INDEPENDENT COMMUNITY BANKERS of AMERICA®

Brad M. Bolton, *Chairman*
Derek B. Williams, *Chairman-Elect*
Lucas White, *Vice Chairman*
Tim R. Aiken, *Treasurer*
Sarah Getzlaff, *Secretary*
Robert M. Fisher, *Immediate Past Chairman*
Rebeca Romero Rainey, *President and CEO*

*Via Electronic Submission*

November 21, 2022

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Suite CC-5610 (Annex B)
Washington, DC 20580

**RE: Commercial Surveillance ANPR, R111004**

Dear Sir or Madam:

The Independent Community Bankers of America ("ICBA")[1] welcomes this opportunity to comment on the Federal Trade Commission's ("FTC" or "The Commission") Advanced Notice of Proposed Rulemaking ("ANPR") on Commercial Surveillance and Data Security.

ICBA and its members appreciate the FTC's concern with the data collection, storage, and security practices of businesses, particularly with respect to businesses who collect, handle, or sell consumer financial information outside of the purview of the federal banking regulators. Community banks play an integral role in protecting consumer data and ensuring the privacy of millions of Americans, so we welcome the opportunity to engage with The Commission on this critical issue.

[1]*The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. ICBA is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education, and high-quality products and services.*

*With nearly 50,000 locations nationwide, community banks constitute 99 percent of all banks, employ nearly 700,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding more than $5.8 trillion in assets, over $4.9 trillion in deposits, and more than $3.5 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities throughout America. For more information, visit ICBA's website at* www.icba.org
.

## Summary

Through this ANPR, the FTC attempts to tackle a critical issue for American consumers – great uncertainty surrounds how consumer data is used, stored, shared, and sold. Most consumer products and services require that consumers provide personal information in order to access said products or services. However, very little is known about how that data is used. While some industries, such as financial services, operate in a highly regulated environment, many other industries have little to no oversight.

In this letter, ICBA outlines three areas the FTC should consider if it is to move forward with rulemaking:

- FinTechs, data aggregators, and other businesses holding large amounts of consumer financial data should be subject to regulatory oversight and transparency with regard to how consumer financial data is used, stored, shared, and sold.
- Gramm-Leach-Bliley Act-like ("GLBA") data security standards should apply to any company possessing or processing consumer financial data.
- Entities that experience a data breach while holding consumer financial data should bear the full financial responsibility for that breach.

ICBA acknowledges the need for greater transparency and security in the protection and uses of consumer data. However, this ANPR attempts to tie together unrelated topics, while providing little detail as to what the scope and parameters of any potential rule may entail. Furthermore, rulemaking would add a significant burden to small and medium-sized businesses by adding to the patchwork of data privacy laws throughout the country. Consumer data cannot be properly secured, and privacy ensured, without a more uniform approach nation-wide.

**Regulatory Oversight**

Over the past decade, non-bank entities, namely large technology companies, fintechs, and data aggregators benefited from unregulated access to storage sharing and selling of sensitive consumer financial data without the scrutiny of regulation, examination, or comparable security requirements that banks are required to follow. These companies aggregate and use those records to create profiles of consumers and offer new products and services based on their findings. ICBA has serious concern that non-bank entities, which access customer information and store bank login credentials, do not take proper care in protecting consumer privacy and data security. The integrity of consumer data and privacy is only as strong as the weakest link protecting that information. As more non-regulated entities handle consumer data, the risks of breach, misuse, and loss increases.

When consumers choose to share their financial data with companies that are not regulated to the same level as banks, they do not have a clear understanding of who will have access to their data, how it will be used, or to whom the data may be shared or sold. This is also a problem when the company chooses to use the data they collect for additional profit by selling the data to a third-party. For example, when a customer provides their banking login information to a third-party

budgeting app that has no relationship to their bank, the consumer may be unknowingly providing additional technology companies with access to the consumer's banking account and financial data for disclosed uses as well as undisclosed uses.

In recent years, application programming interfaces ("API") have increased in popularity as an alternative to direct access to data by consumers sharing their banking system credentials. APIs negate the need for technology companies to hold account log-in credentials. However, the concern is that some APIs have been developed by technology companies as a service to act as a middleman between the bank accounts and the apps passing information between them. Consumers now not only have to worry about the company they think they are dealing with, like a budgeting app or data aggregator, but they may now be dealing with an API middleman who also has access to consumer data. One such company stated that 25% of all people in the U.S. with bank accounts have connected to their company.[2]

Data aggregators, fintechs, and large technology companies benefit from unregulated access to sensitive consumer financial data. In some cases, they have even begun to blur the line between bank and non-bank, adding confusion and deception to an already complex ecosystem. Banks, on the other hand, are vigorously examined by federal regulators for consumer and data protection compliance and must have a strong security and privacy program in place to protect consumer data. It is crucial that all companies that have access to consumer data are regulated to protect that data and the privacy of their customers, as strongly as banks.

**Privacy and Data Security Standards**

It is important that all participants in the payments and financial sector ecosystem, including aggregators, fintechs, and technology companies with access to customer financial information are subject to GLBA-like data security standards.

The FTC and the federal banking regulators help to maintain a safe, secure, and transparent financial system, including overseeing regulations on data security and data privacy. Partially due to this, consumers understand what information is required of them to obtain access to financial products, and financial institutions secure customer data and maintain their customer's privacy.

Financial organizations overseen by the FTC and the federal banking regulators[3] are governed by strict data security laws and regulations, as set forth by GLBA and its implementing regulations.[4]

---

[2] https://www.cnbc.com/2020/01/13/visa-to-acquire-plaid-the-fintech-powering-venmo-and-other-banking-apps-for-5point3-billion.html

[3] Federal banking regulators include the Federal Reserve Board, Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau.

[4] The FTC along with federal banking regulators and the Consumer Financial Protection Bureau enforce Safeguards and Privacy rules of the Gramm-Leach-Bliley Act. These rules require covered entities to develop, implement and maintain information security programs as well as notify customers about the information collected, who it is shared with and how it is protected. More information about the regulations: https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act and https://www.consumerfinance.gov/rules-policy/regulations/1016/

Any financial institution subject to GLBA oversight is examined yearly by their federal regulators to insure they are in compliance. Among other things, these regulations require financial institutions to disclose their information sharing practices to their customers, provide choices to consumers in how data is used, requires banks to safeguard sensitive data, and create robust data security, thus creating a high level of transparency, privacy, and security. Protecting consumer financial data is central to maintaining public trust and key to long-term customer retention.

However, not all entities are governed by such strict security regulations. As previously mentioned, technology companies, fintechs, and data aggregators holding similar are not required to have strict data security practices. No matter how securely community banks store consumer data, if others in the financial and payments ecosystem are not required to have similar safeguards, consumer data will be at higher risk of compromise.

ICBA strongly believes that any entity who stores, shares, or otherwise handles consumer financial data must be governed by similar standards as financial institutions already under the supervision of the FTC or federal banking regulators.

Furthermore, companies must be held responsible for breaches when they are not properly securing data. While consumers are often made as whole as possible, this comes at the expense to other companies such as banks and other institutions responsible for card reissuance, and credit monitoring. These costs should ultimately be borne by the party that incurs the breach. This would serve not only as an incentive for stronger security, but as a recovery mechanism for companies who unfairly bear the cost of poor security elsewhere.

**Concerns with this ANPR**

ICBA is concerned with the overly broad scope of this ANPR. As previously stated, data privacy and data security are of the upmost importance to community banks across the country. The topics raised by this ANPR range from data privacy and security standards to child endangerment, artificial intelligence biases, and mental health. A more focused ANPR would allow for more focused comments from the public, and a more effective rule for each subject the ANPR attempts to tackle.

Furthermore, as multiple commissioners pointed out in their statements, this proposed rulemaking directly conflicts with ongoing efforts in Congress to establish national data security standards, potentially nullifying this effort.[5] ICBA recommends the Commission focuses this effort on standardizing data security standards across industry while Congress works to pass a national data privacy standard that can more uniformly applied. This will ensure consumer data is properly secure while alleviating the burden and confusion additional layers of data privacy regulation will have on smaller businesses.

[5] Trade Regulation Rule on Commercial Surveillance and Data Security. 87 FR 51273 (8/22/2022). *See: Comments from Commissioner Khan (p.51287), Commissioner Slaughter (p. 51288), Commissioner Phillips (p. 51294), and Commissioner Wilson (p. 51298).*

## Conclusion

ICBA acknowledges the need for stricter data security and data privacy standards for industries where no such standards currently exist, particularly for those that store, maintain, or share consumer financial data – or other sensitive personal data. The Commission should closely examine the practices of data aggregators, fintechs, and other technology companies with access to millions of consumers' data, particularly in cases where consumers are unaware of the access they have provided these companies.

As Commissioner Wilson stated in her dissent, "Recent Supreme Court decisions indicate FTC rulemaking overreach likely will not fare well when subjected to judicial review." If this potential rulemaking were to be held up in courts due to overly ambitious regulation, the only victims would be the consumers such a rule is proposing to protect. The Commission should consider a more focused ANPR for individual topics if it wishes to continue down the rulemaking process.

ICBA appreciates the opportunity to respond to this request for comment and offer counter information relating to the FTC ANPR on Commercial Surveillance and Data Security. If you have any questions or would like additional information, please contact me at Steven.Estep@icba.org or (202) 821-4329.

Sincerely,

/s/

Steven Estep
Assistant Vice President, Operational Risk