Privacy: GLBA & CCPA

Training Material for FinTech Employees

FinancialStrides

Overview

As a FinTech, you are the “front-end” for financial services sold to customers, which are also the customers of your partner bank. Your interacting with customers results in responsibilities regarding consumer privacy.

The objectives of this material are to:

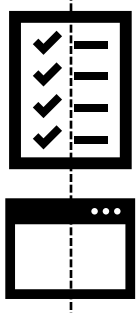
- Define key terms and scope of privacy regulations, including:
  - The Gramm–Leach–Bliley Act (“**GLBA**”)
  - The California Consumer Privacy Act (“**CCPA**”)
- Help create privacy notices: content and timing of distribution
- Help implement data mapping, data security, and processes to implement compliance

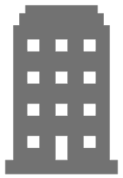
NOTE: this material is not a substitute for professional legal advice

FinTech Has 1st-Line Role

Customers

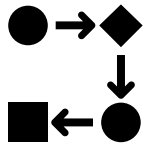
- Receive Privacy Notices
- May opt-out of data sharing
- May request deletion of records
- May request copies of data





FinTech

- Create Product
- Advertise & Sell
- Captures and stores Non-Public PII
- Operate
- Support



\+

Bank*

* Unless FinTech is a state-licensed lender and does not use a partner bank

The Basics

Coverage	Gramm Leach Bliley Act	California Consumer Privacy Act
Who is covered?	• Financial Institutions • Businesses "significantly engaged in financial activities", i.e. FinTechs	For-profits doing business in CA & meeting any of: • >$25M in revenues, or • Data on > 50,000 consumers, households or devices, or • >50% of revenues from selling data
What Data?	• Non-Public Personally Identifiable Info (NPI) • financial information	Extended NPI Extended activities: finance, insurance, health, commerce, education, work…. Tracking: browser, geolocation…
Shareable or not covered	processing & servicing, fraud protection, vendors, business ops and compliance	Data already protected by GLBA
Enforced by	Financial regulators (banks) FTC (non-bank lenders)	California Attorney General

Gramm Leach Bliley Act

The Gramm-Leach-Bliley Act (**GLBA**) was enacted in Dec 1999 and requires financial institutions to explain how they share and protect their customers' private information. Privacy and safeguards rules are enforced by the **FTC** for non-banks. Information security guidelines for banks & credit unions are published by the **FFIEC** (**FDIC + FRB + CFPB + OCC + NCUA**). The **CFPB** enforces privacy rules (Reg. P)

To be GLBA compliant, **financial institutions** and **businesses "significantly engaged in financial activities"**, must:

1. Communicate to their customers how they protect and sometimes share the customers' sensitive data,
2. Inform customers of their right to opt-out if they prefer that their personal data not be shared with third parties, and
3. Apply specific protections to customers' private data in accordance with a Written Information Security Plan created by the institution:
   - ✓ Ensure the security and confidentiality of customer information;
   - ✓ Protect against any anticipated threats or hazards to the security or integrity of such information; and
   - ✓ Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Contact us at info@finstrides.com for more…