May 10, 2024

Privacy and Security Challenges for Fintechs

Jeremy Berkowitz
Paul Hastings LLP

Steve Boms
Allon Advocacy

Seyi Iwarere
Block

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Jeremy Berkowitz

Senior Director, Paul Hastings LLP

Steve Boms

Founder and President
Allon Advocacy

Seyi Iwarere

Payments Regulatory Counsel, Block

Use of Fintech/Banking Applications

Privacy+ Security Forum

1. **What are people's comfort levels with financial applications connected to bank accounts? How many apps on your phone are connected to one of your bank accounts:**

2. **When was the last time you checked the privacy settings on these apps?**

3. **With any given app, how often do you have to reverify yourself or reconnect your bank account?**

Discussion Topics for Today

Privacy+ Security Forum

- 1033 Rulemaking
- Consequences of Recent Data Breaches
- Untangling the Processor-Controller Responsibilities

Overview of 1033 NPRM

- The Dodd-Frank Act passed in 2010, in response to the 2007-2008 banking crisis.
- Section 1033 of the Act required the newly created Consumer Protection Financial Bureau (CFPB) to implement rules around the protection of consumer financial data and how that data could be shared amongst consumers and data providers (e.g. financial institutions).
- In October 2023, the CFPB finally released a draft rule to begin to implement Section 1033 and opened a comment period. The Final Rule is expected to be released before the end of this year.

Overview of 1033 NPRM

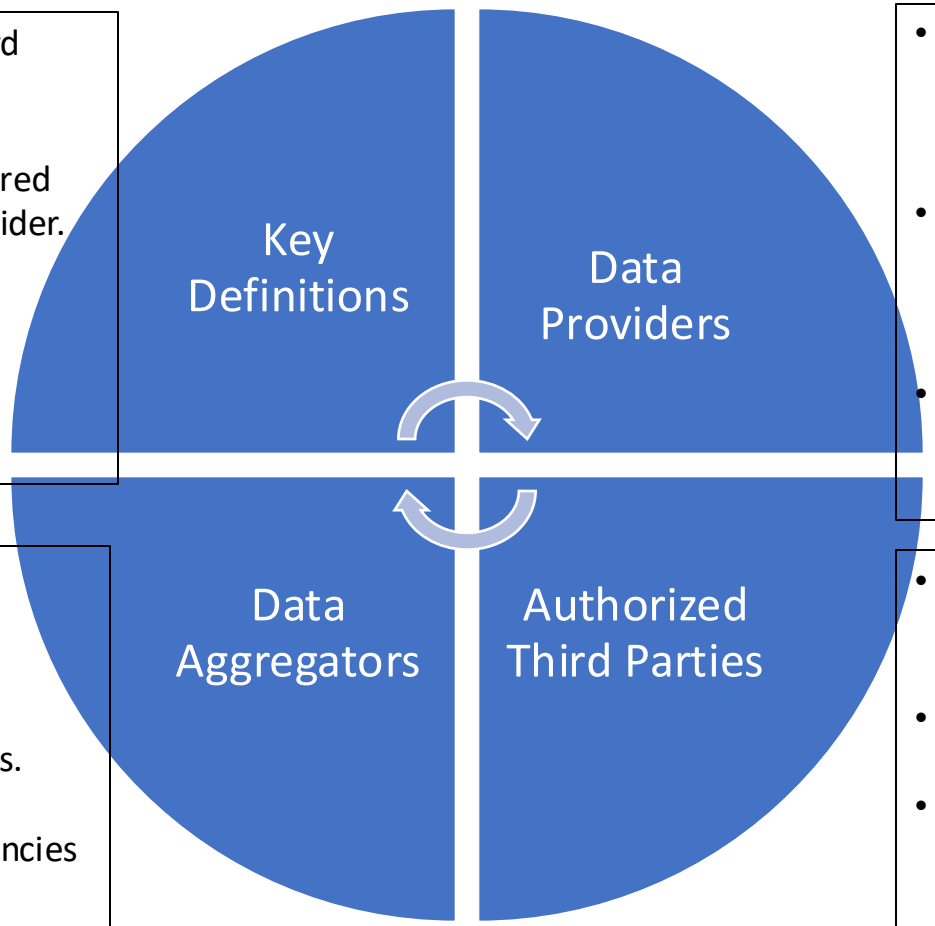
Privacy+ Security Forum

Data Provider: Financial institutions (Reg. E); Card Issuers (Reg Z). This includes digital wallets.

Authorized Third Party: Entity that receives covered data with permission/authorization of Data Provider.

Covered Data:

- Transaction Data
- Account Balances
- Payment Information



- Obligations to provide free access to covered data to consumers, authorized third parties, and data aggregators.
- Develop information security programs that comply with GLBA and/or the FTC's Safeguards Rule.
- Implement developer interfaces (e.g. APIs) to hinder screen scraping by third parties/data aggregators.

- Would be permitted by third parties to access covered data.
- Authorization for aggregators would have to be presented by third parties to consumers.
- May be regulated as consumer reporting agencies under the FCRA.

- Provide GLBA security protections around collection of data.
- Prohibit the use of data for targeted advertising.
- Not retain data for more than 1 year.

Data Breach Challenges

- In May 2024, Evolve Bank & Trust was subject to a data breach after an employee clicked on a link in a phishing email. Evolve offers a banking-as-a-service, exposing its fintech partners.

- Data released into the public realm included 33 terabytes of consumer personal information (e.g. SSNs, bank routing numbers, Account Numbers).

- The Prudential Regulators released an RFI last month that focuses on bank-fintech arrangements and risk management practices, including incident response.

Roles of Controller/Processor

Privacy+ Security Forum

Fintechs have been viewed as data processors of personal data. In recent years, there has been a growing emphasis on fintechs' obligations as data controllers, where they sometimes have also have responsibilities for the ways and means of processing.