consumer relations consortium
connect | collaborate | advance

November 21, 2022

Re: Commercial Surveillance ANPR, R111004
Document Number 2022-22813

To: Federal Trade Commission

Comment to Commercial Surveillance ANPR, R111004

The Consumer Relations Consortium (CRC) is an organization comprised of more than 60 national companies including compliance-oriented debt collectors, creditors, debt buyers and data/technology providers, all of whom are larger market participants. Established in 2013, CRC is dedicated to a consumer-centric shift in the debt collection paradigm. It engages with all stakeholders—including consumer advocates, federal and state regulators, academic and industry thought leaders, creditors and debt collectors—and challenges them to move beyond talking points. The CRC's focus is on fashioning real-world solutions that seek to improve the consumer's experience during debt collection. CRC's collaborative and candid approach is unique in the market.

CRC members exert substantial positive impact in the consumer debt space, servicing the largest U.S. financial institutions and consumer lenders, major healthcare organizations, telecom providers, government entities, hospitality, utilities and other creditors. CRC members engage in millions of compliant and consumer-centric interactions every month at all stages of the revenue cycle. Our members subscribe to the following core principle:

"Collect the Right Debt, from the Right Person, in the Right Way."

We appreciate the opportunity to comment on the Advanced Notice of Proposed Rulemaking from the Federal Trade Commission regarding a potential data trade regulation rule. As the FTC is aware, the debt collection industry is already subject to multiple Federal and State laws that protect the safety and integrity of consumer data. We recommend that the FTC focus on enforcing the existing laws already passed by Congress that have proven effective in ensuring data privacy – such as the federal Gramm Leach Bliley Act – rather than seeking to overlay additional, untested privacy rules that will clearly harm consumers and have other unintended consequences.

Sincerely,

Missy Meggison

Missy Meggison
Executive Director, Consumer Relations Consortium

consumer relations consortium
connect | collaborate | advance

COMMENT TO NOTICE OF PROPOSED RULEMAKING

Sources and Use of Consumer Data by the Collection Industry

Companies in the debt collection industry rely upon consumer data to accurately and effectively provide consumers with the information they request and require to engage in financial transactions. This consumer data includes personal-identifier information that the consumer shared with the original creditor or is otherwise obtained, the creditor's transaction and payment history with the consumer and any other information about credit reporting regarding the consumer, correspondence and transactions on the account.

The Existing Federal Regulatory Framework for Protecting Consumer Data

The Gramm Leach Bliley Act is a comprehensive law enforced by the FTC that requires financial institutions – including debt collectors and debt buyers – to explain their information-sharing practices to their customers and to safeguard sensitive data. Financial institutions covered by the Gramm-Leach-Bliley Act ("GLBA") must disclose to their customers applicable information-sharing practices and explain to customers their right to "opt out" if they don't want their information shared with certain third parties.

The FTC Safeguards Rule requires debt collectors to implement and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information. As the name suggests, the purpose of the Federal Trade Commission's Standards for Safeguarding Customer Information – the Safeguards Rule, for short – is to ensure that entities covered by the Rule maintain safeguards to protect the security of customer information. The Safeguards Rule took effect in 2003, but after public comment, the FTC amended it in 2021 to make sure the Rule keeps pace with current technology. While preserving the flexibility of the original Safeguards Rule, the revised Rule provides more concrete guidance for businesses. It reflects core data security principles that all covered companies need to implement.

Questions from the ANPR and the Response of the Consumer Relations Consortium

Q-#10. Which kinds of data should be subject to a potential trade regulation rule? Should it be limited to, for example, personally identifiable data, sensitive data, data about protected categories and their proxies, data

that is linkable to a device, or non-aggregated data? Or should a potential rule be agnostic about kinds of data?

CRC Response: To the extent the contemplated FTC trade regulation will apply to market participants regulated by existing federal and state privacy laws, we recommend that the contemplated regulation rule apply only to data not otherwise subject to current statutory regulation such as the GLBA and the Safeguards Rule described in detail above. Thus, the proposed trade regulation rule would apply to data used, for instance, for consumer lead generation, telemarketing and other sales related activities where the user of data and its principals have no contractual relationship to the source of data that was authorized by law to use and share it.

Q-# 11. Which, if any, commercial incentives and business models lead to lax data security measures or harmful commercial surveillance practices? Are some commercial incentives and business models more likely to protect consumers than others? On which checks, if any, do companies rely to ensure that they do not cause harm to consumers?

CRC Response: Data security practices in any private industry are strongest when the Federal regulators provide clear and consistent guidance premised upon well-defined laws enacted by Congress. Data security for the debt collection industry is governed by several distinct Federal laws including the GLBA, Security Safeguards Rule and the Health Insurance Portability and Accountability Act. In addition, numerous States have enacted data privacy laws that impact the debt collection industry including California and Massachusetts. We recommend that the FTC focus on issuing clear guidance for businesses regarding data that is not presently subject to regulation.

Q-# 30. Should the Commission pursue a Section 18 rulemaking on commercial surveillance and data security? To what extent are existing legal authorities and extralegal measures, including self-regulation, sufficient? To what extent, if at all, are self-regulatory principles effective

CRC Response: The Commission should not pursue a Section 18 rulemaking on commercial surveillance and data security to the extent such rule will apply to participants in the financial services marketplace, which is already heavily regulated to adequately protect consumer privacy.

Q-# 36. To what extent, if at all, should the Commission require firms to certify that their data practices meet clear security standards? If so, who should set those standards, the FTC or a third-party entity?

CRC Response: Any standards established by proposed regulations must be clear, concise, and commensurate to the size and complexity of the entities expected to meet those standards. The applicability of new proposed standards should also consider the size and nature of the data being gathered, stored, and used by regulated entities as well as the number of consumers which may be at risk of harm resulting from the data security practices of regulated entities. New standards should not be "one size fits all" obligations, but instead consider the size and complexity of regulated entities.