

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 gather, organize, and analyze 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.