FIRST SECURITY
809 Clark Street
P.O. Box 577
Charles City, IA 50616
1stsecuritybank.com

November 6, 2023
By electronic delivery to: CFPB_consumerreporting_rulemaking@cfpb.gov

Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: CFPB's Outline of Proposals and Alternatives Under Consideration, Small Business Advisory Review Panel for Consumer Reporting Rulemaking

Dear Sir or Madam:

First Security Bank and Trust[1] (First Security) appreciates the opportunity to participate in the Small Business Advisory Review Panel (SBREFA) comment on the Consumer Financial Protection Bureau's (CFPB) outline of proposals and alternatives under consideration regarding the Consumer Reporting Rule (outline).

First Security supports the need to update the Fair Credit Reporting Act (FCRA)[2], recognizing that the credit reporting industry is a major source of complaints to the CFPB. We also agree that technology advancements and the growth of consumer data collection necessitates the need for increased consumer protection and industry oversight. There are already extensive regulatory requirements governing how financial institutions use and protect consumer data. There are also regulations that require financial institutions to obtain consumer data from outside sources who may now fall under the scope of an updated FCRA. We encourage the CFPB to consider how changes made with the goal of regulating businesses that collect, evaluate, and sell consumer data can adversely impact financial institutions, inadvertently creating additional compliance burden.

Proposals and Alternatives Under Consideration

The CFPB seeks to understand how the proposal could affect the costs of compliance, additional burdens that might arise, or changes that may be required because of this update. Some of the proposed changes lack clear definitions and are vague so it is challenging to make accurate estimations. For instance, if the definition of a data broker is overly broad, some vendors we currently engage with might fall under this definition. This could potentially result in increased expenses associated with using the vendor, prompting vendors to exit the industry due to compliance costs. Vendors who do adjust to

[1] First Security Bank and Trust is an FDIC regulated community bank headquartered in Charles City, IA. With 10 locations across North Central Iowa, First Security had assets of $576,349 as of 6/30/2023.
[2] 12 CFR Part 1022

evolving compliances standards may need to invest in extra resources to meet new requirements which can squeeze their profit margins. To sustain profitability and competitiveness, they may raise prices, and these heightened costs will eventually be transferred to financial institutions. Consequently, financial institutions will have to absorb these extra expenses from vendors as well as covering their own costs of adapting to any changes because of new regulatory requirements. Ultimately, this may necessitate passing a portion of these expenses on to customers.

As a user of data that could potentially fall into the category of a consumer report, there is uncertainty about the additional compliance obligations that may emerge. This could encompass new disclosure requirements. Written permission for permissible purpose might become necessary as current permissible options under FCRA do not align with current banking operations.

New situations that necessitate adverse action, beyond the scope of how the FCRA is currently applied, may arise. Financial institutions could find themselves designated as data furnishers, introducing the potential for new dispute resolution procedures that could impact various functions within the bank.

Community banks like ours already face disproportionate compliance costs compared to larger banks and credit unions due to limited resources. Our staffing capacity is constrained, and acquiring technology to facilitate regulatory compliance is not always feasible. Consequently, many of the processes in place for regulatory compliance at community banks are manual. Introducing additional regulatory requirements may, at the very least, necessitate redistributing the already heavy workloads among limited staff. It will likely lead to the need to hire additional staff–a challenging prospect in rural locations like ours.

We ask that the CFPB consider furnishing a comprehensive Advanced Notice of Proposed Rule Making, incorporating specific definitions, detailed proposals, and potential questions. This would enable industry players to offer more informed insights into the impact on their sectors, suggest alternative solutions, and thoroughly assess the associated costs and operational implications.

Disputes

The CFPB is considering proposals related to two types of disputes: (1) those that are classified by a consumer reporting agency or furnisher as involving legal matters and (2) those involving systemic issues at a reporting agency or furnisher.

The CFPB is seeking to codify its previous interpretation that the FCRA does not distinguish between legal and factual disputes and that "legal disputes" are not exempt from FCRA's requirement regarding the investigation of disputes. First Security believes Congress's original intent with the Fair Credit Reporting Act was to ensure factual accuracy. As the CFPB states in the introduction of the outline, "Congress created accuracy requirements and gave consumers a right to see their data, and due process rights to dispute inaccurate or incomplete information in their files."[3]

---

[3] 15U.S.C.1681e(b) (accuracy procedures), 1681g (disclosures to consumers), 1681i (procedures in case of disputed accuracy)

Exempting instances of identity theft or fraudulently opened accounts, we believe a legal dispute is a dispute to the validity of the debt on the consumer's report and thus the validity of the consumer owing the debt to the institution. These should be resolved by the courts not via a dispute under the FCRA. Financial institution employees who process disputes are not attorneys. They don't have the educational background to determine the validity of a contractual obligation from a legality standpoint.

Moreover, community financial institutions lack in-house legal staff for such reviews and lack the resources to engage an attorney each time a legal dispute arises. Unlike larger financial institutions, which have dedicated staff attorneys to navigate the daily complexities of their operations, smaller institutions like ours only reach out to local attorneys for occasional legal inquires or litigation needs. Opting for ad-hoc legal services incurs hourly charges, making it more financially burdensome than maintaining a dedicated legal team. Given that these disputes often required specialized legal advice, community banks will find themselves at a disadvantage compared to larger counterparts who can readily assign these matters to their in-house legal team. The proposed change would disproportionately affect small financial institutions.

Requiring a furnisher to determine the legality of a contract may lead to unintended repercussions. Initially, challenges concerning the contract's validity will necessitate legal examination, which becomes increasingly expensive over time. Instead of resorting to legal counsel, a financial institution might opt to remove the trade from the credit report, citing a lack of resources for a thorough investigation. However, this action could result in potential legal claims from borrowers questioning the contract's legality due to the institution's inability to substantiate the validity of the debt when the dispute was filed. Even without the risk of potential legal claims, institutions who choose to automatically remove a trade because of lack of resources to investigate the dispute will give rise to legal disputes automatically being submitted by consumers.

The CFPB is considering proposals concerning disputes that relate to systemic issues. First Security examines each dispute to assess its validity and ascertain whether a correction is warranted. In instances where a reporting error is identified, the investigation also delves into the reason why the inaccuracy occurred. Given our thorough investigative approach, we do not see the need to institute a new requirement and procedure specifically for addressing systemic issues. Requiring identification of system issues might necessitate manual tracking of disputes. This manual tracking, following trend analysis, would be the only means to document and demonstrate that identical disputes were not received and that system issues were not present.

We believe that systemic issues, if they do occur, are rare. Because there is a low or no risk of occurrence, it would not justify the need for an overly burdensome process of manual tracking and trend analysis. We suggest instead that regulators examine an institution's dispute process to ensure that institutions are determining the root cause of the error when an error is identified. A thorough investigation and root cause analysis will identify systemic errors without the necessity of additional processes or forms.

The CFPB also questions if a systemic issue is identified affecting multiple customers, should those customers be notified even if they did not identify a problem themselves on their credit report and

submit a dispute. We believe that sending notifications to customers who did not otherwise report a dispute would only create confusion for those customers and is not necessary.

First Security acknowledges that a substantial number of complaints received by the CFPB annually are linked to credit reporting errors. We believe that institutions and credit reporting agencies have made progress in enhancing the accuracy of their reporting and are committed to promptly resolving disputes. It is common for financial institutions to encounter a customer dissatisfied with dispute outcomes, particularly when there are derogatory marks on their credit. However, this doesn't necessarily indicate an ineffectiveness in the dispute process or inaccuracies in reported information. We believe that consumer education could be beneficial in acknowledging that borrower circumstances may lead to derogatory credit reporting. By informing consumers about ways to improve their credit in such situations, it may contribute to a reduction in complaints related to the dispute process.

We believe that the ongoing reporting of credit tradelines to credit reporting agencies is crucial for fostering a positive credit culture, benefiting both consumers and institutions. It is important to note that reporting by institutions is a voluntary practice. There is a concern that certain institutions, particularly smaller community banks, might eventually reach a point where they deem the cost of compliance to outweigh the benefits of reporting to credit reporting agencies and decide to discontinue the practice.

Definition of Consumer Report and Consumer Reporting Agency

The CFPB is considering proposals to address the application of the FCRA to data brokers. The proposal would stipulate that "credit header" data containing certain consumer-identifying information would now be considered a consumer report. Consumer information provided to a user who uses it for a permissible purpose is also a "consumer report" and data brokers who sell certain types of consumer data such as data typically used for credit and employment eligibility determinations are selling consumer reports. A data broker that collects consumer information for a permissible purpose may not sell it for a non-permissible purpose and a data broker may not sell such information to a user unless the user has a permissible purpose. Further, a data broker "assembling or evaluating" and selling such data would be a consumer reporting agency because it would be assembling or evaluating information on consumers for the purpose of furnishing consumer reports to third parties.

The CFPB points out that "currently, some data brokers that collect, aggregate, sell, resell, license, or otherwise share personal information about consumers with other party's act as consumer reporting agencies under the statute, but others that engage in very similar activities or sell the same types of data do not. By engaging in these activities outside of FCRA's protections regarding, for example, data confidentiality and accuracy, these companies threaten consumer privacy and arguably evade the FCRA's purposes and objectives."[4] The CFPB appears to be concerned that these data brokers either fall outside the scope of existing regulations or they assert that they are not subject to current rules. First Security acknowledges the importance of subjecting companies of this nature to privacy regulations like those imposed on financial institutions.

---

[4] Small Business Advisory Review Panel for Consumer Reporting Rulemaking Outline of Proposals and Alternatives Under Consideration page 8.

It's crucial to recognize that financial institutions are already extensively regulated and adhere to privacy laws, including the FCRA, Regulation P[5], and the Gramm-Leach-Bliley Act[6]. A blanket application of the Consumer Reporting Agency definition to data brokers could have unintended repercussions for financial institutions, and by extension, consumers. We urge careful consideration of the approach to this definition. We ask the CFPB to contemplate providing exemptions to financial institutions subject to examination by prudential regulators from the definition of user or furnisher in specific scenarios. This exemption would apply when financial institutions need to utilize consumer reports to fulfill regulatory obligations outside how the FCRA is traditionally applied, engage in lawful banking activities, and address industry-specific requirements.

Financial institutions require consumer information from numerous vendors for many purposes that may not presently align with the definition of permissible purpose. Moreover, these institutions share information with partners for authorized purposes. First Security uses consumer-identifying information to benefit our customers through activities like fraud prevention and identity theft mitigation. Additionally, reports are procured for the purposes of compliance with the Bank Security Act (BSA), identity verification on existing accounts, and analysis aimed at detecting potential suspicious activities. It is important that data use requirements under the FCRA do not conflict with how financial institutions must comply with customer identification and suspicious activity monitoring requirements.

Apart from the various reports acquired to fulfill the requirements under BSA, we obtain consumer reports for additional reasons that may not meet the definition of permissible purposes under the FCRA. For instance, when utilizing electronic signatures, we employ knowledge-based authentication using a vendor. This involves posing questions sourced from various databases, and the customer must provide correct answers before accessing the document for signature. A similar technology, facilitated by a different vendor, is used for remote notarization. In the case of verifying updated property values on existing loans, a vendor employs public and customer information to generate Automated Valuation Models (AVM). Some financial institutions utilize vendors for skip tracking when attempting to locate customers during debt collection. In all these scenarios, the current definition of permissible purpose does not apply.

The definition of permissible purpose[7] is narrowly confined to specific situations including governmental reasons, court orders, employment, credit, insurance, and consumer-provided written instructions. Initially, when the FCRA outlined permissible purpose, it did not consider the utilization of consumer identifying information within the internal operations of a financial institution beyond the matters related to creditworthiness. The initial framework did not consider the incorporation of consumer reports as part of the operational functions of financial institutions that must offer changing products and services that adapt to consumer needs amid an evolving regulatory landscape. The present diversity of institutions and the range of products and services they provide results in distinct operational functions that align with the size and complexity of each financial institution. This has led to varied uses of consumer reports across the industry.

---

[5] 12 C.F.R. Part 1016 Privacy of Consumer Financial Information (Regulation P)
[6] 15 U.S.C. 6801 Protection of nonpublic personal information
[7] 15 U.S.C 1681b Permissible purposes of consumer reports

At present, aside from the credit function, the sole permissible purpose for obtaining a consumer report as part of an operation function is securing written consent. Yet acquiring written consent for every operation-specific need is impractical for a financial institution aiming to operate safely, soundly, and with a consumer-centric approach. To facilitate financial institutions' access to essential information without imposing excessive compliance burdens or costs, there is a need to expand the definition or introduce exemptions specifically tailored to operational needs.

Permissible Purposes

The CFPB is considering proposals to address what is needed for a consumer report to be furnished in accordance with a consumer's written instructions under FCRA. Under consideration would be steps companies must take to obtain written instructions, who may collect it, limits on the scope of authorization, and methods for revoking any ongoing authorizations. First Security appreciates and welcomes any guidance that would be provided.

First Security relies on written authorizations in commercial lending in the process of completing customer reviews. These reviews are not completed at the same time a loan is originated. The authorization signed by the customer authorizes First Security to obtain a credit report for business purposes through a consumer reporting agency. This authorization is only used one time. If a future credit report is needed, another written authorization is obtained.

Medical Debt Collection Information

The CFPB is considering proposals to (1) revise Regulation V to modify the exemption such that creditors are prohibited from obtaining or using medical debt collection information to make determinations about consumers' credit eligibility and (2) prohibit consumer reporting agencies from including medical debt collection tradelines on consumer reports furnished to creditors for purposes of making credit eligibility determinations.

It is important that the CFPB precisely articulates the definition of medical debt. Some creditors offer loans and credit cards specifically designed to pay for medical procedures. Additionally, consumers obtain consumer and real estate loans to pay existing medical debt. Personal credit cards may also be used for this purpose. We believe that none of these debt categories should fall under the classification of medical debt. Our proposed definition of medical debt is limited to a collection arising from an unpaid medical bill from a medical establishment or procedure, excluding any loans or credit cards established through a contractual agreement with periodic payments to pay any type of medical debt over time.

Recently there have been positive changes to how medical collections affect consumer credit. In July 2022, major credit reporting agencies removed paid medical debt from credit reports and no longer report unpaid medical collections until those debts are one year old. As of April 2023, medical collections under $500.00 no longer appear on credit reports.[8] This has resulted in a dramatic decline in

[8] ACA International "First Wave of Medical Debt Credit Reporting Changes Starts July 1", June 23, 2022 First Wave of Medical Debt Credit Reporting Changes Starts July 1 - ACA International

medical debt on consumer credit reports which has increased credit scores. [9] The credit reporting agency's actions have benefited consumers by preventing the negative impact of paid medical collections and minor unpaid medical collections on credit scores.

First Security holds the view that addressing the challenge of medical debt is a broader and more intricate issue beyond the scope of the CFPB's authority to resolve. Mitigating the impact of medical debt on the lives on Americans requires a comprehensive approach, best achieved through congressional action by enacting legislation to reform the medical industry.

Financial institutions approach medical collections and payment agreements between consumers and medical establishments differently. First Security does not consider medical collections that are reported on credit reports unless we are aware that the consumer has made payment arrangements to make periodic payments to a collection agency or medical establishment. If payment arrangements have been made, we will include those payments in their debt-to-income ratio.

Requiring financial institution to entirely overlook a specific category of debt and any associated periodic payments contradicts a key aspect of the Dodd-Frank Wall Street Reform and Consumer Protect Act[10] (Dodd-Frank Act), designed to encourage responsible lending. The inability of financial institutions to factor in payments related to medical debt would result in an inadequate assessment of a consumer's debt-to-income ratio. This oversight could potentially contribute to a borrower facing challenges in meeting their future mortgage payments.

First Security believes that financial institutions should have the flexibility to determine how they treat medical debt. Outstanding debt is one gauge of a borrower's overall credit risk. Significant medical debt increases a borrower's risk and impacts their ability to repay debt. These consumers are at an increased risk for legal actions such as garnishment judgements and bankruptcy. If financial institutions are not aware this debt exists or they can't inquire about it, there is an increased risk for credit loss. Financial institutions need to have the ability to develop credit policies that align with their risk appetite while accounting for market conditions and the economic landscape. Restricting the ability to consider certain debts could put financial institutions at a disadvantage when attempting to manage their risks affectively.

Each financial institution's approach to underwriting, in compliance with regulations and safe and sound business practices, is distinct. It falls beyond the scope of the CFPB's authority to prescribe how financial institutions should assess any type of debt that consumers are legally obligated to pay.

Implementation Period

The CFPB is seeking input on the appropriate timeline for compliance with the final rule. We anticipate the most challenging aspect of compliance will be the determination of data brokers as consumer reporting agencies. As previously mentioned, this is poised to impact the vendors utilized by financial

---

[9] Urban Institute "Medical Debit Was Erased from Credit Records for Most Consumers, Potentially Improving Many Americans' Lives, November 2, 2023 Medical Debt Was Erased from Credit Records for Most Consumers, Potentially Improving Many Americans' Lives | Urban Institute

[10] 12 U.S.C. Chapter 53 Wall Street Reform and Consumer Protection

institutions, alter how consumer data is employed, and impact various processes within our current operations. These potential changes extend beyond our existing application of the Fair Credit Reporting Act in lending and account opening; they would permeate every operational facet of the bank.
We urge the CFPB to consider the recent regulatory rules that the financial industry is currently working to implement. Over the next 24-36 months, banks will be actively engaged in implementing policies and procedures for the Small Business Collection Rule (1071).[11] Simultaneously, efforts will be underway to incorporate changes to the Community Reinvestment Act (CRA)[12]. The CFPB's proposed rule on Personal Financial Data Rights[13], set to implement Section 1033 of the Dodd-Frank Act, introduces another layer of complexity, with the final rule expected in 2024.

Our compliance department is currently running at maximum capacity to oversee our Compliance Management System. At present, there are no plans to increase staffing to accommodate the implement of 1071 or the changes to CRA. Over the next two to three years, our priority will shift to concentrate on 1071 and the CRA implementation as an Intermediate-Small Bank. To manage this, we'll enlist support from staff in other departments to aid in the implementation process and to meet the ongoing reporting demands of 1071. The upcoming two to three years will be completely dedicated to diligently addressing these two regulations while ensuring the continued compliance of consumer protection laws by our financial institution.

Given this landscape, we advocate for an extended implementation period that aligns with the complexity of this final rule. We believe a minimum of three years is essential, as we anticipate that addressing changes to the Fair Credit Reporting Act will only be completed after we implement the aforementioned regulations.

Interaction With Personal Financial Data Rights Implementing Section 1033
While not explicitly addressed in the outline, it's crucial for the CFPB to consider the intersection between the proposed section 1033 rule and updates to the FCRA. According to the proposal, financial institutions would be required to furnish comprehensive consumer and account information to a third party upon the consumer's directive. The recipient of this data could potentially be deemed a consumer reporting agency, thereby classifying financial institutions as furnishers. The imposition under section 1033 introduces an additional layer of compliance obligations under the FCRA.

Conclusion
First Security Bank and Trust expresses gratitude to the CFPB for providing us with the opportunity to share our thoughts and concerns regarding the Consumer Reporting Rulemaking process. Of the proposed changes, we believe that the application of the FCRA's definition of consumer reports to data brokers will have the most impact on financial institutions. We recognize that third parties access consumer data for profit without the consumers' knowledge and with no oversight or regulation. We support the notion that consumers have a right to know who is using their data and how it is being utilized.

---

[11] 12 C.F.R. Part 1002 Equal Credit Opportunity Act (Regulation B)
[12] 12 C.F.R. 345 Community Reinvestment
[13] Required Rulemaking on Personal Financial Data Rights issued October 19, 2023

Consumers trust financial institutions because they understand we adhere to privacy laws and safeguard their information. They are aware that we do not access their private information without permission and that financial institutions must comply with regulations. While we advocate for holding data brokers to the same standards that financial institutions are already held to, we want to ensure that the pursuit does not inadvertently result in unforeseen consequences for financial institutions already using consumer information legitimately in the course of their business operations.

Evelyn Schroeder

Sincerely,
Evelyn Schroeder
Vice President, Compliance Manager

November 6th, 2023

Giovanni Sollazzo
Founder & Chairman
AIDEM US, Inc.
228 Park Ave South, PMB 52487
New York, NY 10003 US

Attention: Consumer Financial Protection Bureau (CFPB) SBREFA Panel

I am writing on behalf of AIDEM US, Inc. to offer our insights and recommendations regarding the CFPB's proposed rulemaking under the Fair Credit Reporting Act (FCRA). We would like to express our gratitude for the opportunity to participate in the Small Business Review Panel, as it allows us to contribute to the development of regulations that can significantly impact small businesses' operations.

AIDEM offers a self-service, cloud-based, ad-buying supply chain platform that empowers our clients to plan, manage, optimize, and measure digital advertising campaigns. We believe that the proposed rulemaking should also consider the evolving nature of data transactions, especially within the digital advertising ecosystem. The intersection of digital advertising and data brokerage presents unique challenges and opportunities that warrant careful consideration.

We believe that several trends in the advertising industry will result in Programmatic Advertising (the buying and selling of advertising inventory using algorithmic software that automates the process) being the predominant means by which companies reach consumers. A fundamental component utilized by these algorithms is personal data encompassing details such as consumer's name, payment history, income, address, email, and phone number, therefore we believe that the forthcoming rulemaking proposed by the CFPB warrants consideration of its implications on the domain of digital advertising.

Programmatic Advertising is built on top of Real-Time Bidding (RTB) a complex, automated, and instantaneous auction process where ads are bought and sold individually, leveraging data from multiple sources. The supply chain includes buyers (advertisers, and agencies), sellers (publishers), and Technological Enablers (Demand Side Platforms (DSPs), Supply Side Platforms (SSPs), Data Management Platforms (DPMs), and data providers). Information used in RTB comes from cookies, device IDs, browsing history, demographics, personal data, and other behavioral data: the supply chain collects and sell this information to target ads.

There are four key categories of Technological Enablers in RTB: *[Q14]*

Demand Side Platforms (DSPs): enable advertisers to purchase and manage digital advertising space across various websites and platforms. Empower advertisers to target their desired audience and optimize their ad campaigns.

Supply Side Platforms (SSPs): enable publishers to streamline the sale of advertising space on their websites. Help publishers maximize revenue by making their ad inventory available to advertisers and facilitating the pricing and delivery of ads.

Data Management Platforms (DMPs): enable advertisers and publishers to gathers, organizes, and analyzes data related to online user behavior. Assist advertisers and publishers by providing insights into their audience's.

Data Providers: collect and sell consumer data, such as demographic information, user behavior, financials, and interests, often without consumers' direct knowledge or consent. Assists the RTB supply chain in providing consumers' data on advertising spaces.

Under CFPB's rulemaking proposal, all four categories of Technological Enabler would fall within the definition of Consumer Reporting Agencies (CRAs), due to their "assembling or evaluating" of consumer's personal data protected under FCRA. At present, they are not classified as CRAs. *[Q8]*

Technological Enablers interpret and modify the gathered data to infer and build consumer profiles, which are subsequently resold throughout the RTB supply chain to enhance the perceived value of individual advertising placements. These profiles are constructed based on data points gathered and processed through the supply chain. However, these profiles are vulnerable to errors stemming from data degradation, which occurs when the quality of data deteriorates over time or through transmission. This degradation can lead to inaccuracies in the profiles, such as outdated or incorrect information.

While certain cybersecurity controls are implemented by vendors on the RTB supply chain to safeguard data, it is crucial to recognize that these measures do not entirely preclude the risk of data breaches. Furthermore, even in cases where data is securely handled, there remains the potential for consumer harm arising from inaccuracies in the data or from the inferences drawn from such data when employed in decision-making contexts. Furthermore, it is possible for data that is ostensibly secure to be utilized for discriminatory purposes, underscoring the multifaceted nature of the risks involved. *[Q15]*

On credit header data, the RTB supply chain has automated its usage for targeted advertising, with businesses typically not storing this data directly and, instead, relying on Technological Enablers. These enablers may not categorize these transactions as involving credit header data, even though the data used is often identical to traditional credit headers. *[Q16]* To align with the CFPB's proposed rulemaking, these Technological Enablers may incur one-time costs associated with compliance upgrades and system modifications. However, past adaptations to regulations, such as the Telephone Consumer Protection Act (TCPA) and the Do Not Call registry, indicate that achieving compliance can be accomplished with minimal disruption to business operations and with limited impact on profitability. *[Q17]*

The transaction of credit header data in the RTB supply chain appears incongruent with FCRA Section 607(a) due to (i) the absence of procedures to restrict the purposes of consumer reports and the absence of vetting requirements for data sharing, and (ii) the dynamic and open nature of the RTB ecosystem posing challenges in enumerating all Technological Enablers receiving credit header data. *[Q18]*

i. There are currently no established procedures in place to confine the purposes for which consumer reports are utilized. This is partly because the participants in the RTB supply chain do not classify the data they exchange as consumer reports; thus, circumventing the stipulations of Section 607(a). Moreover, there is a notable lack of vetting requirements governing data sharing with vendors and partners, enhancing compliance challenges.
ii. The open and evolving nature of the RTB ecosystem makes it practically impossible to enumerate all the Technological Enablers that may come into contact with credit header data. This intricate and dynamic landscape complicates efforts to verify the identity and intentions of prospective users, as stipulated by Section 607(a). Consequently, the transaction of credit header data within the RTB supply chain faces compliance hurdles under the current framework.

On the furnishing of consumer reports for marketing and advertising, concerns arise regarding compliance with FCRA, as the RTB supply chain extensively uses and shares consumer data for marketing - often without adequate safeguards or transparency. While aggregated data products may escape being categorized as consumer reports, there is a potential for misuse - underscoring the need for clarity on purpose limitations and privacy implications.

In the realm of marketing and advertising services, there are multiple concerns related to FCRA compliance:

i. Technological Enablers perform a wide range of tasks (including identification of target audiences and delivery of advertising materials to consumers) without adherence to FCRA. While established CRAs possess the infrastructure to ensure compliance, ancillary service companies appear to prioritize profitability over legal adherence. *[Q19]*

ii. Technological Enablers lack comprehensive understanding of the FCRA and do not have sufficient safeguards in place to prevent the misuse of consumer report information within the RTB supply chain. Revisions to vendor contracts may be necessary to enforce purpose limitations. Furthermore, identity solutions providers may repurpose data originally intended for security services for targeted advertising, often without the direct knowledge and consent of consumers. *[Q20]*

iii. Aggregated data products, frequently sourced from open web scraping and third-party contributors, are subjected to processes of inferencing and categorization with the intent of facilitating targeted advertising. Such practices may potentially lead to a deterioration in the quality of the data and do not invariably guarantee improved accuracy in targeting. Consequently, this raises pertinent questions regarding the effectiveness and ethical considerations associated with the application of targeted advertising and predictive analytics. *[Q21]*

iv. Technological Enablers refrain from categorizing aggregated data products as consumer reports - a practice that could, potentially, place an emphasis on profitability over adherence to the FCRA and the safeguarding of consumer interests. The CFPB's rulemaking proposal should enforce all entities within the RTB supply chain to collectively uphold their respective responsibilities. That is, ensure that the utilization of data aligns with its intended purpose; thereby ensuring consumer protection and compliance with regulatory standards. *[Q22]*

v. As data aggregation continues apace, the issue of consumer privacy becomes increasingly complex. The RTB supply chain enables the linking of aggregated information back to specific consumers: Technological Enablers allow advertisers to target groups of consumers based on aggregate criteria such as household income, gather personal data from consumers on advertisers' websites and, subsequently, utilize the re-associated and de-aggregated data for measurement purposes or to deliver additional targeted advertising. *[Q23]*

The reliance on consumer authorizations or certifications of written instruction, to obtain consumer reports, especially in the context of marketing, appears to be uncertain. We recommend that existing systems, such as Data Subject Access Request (DSAR), should be expanded to facilitate the revocation of data processing authorizations. Anticipated global privacy controls and state-specific regulations (for example, the California Delete Act), emphasize the need for a streamlined process for data deletion upon consumer request, aligning with developments in the European Union and California. *[Q24]*

We believe that an inclusive and cooperative approach is crucial in achieving the desired objectives of this rulemaking, and we look forward to collaborating with the CFPB and fellow panel participants in the development of effective regulations under the FCRA.

Thank you once again for the opportunity to participate in this Small Business Review Panel.

Giovanni Sollazzo
Founder & Chairman
AIDEM US, Inc.