distinction is important under the Financial Privacy Rule, which treats customers and consumers somewhat differently (see “The Financial Privacy Rule” below).

A “consumer” is an individual who obtains or has obtained a financial product or service from a financial institution primarily for personal, family, or household purposes — or that individual’s legal representative. Some typical consumer relationships include:

- applying for a loan, whether or not it’s accepted
- obtaining cash from an ATM where an account is not held (even repeatedly)
- making or arranging for a wire transfer
- cashing a check with a check-cashing company

A “customer” is a subclass of consumer who maintains a continuing relationship with a financial institution. Some common customer relationships include:

- obtaining a loan from a mortgage lender or payday lender
- opening a credit card account with an institution
- leasing a car from a car dealership
- using a mortgage broker to secure financing
- engaging the services of a tax preparer or investment advisor



# Maintaining GLBA Compliance: The 3 Sections of the GLBA

---

GLBA consists of three sections, each establishing a different rule:

**The Financial Privacy Rule**, which regulates the collection and disclosure of private financial information

**The Safeguards Rule**, which requires financial institutions to implement security programs to protect this information

**The Pretexting Prohibition**, which prohibits the access of private information under false pretenses

---

## THE FINANCIAL PRIVACY RULE

The Financial Privacy Rule (or just the Privacy Rule) mainly concerns disclosure of practices. It requires financial institutions to give their customers (and sometimes consumers) clear and conspicuous written notice describing their privacy practices and policies.

Organizations must provide each consumer with a privacy notice at the time they become a customer, and every year while they remain one.

The notice must contain the information collected about the customer, where it's shared, with whom, and how it's used and protected. It also specifies the customer's right to opt out of having their information shared with third parties.

The distinction between consumers and customers is relevant under GLBA because it requires companies to give these notices to all their customers, but only to certain consumers.

## THE SAFEGUARDS RULE

The Safeguards Rule focuses mainly on information security. It mandates that financial organizations protect the customer information they collect. To comply with the rule, companies must develop a written information security plan that describes how they protect their data.

Some of the protections they need to provide involve:

- designating employees to coordinate an information security program
- assessing risk in each area of the company
- monitoring and testing safeguards
- maintaining contractors who also meet compliance standards
- constantly evaluating and optimizing as business operations and risk assessments change

Companies must also secure private information against unauthorized access and track user activity, including any attempts to access protected records.

The specific requirements vary depending on the company's size, complexity, and circumstances, but they're all designed to ensure that financial institutions address risks to customer information across all areas of their operation, in particular:

- employee management and training
- information systems
- detecting and managing system failures

## THE PRETEXTING PROHIBITION

The Pretexting Prohibition basically amounts to: don't lie to institutions or customers to obtain information.

Pretexting involves collecting information under false pretenses, or knowingly convincing customers to divulge information in the context of a made-up story. The prohibition forbids the use of false, fictitious, or fraudulent statements to get customer information — either from a financial institution or directly from a customer.



# GLBA Fines, Violation Penalties, and Compliance Benefits

---

Financial institutions found in violation of GLBA can face civil penalties of up to \$100,000 for each violation.

Officers, directors, and other individuals in charge at the organization can also personally face fines of \$100,000 for each violation — and even possible prison time of up to five years. In other words, non-compliance can be detrimental to businesses and individuals, and also life-altering.

**Institutions that violate GLBA face fines of up to \$100,000 per violation — and so do individuals.**

Organizations who do maintain compliance with GLBA, on the other hand, not only avoid financial penalties, but increase trust and loyalty among customers. When customers feel secure in the way their information is being handled by their financial institution, it can boost reputation and repeat business.



# CCPA For Financial Institutions: Exemptions for Data Protected Under GLBA

With the adoption of the CCPA, financial institutions face new regulations.

While CCPA allows for certain exemptions on the specific data that is covered by the GLBA, it does not exempt the financial organizations themselves. The exemption allows for information that is already “collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act.”

However, CCPA covers a wider range of information, defined as “personal information (PI),” or “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”

So, **while NPI is exempt from CCPA compliance and the scrutiny of the California Attorney General’s Office, PI is still fair game.** Put simply, this means that anytime a financial institution collects information for purposes other than financial ones — or draws “inferences” from that data — it is subject to the same CCPA requirements as everyone else. Think data for marketing purposes, website visitors, and geolocation data.

“While NPI is exempt from CCPA compliance,  
PI is still fair game.”

Financial institutions are also subject to the right of private action that CCPA covers, which is the right of consumers to seek statutory damages in the event of a breach.

# How BigID's Data Intelligence Platform Helps With GLBA Compliance

---

Ensuring the confidentiality and security of consumers' data requires building a modern privacy framework that can quickly respond to GLBA, CCPA, and all regulatory requirements that impact financial institutions.

Managing, securing, and reporting on data starts with knowing what you have, where it lives, who it belongs to, why you collected it in the first place, and so on. BigID leverages next-generation data discovery to give you full visibility into all of your data — including NPI — everywhere, at petabyte-scale.

Discovery-in-depth goes beyond traditional discovery, which only sees one type of data, and targeted data discovery, which only finds data that you already know about. A deep discovery foundation provides real insight into your data so you can better protect it and maintain full compliance. Using advanced machine learning, BigID empowers financial institutions to:

- identify and classify NPI and critical data to help know its purpose of use, quality, risk impacts, and more
- automatically catalog sensitive data and metadata in data from structured, unstructured, cloud, Big Data, noSQL, and data lake sources
- find, flag, and tag combinations of data
- leverage cluster analysis to identify duplicate, derivative, and similar data

Here's a deeper look at some of the ways BigID helps financial institutions manage, protect, and report on consumer data.

---

### **UNMATCHED COVERAGE IN A SINGLE PANE OF GLASS**

Get broad coverage for unstructured, structured, semi-structured, big data, data in motion, and more, so you can get full visibility and enforce policy not just on a segment of your data, but all of it — financial, customer, consumer, employee — in a single pane of glass.

---

### **PATENTED DISCOVERY-IN-DEPTH TECHNOLOGY**

Traditional auditing and compliance tools focus on pattern-based classification. BigID goes beyond that, leveraging patented machine learning technology including NLP and deep learning to identify and classify everything from dark data to sensitive data to first name.

---

### **COMPLIANCE, CUSTOM CLASSIFIERS, AND REPORTING**

BigID helps organizations meet compliance for not only GLBA and CCPA, but a variety of regulations affecting financial services, including NY DFS, SOX, NY SHIELD & more.

We automatically classify regulated data — including NPI and PI — to help you enforce its proper handling. You can also create custom classifiers for specific policies to make reporting easier.

---

### **DISCOVER DARK DATA**

Traditional data approaches require that you know where your data is in order to protect it. BigID's ML-based discovery and classification means we identify and classify sensitive data even if you don't know it's there.

## LEVERAGE SECURITY ECOSYSTEM

Integrate with your investments: with BigID, get smarter DLP enforcement, targeted data encryption, and OOB integrations with Cyberark, ServiceNow, Hashicorp, and more.

## REDEFINE DATA SECURITY FOR YOUR ORGANIZATION

When you achieve full visibility into your data, compliance with GLBA and other privacy regulations is just one business outcome you can look forward to. BigID helps financial organizations drive a solid security framework by enabling organizations to:

- map and inventory NPI, sensitive, and critical data
- automate policy checks and enforcement around data movement
- review open access and overexposed data
- get insights on access intelligence to reduce risk and protect NPI and PI
- accurately determine impacted users in the event of a data breach
- prioritize risk remediation with risk scoring based on data type, location, access, consent, and more
- enable workflows to remediate at-risk data and proactively protect sensitive data

### Want to know more?

[Schedule a demo](#) to see how BigID can help you discover, classify, and catalog all types of sensitive data across an organization's data landscape in a single pane of glass.