November 17, 2022

Submitted Via Regulations.gov

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

RE: Trade Regulation Rule on Commercial Surveillance and Data Security (Commercial Surveillance ANPR, R111004)

Dear Ms. Tabor:

On behalf of ACA International, the Association of Credit and Collection Professionals ("ACA"), I appreciate the opportunity to comment on the Federal Trade Commission's ("FTC" or "Commission") Trade Regulation Rule on Commercial Surveillance and Data Security ANPR ("ANPR").[1] ACA represents approximately 1,800 members, including credit grantors, third-party collection agencies, asset buyers, attorneys, and vendor affiliates in an industry that employs more than 125,000 people worldwide. Most ACA member debt collection companies are small businesses. Women comprise 70% of the ethnically diverse debt collection workforce.

BACKGROUND

ACA members work with consumers to resolve their past debts, which in turn saves every American household more than $700 year after year. The accounts receivable management ("ARM") industry's role serves a critical need in America's credit-based economy. Its efforts keep consumer access to credit at the lowest possible cost. For example, in 2018, the ARM industry *returned over $90 billion* to creditors for goods and services they already provided to their customers.

[1] 87 Fed. Reg. 51,273 (Aug. 22, 2022).

Our industry's collections benefit all consumers by lowering the costs of goods and services, especially when rising prices are hurting Americans throughout our country. Our members use comprehensive compliance tools and apply high ethical standards to ensure consumers are treated fairly. ACA contributes to these efforts by providing timely industry-sponsored education as well as compliance certifications. In short, ACA members are committed to assisting consumers as they work together to resolve their financial obligations, all in accordance with the Collector's Pledge that all consumers are treated with dignity and respect.

The FTC in its ANPR is requesting public comment on the prevalence of commercial surveillance and data security practices that harm consumers. Specifically, the Commission invites comment on whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive.[2] ACA is concerned that the broad scope of the FTC's request (1) goes beyond the authority Congress delegated to the FTC in this area and (2) conflicts and overlaps with planned congressional activity in this area. Accordingly, ACA respectfully requests more information regarding the FTC's views on the interplay between its actions and the impact on the ARM industry before it begins the process of considering and potentially implementing a new and complex regulatory framework in this space.

GENERAL COMMENTS

ACA members are committed to ensuring data security and privacy through robust compliance programs. The existing protections in the ARM industry's data privacy landscape are strong, including, but not limited to, sweeping and complex state legislation such as the California Consumer Privacy Act.[3] Other federal privacy laws in this area include the Health Insurance Portability and Accountability Act of 1996,[4] the Fair Credit Reporting Act,[5] the Gramm-Leach Bliley Act ("GLBA"), which was recently updated by amending the Standards for Safeguarding Customer Information ("Safeguards Rule"),[6] and the Family Educational Rights and Privacy Act of 1974.[7] ACA members abide by these laws in their daily work and spent significant time and resources implementing the changes from the

[2] *Id.*
[3] 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375).
[4] Pub.L. 104–191.
[5] Pub.L. 91-508.
[6] Pub.L. 106–102.
[7] 20 U.S.C.A. § 1232g.

Safeguards Rule.[8] It is critical for the FTC to see how these changes impact consumers and regulated entities before moving ahead with any additional changes to this regulatory framework.

Beyond these important privacy laws, the ARM industry also operates under the Fair Debt Collection Practices Act ("FDCPA"),[9] which protects consumer information and governs how it is communicated. The FDCPA also imposes appropriate limits on what consumer information can be disclosed to others. These protections were further strengthened through the implementation of Regulation F,[10] which was issued by the Consumer Financial Protection Bureau in 2020 and took effect in November 2021. Regulation F alone outlines very prescriptive requirements for interacting with consumers and data sharing protections.

As the FTC considers these potential regulations, it is critical that it more narrowly define its interests in relation to data security and privacy in the ARM industry and financial services industry. Instead, the ANPR takes a sweeping and broad view of the FTC's authority in this area by defining "commercial surveillance" to cover the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information.[11] The ANPR also expands the definition of consumer and states that new rules will cover data that is collected directly from the consumer, as well as data including personal identifiers.[12] As Commissioner Noah Phillips noted in his dissenting statement from August 11, 2022,

> "[the ANPR] requests information ranging from what practices companies currently use to "surveil consumers" to whether there should be a rule granting teens an "erasure mechanism," what extent any new commercial surveillance rule would impede or enhance innovation, the administrability of any data minimization or purpose limitation requirements, the "nature of the opacity of different forms of commercial surveillance practices," and whether the Commission has "adequately addressed indirect pecuniary harms, including . . . psychological harms."[13]

[8] 16 CFR part 314.
[9] U.S.C. § 1692-1692p.
[10] 85 Fed. Reg. 76734, 76735 (Nov. 30, 2020).
[11] 87 Fed. Reg. 51,273 (Aug. 22, 2022).
[12] *Id.*
[13] See Dissenting Statement of Commissioner Noah Joshua Phillips (August 11, 2022), available at https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Phillips%20Dissent%20to%20Commercial%20Surveillance%20ANPR%2008112022.pdf.

Ultimately, the scope and breadth of the FTC's ANPR is overly broad and arguably beyond the scope of the FTC's jurisdiction. Moreover, it does not identify any measurable range of proposals being contemplated by the FTC nor does it establish any jurisdictional limit or guardrails as to which issues in the privacy and data security space would appropriately fall under the purview of any future proposed rules. Thus, it is impossible, without more information on these issues, to provide a meaningful response to the ANPR.

The FTC needs to (a) provide more clarity with respect to its jurisdiction to implement such an overly-broad regulatory framework, particularly in light of Congress' express statutory authority to legislate in this space, and (b) in doing so, explain its intent with respect to future rules for financial services providers including participants in the ARM industry. The ARM industry, as mentioned, is already subject to robust standards under the GLBA and likely should be exempt from conflicting or duplicate rulemaking efforts by the FTC. The financial services landscape has robust protections already in place and the FTC should consult with financial regulators, as well as study how consumers in this space are impacted, before any sweeping changes are made.

Additionally, as you know, Congress is also considering changes in the data privacy landscape through the American Data Privacy and Protection Act ("ADPPA"), as well as several other proposed bills related to establishing a federal privacy standard. Given recent congressional action in the data privacy space (i.e., passage of the ADPPA out of committee with nearly unanimous consent), it is premature for the FTC to consider such a broad scope of rulemaking without waiting for Congress to provide appropriate statutory authority and direction as part of currently pending privacy-related legislation. For example, the ADPPA, as well as other data security legislative proposals pending in Congress, expressly grant the FTC authority to engage in rulemaking with respect to certain issues (e.g. establishing guidelines for algorithmic impact, data minimization, and other issues).

In contrast, the FTC's ANPR encompasses 95 questions with no express jurisdictional limit. We recognize that the FTC's ANPR reflects a request for public input, and therefore, is not a proposal for final rulemaking. However, given the broad scope of the 95 questions contained in the ANPR, we, along with other industry participants, are concerned that the ANPR's scope and discussion of several matters currently pending before Congress are an effort by the Commission to usurp the express authority of Congress and shape the country's privacy-related framework without oversight or direction from the necessary elected officials.

While we firmly believe that the broad scope of the FTC's ANPR sidesteps Congress' rightful statutory authority in the data privacy space, we also believe that the FTC currently has an appropriate role in

the rulemaking process so long as its actions are consistent with the authority delegated to it by Congress. For example, the FTC should establish clear and streamlined guidance with respect to its data security rules (instead of the current patchwork of regulations and nonbinding guidance) so that the marketplace and industry participants are subject to a clear set of uniform rules. In particular, this rulemaking would complement Congress' pending consideration of the ADPPA and other data privacy legislative proposals.

Action by the FTC with respect to data security would not only supplement current congressional consideration of pending legislation, it would also build on the FTC's existing precedent focusing on data security and the role that it plays in the data privacy ecosystem. Ultimately, we urge the FTC to focus on areas for which it has been delegated the authority to promulgate rules and regulations by Congress, including data security. The current scope of the ANPR goes far beyond the FTC's authority and would result in an encroachment of Congress' rightful statutory authority. We recognize the need for further data privacy guidance and standards, particularly in comparison to the regulatory frameworks implemented by other countries; however, the FTC should refrain from seeking to implement such a framework without first giving Congress the opportunity to address privacy issues from a legislative perspective.

It is also critical that regulations in this area promulgated by the FTC do not result in additional and unnecessary burdens for the ARM industry because they contain duplicative or overly burdensome new requirements, either on their own, or taken together with existing regulatory and statutory requirements. Most ACA members are small businesses and are often working to help other small businesses. They are already working diligently to protect private consumer data in compliance with the existing and robust privacy laws and regulations. Further, small businesses generally do not collect, retain or otherwise utilize the copious amounts of data that larger businesses utilize in their ordinary course of business. Thus, the FTC should acknowledge that any proposed regulations should consider the different needs and uses of consumer data by small businesses versus larger businesses.

Uniform regulations that do not consider the different needs, uses and costs of collecting and retaining data by different businesses would result in undue burdens on smaller businesses that do not have the resources to absorb such costs compared to larger businesses. However, congressional legislation that preempts the tangled web of state privacy laws would benefit Americans who deserve to receive a uniform level of privacy protections. Sweeping, costly, and burdensome regulations from the FTC hinted at in this ANPR would not accomplish that goal. To the extent a regulatory framework in the privacy space is established, there must be different tiers for compliance with such requirements to ensure small businesses do not face significant compliance costs that they cannot afford, particularly

in our current economic climate riddled with historically high levels of inflation. Further, the FTC should consider a grant or other program for funding purposes to ensure small businesses are supported in their efforts to comply with new rules and regulations. Ultimately, any proposed regulatory framework under consideration by the FTC must balance the need for data security with ensuring that regulated entities can continue to operate in their ordinary course of business without negative impacts to revenue and innovation.

As the FTC continues to consider how it might move forward with rulemaking in this area, we appreciate the opportunity to be part of that conversation on behalf of the ARM industry. Thank you for your attention to our comments, please contact Leah Dempsey at Ldempsey@bhfs.com or myself if you have any questions and would like to discuss this further.

Sincerely,

Scott Purcell
Chief Executive Officer