RECEIVABLES MGMT. ASSOC. INTL.
SETTING THE GLOBAL STANDARD

1050 Fulton Avenue #120
Sacramento, California 95825
916.482.2462

January 25, 2023

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

Sent via email: Financial_Data_Rights_SBREFA@cfpb.gov

Re: SBREFA Outline – Section 1033 Personal Financial Data Rights

Dear Consumer Financial Protection Bureau:

The Receivables Management Association International ("RMAI") appreciates this opportunity to submit the following comments in response to the Bureau's Section 1033 SBREFA[1] Outline of Proposals and Alternatives Under Consideration.

RMAI supports the Bureau's efforts to develop clear and concise rules concerning the Bureau's expectations on how businesses should respond to consumer requests regarding financial records. RMAI believes that the rulemaking has the potential to benefit consumers, industry, and the regulatory community by providing clarity and standardization.

I. BACKGROUND

RMAI is the nonprofit trade association that represents more than 600 companies that purchase or support the purchase of performing and non-performing receivables on the secondary market. The existence of the secondary market is critical to the functioning of the primary market in which credit originators extend credit to consumers. An efficient secondary market lowers the cost of credit extended to consumers and increases the availability and diversity of such credit.

RMAI is an international leader in promoting strong and ethical business practices within the receivables management industry. RMAI requires all its member companies who are purchasing receivables on the secondary market to become certified through RMAI's Receivables Management Certification Program ("RMCP")[2] as a requisite for membership. The RMCP is a comprehensive and uniform source of industry standards that has been recognized by the collection industry's federal regulator, the Bureau of Consumer Financial Protection , as "best practices."[3]

RMAI supports the adoption of reasonable measures designed to protect consumer privacy. With respect to data security, RMCP certified companies are required to establish and maintain a reasonable and appropriate data security policy that includes, at a minimum, measures to ensure:

---

[1] Small Business Regulatory Enforcement Fairness Act of 1996.
[2] RMAI, *RMAI Receivables Management Certification Program*, https://rmaintl.org/certification/.
[3] Consumer Financial Protection Bureau, *Small Business Review Panel for Debt Collector and Debt Buyer Rulemaking, Outline of Proposals Under Consideration*, July 28, 2016, p. 38, http://files.consumerfinance.gov/f/documents/20160727_cfpb_Outline_of_proposals.pdf.

(a) The safe and secure storage of physical and electronic Consumer Data;

(b) Computers and other electronic devices that have access to Consumer Data contain reasonable security measures such as updated antivirus software and firewalls;

(c) Receivables portfolios are not advertised or marketed in such a manner that would allow Consumer Data and Original Account Level Documentation to be available to or accessible by the public;

(d) If there is any offsite access to a Certified Company's network, the offsite access shall be through the use of a virtual private network "VPN" or other system that requires usernames and passwords, complex and non-intuitive passwords, recurring password changes, and multifactor authentication;

(e) The Certified Company can prevent connectivity with the network and/or remotely disable or wipe company-issued computers and electronic devices that contain Consumer Data when an employee or agent no longer has an employment/agency relationship with the company or if a device is lost or stolen;

(f) Consumer Data that is transferred to a third-party is transferred securely through the use of encryption or other secure transmission sources;

(g) An action plan has been developed and communicated with relevant employees on how to handle a data breach in accordance with applicable laws, which shall include any required disclosures of such breach;

(h) A disaster recovery plan has been developed and communicated with relevant employees on how to respond to emergencies (e.g., fire, natural disaster, etc.) that have the potential to impact the use and storage of data; and

(i) The secure and timely disposal of Consumer Data that complies with applicable laws and contractual requirements, provided that account records are maintained for at least three (3) years from the date of last collection activity.[4]

A majority of RMAI members are small businesses. Most of its debt buyer members have annual receipts of less than $47 million. Most of its debt collector members have annual receipts of less than $19.5 million.[5] Many vendors to debt buyers and debt collectors would also be fall within the U.S. Small Business Administration's (SBA) small business threshold.

---

[4] RMAI Certification Standard A7, v10.

[5] See U.S. Small Business Administration, *Table of Small Business Size Standards Matched to North American Industry Classification System Codes*, Effective December 19, 2022, publicly available at https://www.sba.gov/sites/default/files/2022-12/Table%20of%20Size%20Standards_Effective%20December%2019%2C%202022.xlsx and archived at https://perma.cc/ED7C-PZHQ. Debt buyers have a NAICS classification code of 522299, collection agencies 561440.

II. COMMENTS

Q2. Are there any relevant statutes or regulations with which you must comply that you are concerned may duplicate, overlap, or conflict with the CFPB's proposals under consideration beyond those described in Appendix C?

- Appendix C does not include a reference to the federal Fair Debt Collection Practices Act, 15, U.S.C § 1692g, et seq. ("FDCPA"). If the rule is expanded to include financial institutions subject to the FDCPA, consideration must be given to the potential conflicts with the Bureau's proposed § 1033 rulemaking.

  For example, the FDCPA generally prohibits covered debt collectors from sharing information with third parties "without the prior consent of the consumer given *directly* to the debt collector . . ."[6] Associated with that prohibition, entities subject to the FDCPA have developed best practices to verify the identity of the consumer with whom they are communicating prior to disclosing information regarding a debt.

  Additionally, the FDCPA, Regulation F, numerous state laws, and case law outline the information a covered debt collector must provide in response to a consumer's written request for validation. The information required in connection with a response to a consumer's request for validation under is the subject of extensive decisional law and recent rulemaking, all of which is designed to provide accuracy, and integrity in the provision of information in response to a consumer's validation request. RMAI is concerned that application of § 1033 rulemaking to debt collectors could be construed to require a debt collector to treat a request for validation as a § 1033 request and the provision of information not suitable for validation purposes.

  For these reasons, RMAI believes Congress did not intend to include debt collectors, as defined by the FDCPA, to fall within the scope of §1033 and such debt collectors should be exempt from any rules promulgated under § 1033. Alternatively, any rule promulgated under § 1033 should provide that a debt collector in compliance with 15 U.S.C. § 1692g and 12 C.F.R. § 1006.34 complies with § 1033.

Q11. Please provide input on the approach the CFPB is considering with respect to accounts held by multiple consumers. What alternative approaches should the CFPB consider?

- RMAI suggests that CFPB consider the implications of divorce, death, bankruptcy, and minors with regard to multiple consumers holding the same accounts.

Q16. Where a covered account is held by more than one consumer, should the rule allow any consumer holding the account to authorize access, or should authorization procedures include a

---

[6] 15 U.S.C. § 1692c(b) (emphasis added). See RMAI's response to Q73.

requirement that the third party provide authorization disclosures to and obtain consent from each consumer who is an accountholder?

- RMAI believes access to account information is determined by the account agreement and applicable state law. For example, N.J. Admin. Code § 3:1-12.1 and MCL § 490.51. Any rule should not be contrary to these established rights.

Q18. Should the CFPB provide model clauses and/or forms for some or all of the content of the authorization disclosure?

- RMAI supports this proposal, with a safe-harbor provision for the adoption of such clauses and/or forms.

Q20. Please provide input on the approach the CFPB is considering with respect to providing consumers a copy of the signed authorization.

- RMAI generally supports this proposal.

Q21. Please provide input on whether the full certification statement should be included in the authorization disclosure.

- RMAI agrees with this proposal and recommends a standardized form for the certification statement and authorization disclosure.

Q22. Please provide input on the approach the CFPB is considering with respect to these categories of information. What alternative approaches should the CFPB consider?

- RMAI recommends adherence to the requirements of the Gramm-Leach-Bliley Act ("GLBA")[7] and Fair Credit Reporting Act ("FCRA")[8] in this and related matters.

Q23. Is additional clarity needed with respect to the data elements the CFPB is considering proposing? What further information would be helpful? For example, should the rule set forth all the specific data elements that the rule requires covered data providers to make available?

- RMAI agrees with this proposal and suggests that specificity and uniformity with respect to the data elements will advance compliance.

Q25. Please provide input on whether the CFPB should require a covered data provider to make available to a consumer or an authorized third-party information about all of the companies, or other payees, for which the consumer has provided information to the covered data provider to make payments to the companies on the consumer's behalf, including information about the consumer's "account" or "identification" number with the companies.

---

[7] 15 U.S.C. § 6801, et seq.
[8] 15 U.S.C. § 1681 et seq.

- RMAI generally supports the Bureau's proposal.

Q26. Please provide input about the data security and privacy risks that would result from a requirement that covered data providers make available to authorized third parties the above-described information.

- RMAI generally supports the Bureau's proposal.

Q27. Please provide input on whether the above-described confirm/deny approach would be feasible to implement and could suffice to achieve the contemplated consumer benefits of authorized third-party access to consumer financial data.

- RMAI generally supports the Bureau's proposal.

Q32. How should the CFPB interpret "confidential commercial information"? What existing legal standards, if any, should inform the CFPB's considerations regarding interpreting that term in the context of Dodd-Frank Act section 1033? To what extent should a covered data provider's ownership interest in such information be a factor?

- RMAI recommends interpretation in accordance with GLBA, anti-money laundering/Office of Foreign Assets Control ("AML/OFAC") requirements and related protections.

Q33. To what extent are there data elements kept confidential from the consumers to which they pertain? To what extent are there data elements concerning the consumer financial product or service that the consumer obtained that are kept confidential from the consumers to which they pertain?

- RMAI suggests this topic pertains to AML/OFAC and related efforts

Q34. How should the CFPB interpret "for the purpose of"? What existing legal requirements, if any, should inform the CFPB's considerations regarding which information covered data providers collect for the purpose of preventing fraud or money laundering, or detecting or reporting other unlawful conduct?

- RMAI suggests the GLBA, FCRA and AML/OFAC requirements are pertinent.

Q35. How should the CFPB interpret "kept confidential"? What existing legal requirements, if any, should inform the CFPB's considerations regarding which information covered data providers should be required to keep confidential from consumers?

- RMAI suggests the AML/OFAC requirements are pertinent.

Q37. How should the CFPB interpret "ordinary course of business"?

- RMAI suggests that information can be retrieved in the "ordinary course of business" if the information was obtained and stored by a covered data provider consistent with its customary business practices and procedures. Information cannot be retrieved in the "ordinary course of business" if the resources expended by the covered data provider to provide the information to the consumer are unreasonably burdensome taking into account applicable circumstances such as the size of the covered data provider, the nature of the request, and the technical limitations.

Q38. Please provide input on the approach the CFPB is considering with respect to making current and historical information available. What alternative approaches should the CFPB consider? Please provide input on whether or how the CFPB should define "current."

- RMAI notes that the 36-month example cited comports with Regulation F, which is appropriate. As to the use of the word "current," definitions could consider "not obsolete" or "currently considered to be accurate."

Q39. Please provide input on the approach the CFPB is considering with respect to requiring covered data providers to make information available directly to consumers if they have enough information to reasonably authenticate the consumer's identity and reasonably identify the information requested. What alternative approaches should the CFPB consider?

- RMAI suggests that the ability for consumers to access and download their information via a website ("account management portal"), in popular formats is common today and is therefore a reasonable expectation.

Q40. Please provide input on the approach the CFPB is considering with respect to requiring covered data providers to make information available directly to consumers through an online financial account management portal and to give consumers the option to export the information in both human and machine-readable file formats. What alternatives should the CFPB consider?

- RMAI suggests that the ability for consumers to access and download their information via a website ("account management portal"), in popular formats is common today and is therefore a reasonable expectation, except for small businesses Our member small businesses would incur significant expense to develop the technology to allow consumer access to historical information or to outsource it to a third-party vendor, in *both* machine readable and "human" formats. Small businesses typically do not maintain interactive websites, let alone an "online financial account management portal." As of 2021, web development service providers charge an hourly rate anywhere from $70 to $150 and one source estimates the cost of developing a customer portal to be between $5,000 and $50,000.[9] Further, providing such a portal implicates added costs to maintain data security over such a portal.

---

[9] Topdevs.org, "How Much Does It Cost to Make a Web Portal in 2023?" available at https://topdevs.org/blog/web-portal-development-costs#:~:text=Thus%2C%20the%20basic%20development%20of,cost%20between%20%245%2C000%20and%20%2450%2C000 and archived at https://topdevs.org/blog/web-portal-development-

Q43. Do covered data providers currently provide consumers with the ability to export account-related information? In what format or formats are consumers able to export account-related information?

- RMAI small business members typically do not provide consumers with the ability to export account-related information, largely due to the significant costs for such portals. See response to Q40.

Q48. Please provide input on the approach the CFPB is considering with respect to whether to require covered data providers to make available information it knows is inaccurate. What alternative approaches should the CFPB consider? Are there circumstances under which the transmission of information that the covered data provider knows is inaccurate could nonetheless be beneficial to a consumer (e.g., to address disputes)?

- RMAI suggests that "belief" should be substituted for "knowledge" in this context. It is not considered ethically normative to trade on information "known" to be "inaccurate" (apart from the process of managing fraud and disputes). The Bureau may wish to consider a definition of "inaccurate" beyond the example cited, and to consider who is at fault if "inaccurate" information is in fact supplied by the consumer or a governmental agency (e.g., real estate ownership records).

Q49. Please provide input on whether covered data providers have systems in place to both identify and withhold from transmission inaccurate information. Please provide input on the costs to covered data providers if such a system would need to be developed.

- RMAI suggests that identification of inaccurate information would be difficult to assure, particularly given the sources from which inaccurate information may be obtained, including from the consumer.

Q50. Please provide input on the approach the CFPB is considering with respect to the third-party access portal proposal.

- RMAI believes that any rule requiring such a portal imposes a material, adverse impact on small businesses for the reasons outlined above. However, if such a portal is required it should include safe-harbor provisions over the structure and data security requirements associated with such a portal.

Q52. With respect to covered data providers that have not yet established a third-party access portal at the time the rule is final and effective, should the CFPB require that they make information available to authorized third parties before they establish a third-party access portal? Would such a requirement necessitate covered data providers allowing authorized third parties to engage in screen scraping? Are there alternatives to screen scraping that a covered data provider

---

costs#:~:text=Thus%2C%20the%20basic%20development%20of,cost%20between%20%245%2C000%20and%20%2450%2C000., archived at https://perma.cc/HGA7-RKTW.

could implement to make information available to authorized third parties in electronic form while establishing a third-party access portal?

- RMAI notes that "screen scraping" is nominally defined as "the action of using a computer program to copy data from a website." As such, it is a tool for data access; publicly available data (e.g., listed telephone numbers, lawsuit filings, county real estate records) should be uniformly considered as acceptable. For confidential data, the control should tie to consumer authentication and consent.

Q53. Assuming the CFPB imposes staggered deadlines with respect to a requirement to establish a third-party access portal, please provide input on how the CFPB should do so.

- RMAI believes that any rule requiring such a portal imposes a material, adverse impact on small businesses for the reasons outlined above. RMAI generally encourages conformity with GLBA, consumer consent and the comments on Q52.

Q54. Assuming the CFPB imposes staggered implementation periods with respect to establishing a third-party access portal, please provide input on the appropriate time period that each class of covered data providers should have in order to come into compliance with the third-party access portal proposal under consideration.

- RMAI believes that any rule requiring such a portal imposes a material, adverse impact on small businesses for the reasons outlined above. Also, see response to Q52.

Q57. Please provide input on whether CFPB-defined standards are needed to promote the availability of data to authorized third parties, whether certain aspects of the regulation of third-party access portals are better suited to be regulated by industry participants, and how the CFPB can promote the development of industry standards.

- RMAI believes that any rule requiring such a portal imposes a material, adverse impact on small businesses for the reasons outlined above. However, if such a portal is required it should include safe-harbor provisions over the structure and data security requirements associated with such a portal. RMAI suggests that a committee of industry participants be impaneled to address this topic, due to the breadth of scope.

Q58. How can the CFPB incentivize the establishment of industry-led mechanisms and fora through which disputes between ecosystem participants could be surfaced, adjudicated, and otherwise addressed?

- RMAI recommends that the CFPB emphasize the value of participating in the proposed mechanisms and fora, in terms of being heard and helping shape the future environment.

Q70. What methods of securely authenticating an authorized third party do not require consumers to share their credentials with the authorized third party?

- RMAI notes that secure authentication can be effected in different ways, e.g., tokenization and MFA, and recommends a safe-harbor for following agreed-upon standards.

Q72. Please provide input on what steps the CFPB should take to prevent third parties that do not satisfy the conditions described above from obtaining information. Are there other conditions beyond what is described here that a third party should need to satisfy before a covered data provider is obligated to make information available? Are there circumstances in which third parties should be permitted to access information even if they do not satisfy the conditions the CFPB is considering proposing?

- RMAI recommends that publicly available information be exempt from these conditions.

Q73. Please provide input on the approach the CFPB is considering. What alternative approaches should the CFPB consider? Should covered data providers be able to obtain evidence of authorization directly from a consumer, rather than through an authorized third party?

- Under the current proposal, RMAI recommends that in addition to providing authorization to the ATP which would then transmit the authorization to the covered data provider, the consumer also provide authorization to release the information directly to the covered data provider. There is a distinction between providing an ATP authorization to *request* information and providing a covered data provider authorization to *release* information.

  First, the covered data provider may have no relationship, contractual or otherwise, with the ATP and therefore have no ability to assess or monitor the authorized third party's information security program or its use or sharing of the consumer's information. The covered data provider's contractual relationship is solely with the consumer and the covered data provider should not be put in the tenuous position of relying only on authorization provided by a third party.

  Second, requiring direct authorization to the covered data provider to release information to will significantly reduce the risk of potentially fraudulently obtained authorizations from authorized third parties.

  Third, the Bureau indicates the rule could be expanded in the future to include other types of financial institutions beyond the current limited subset. If the rule is expanded to include financial institutions subject to the Fair Debt Collection Practices Act,[10] such institutions cannot share information with third parties "without the prior consent of the consumer given directly to the debt collector . . ."[11]

---

[10] 15 U.S.C. § 1692g, et seq.

[11] "Except as provided in section 1692b of this title, without the prior consent of the consumer given directly to the debt collector, or the express permission of a court of competent jurisdiction, or as reasonably necessary to effectuate a postjudgment judicial remedy, a debt collector may not communicate, in connection with the collection of any debt, with any person other than the consumer, his attorney, a consumer reporting agency if otherwise

Q74. Please provide input on what type of evidence of revocation of a third party's authorization a covered data provider should be required to receive before they terminate access.

- RMAI suggests the Bureau develop a standardized revocation that covered data providers may provide to consumers in either paper or electronic form. Upon receipt of the revocation form, the covered data provider would cease providing access to the consumer's information. Providing revocation to the covered data provider instead of the authorized third party ensures receipt and timely cessation of sharing. There is a distinction between revoking an authorized third party's authorization to *request* information and revoking a covered data provider's authorization to *release* information.

  RMAI recommends evidence that is electronic, encrypted and/or tokenized with a low-cost method.

Q75. To reduce the risk of potentially fraudulently obtained authorizations, should a covered data provider be required to notify a consumer of a third party's initial access attempt (such as by providing consumers a copy of the evidence of authorization submitted by a third party), or be permitted to confirm with the consumer the authorization of a particular third party before making information available?

- As noted above (Q73), requiring a consumer to provide authorization for third party access directly to the covered data provider will reduce the risk of potentially fraudulently obtained authorizations.

Q79. Please provide input on the proposal the CFPB is considering. What alternative approaches should the CFPB consider?

- The Bureau has provided significant specificity regarding the type of information that would be covered by the rule. Accordingly, RMAI believes the Bureau should develop a standardized authorization form that an authorized third party would use to select the specific covered information sought.

Q80. Please provide input on the approach the CFPB is considering with respect to authenticating the identity of the authorized third party.

- RMAI agrees with the proposal that would require an authorized third party to provide information sufficient for a covered data provider to authenticate the authorized third party's identity and legitimacy, in addition to requiring direct authorization from the consumer.

---

permitted by law, the creditor, the attorney of the creditor, or the attorney of the debt collector." 15 U.S.C. § 1692c(b).

Q81. Please provide input on whether it would facilitate compliance or reduce costs to covered data providers and authorized third parties if covered data providers were required to follow certain specific procedures in authenticating an authorized third party's identity.

- RMAI supports the concept of the Bureau developing a uniform set of information to authenticate an authorized third party's identity prior to making information available to the authorized third party.

Q82. Should covered data providers be required to make information available to third parties when they know the information requested is inaccurate?

- Under the proposal, a consumer would have the opportunity to request and review the personal information held by a covered data provider prior to authorizing an authorized third party to access that information. To the extent a consumer disputes information held by the covered data provider, RMAI believes such information should be identified as disputed prior to providing access to the authorized third party. Otherwise, covered data providers should not be required to search each consumer's information for inconsistencies prior to providing access *as requested by the consumer*.

Q85. With respect to disclosing why access is prevented, should covered data providers be required to provide disclosures to third parties, consumers, or both? Does the answer depend on the reason access is prevented?

- A covered data provider's relationship is with the consumer, and RMAI therefore suggests it would be appropriate to disclose only to the consumer the reason access by the authorized third party was prevented.

Q86. Please provide input on whether it would facilitate compliance or reduce costs to covered data providers if, rather than prescribe disclosures, they were required to implement reasonable policies and procedures with respect to explaining why information is withheld.

- With or without prescribed disclosures, a covered data provider would necessarily develop policies and procedures with respect to access refusals, so it is unlikely this proposal would significantly affect costs.

Q87. Please provide input on whether and how covered data providers should inform consumers of rights afforded to them pursuant to the rule.

- RMAI believes that informing consumers of the rights afforded them under rule can be accomplished by an including an explanation of those rights in the agreement the consumer enters into with the covered data provider.

Q88. Please provide input on the approach the CFPB is considering to limit third party collection, use, and retention of consumer-authorized information to what is reasonably necessary to provide the requested product or service.

- RMAI agrees that the collection, use, and retention of consumer-authorized information should be limited to that which is reasonably necessary to provide the requested service.

Q89. Please provide input on whether additional collection limitations are needed for potentially sensitive information that might cause particular harm to consumers if exposed (such as Social Security numbers).

- RMAI does not believe additional collection limitations are needed for potentially sensitive information because a consumer has the right to request and review the information held by the covered data provider prior to authorizing third party access and implicitly approves the sharing of that information regardless of its sensitivity when providing the third party authorization for access.

Q91. Please provide input on the approach the CFPB is considering to limit duration and frequency according to what is reasonably necessary to provide the product or service the consumer has requested.

- RMAI agrees with the proposal to limit authorized third-party access in terms of duration and frequency to that which is reasonably necessary to provide the product or service requested by the consumer.

Q92. Please provide input on the approach the CFPB is considering that would establish a maximum durational period for all use cases, along with any alternative approaches the CFPB should consider.

- RMAI believes that imposing a maximum durational period to authorized third party access is unnecessary provided such access is limited to that which is necessary to provide the product or service requested by the consumer.

Q93. If the rule were to require third parties to obtain reauthorization after a durational period has lapsed, how could the CFPB reduce negative impacts on consumers and unnecessary costs on authorized third parties?

- RMAI agrees with the proposal that a consumer's continuing use of a requested product or service creates a presumption of reauthorization. This prevents the potential for an unexpected cessation of requested products or services, provided the continuation of access remains reasonably necessary to provide the requested product or service.

Q94. Please provide input on the approach the CFPB is considering that would require authorized third parties to provide consumers with a mechanism through which they may revoke the third-party's access to their information.

- RMAI agrees that if the Bureau determines that the revocation will be provided by the consumer to the authorized third party, the authorized third party should provide a consumer with a simple way to revoke authorization consistent with the manner in which the authorization was granted.

Q95. Please provide input on whether covered data providers should also be required to provide consumers with a mechanism by which they may revoke third-party authorization, and the costs and benefits of such an approach.

- The consumer should provide revocation to the covered data provider to ensure the covered data provider's awareness and to avoid issues that could arise in the case of an unscrupulous authorized third party, or one that simply has flawed procedures for effectively acting on revocation requests.

Q96. Please provide input on whether authorized third parties should be required to report consumer revocation requests to covered data providers.

- Requiring the consumer rather than the authorized third party to report revocation to the covered data provider will prevent the potential issue described immediately above.

Q98. Please provide input on the standard the CFPB is considering for defining secondary use of consumer-authorized information.

- RMAI recommends that an authorized third party's secondary use of a consumer's information should not be limited provided such use is either explained in the authorization.

Q99. Please provide input on the various approaches the CFPB is considering to limit third parties' secondary use of consumer-authorized information and any alternative approaches the CFPB should consider.

- RMAI suggests that the third-party authorization explain to a consumer the authorized third party's anticipated secondary use of the consumer's information and provide an opt-out mechanism. However, the opt-out mechanism should not be available for an authorized third party's secondary use of the of the information if the information is necessary for the authorized third party to:
    - Comply with federal, state, or local laws or regulations;
    - Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena or summons by federal, state, local, or other governmental authorities;
    - Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;
    - Investigate, establish, exercise, prepare for, or defend legal claims;
    - Perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or enforce the consumer's contractual obligations.
    - Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual; or
    - Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity,

preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any such action.

Q100. Please provide input on whether the rule should include a prohibition on third parties' use of consumer-authorized information that is not otherwise necessary to obtain the product or service requested by the consumer.

- RMAI believes that secondary use of a consumer's information should be prohibited if such use is not necessary to provide the product or service requested by the consumer unless the information is necessary for the authorized third party to:
    - Comply with federal, state, or local laws or regulations;
    - Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena or summons by federal, state, local, or other governmental authorities;
    - Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;
    - Investigate, establish, exercise, prepare for, or defend legal claims;
    - Perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or enforce the consumer's contractual obligations.
    - Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual; or
    - Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any such action.

Q103. Please provide input on the approach the CFPB is considering that would require authorized third parties to delete consumer information that is no longer reasonably necessary for providing the consumer's requested product or service.

- RMAI agrees with the proposal requiring an authorized third party to delete consumer information that is no longer reasonably necessary for providing the consumer's requested product or service unless the information is necessary for the authorized third party to:
    - Comply with federal, state, or local laws or regulations;
    - Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena or summons by federal, state, local, or other governmental authorities;
    - Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;
    - Investigate, establish, exercise, prepare for, or defend legal claims;
    - Perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or enforce the consumer's contractual obligations.
    - Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual; or

- Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any such action.

Q104. Should an authorized third party be required to delete consumer information upon receipt of the consumer's revocation request? Under what circumstances should an authorized third party be allowed to retain consumer information beyond receipt of the consumer's revocation request?

- RMAI believes that if the Bureau requires an authorized third party to delete consumer information upon receipt of the consumer's revocation request, an exception should be made if the information is necessary for the authorized third party to:
  - Comply with federal, state, or local laws or regulations;
  - Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena or summons by federal, state, local, or other governmental authorities;
  - Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;
  - Investigate, establish, exercise, prepare for, or defend legal claims;
  - Perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or enforce the consumer's contractual obligations.
  - Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual; or
  - Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any such action.

Q105. If retention is required to comply with other laws, should authorized third parties be required to disclose to consumers that the consumer-authorized information is being retained?

- RMAI suggests that if retention is required to comply with other laws, an authorized third party should only be required to disclose that fact to consumers in the original agreement between the authorized third party and consumer.

Q106. Should an authorized third party be permitted to ask consumers for permission to retain consumer-authorized information after receipt of a revocation request, and for what reasons?

- If the authorized third party's agreement with the consumer explains that certain information will be deleted upon receipt of a revocation request, and the exceptions, the authorized third party should assume the informed consumer does not desire to be contracted regarding retention post revocation.

Q108. Should deletion of consumer-authorized information be required when authorization lapses at the end of a durational period?

- Upon the lapse of authorization, an authorized third party should delete consumer-authorized information that is no longer reasonably necessary for providing the consumer's requested product or service unless the information is necessary for the authorized third party to:
    - Comply with federal, state, or local laws or regulations;
    - Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena or summons by federal, state, local, or other governmental authorities;
    - Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;
    - Investigate, establish, exercise, prepare for, or defend legal claims;
    - Perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or enforce the consumer's contractual obligations.
    - Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual; or
    - Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any such action.

Q111. Please provide input on the approach the CFPB is considering regarding data security.

- Unlike covered data providers, not all authorized third parties will be subject to the Safeguards Rule and covered data providers will have no ability to assess or monitor an authorized third party's information security program. Therefore, rather than general information security program requirements, RMAI believes authorized third parties should be subject to requirements substantially similar to those in the Safeguards Rule. The Bureau could reduce the cost to small entities by including the same small business exceptions found in the Safeguards Rule.[12]

Q117. Please provide input on the approach the CFPB is considering with respect to periodic disclosures regarding an authorized third party's access to consumer information.

- RMAI believes that if the disclosure requirements proposed by the Bureau are provided to the consumer in the third-party authorization, periodic disclosures are unnecessary, particularly since authorized third parties are limited to the collection of information which is "reasonably necessary" and the consumer's right to revoke at any time.

Q119. Please provide input on the approach the CFPB is considering regarding a record retention requirement, along with any alternative approaches the CFPB should consider.

- The Bureau is proposing on one hand that authorized third parties "delete consumer information that is no longer reasonably necessary to provide the consumer's requested

[12] 16 CFR § 314.6.

product or service, or upon the consumer's revocation of the third-party's authorization." On the other hand, the Bureau is proposing a "record retention requirement [that] would assist with the CFPB's ability to monitor compliance . . ."

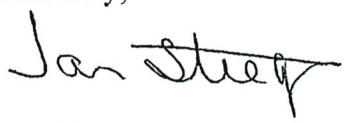
Respectfully, RMAI is opposed to a record retention requirement because requiring entities to retain consumer information longer than reasonably necessary unnecessarily puts more consumers' data at risk in the event of a cybersecurity event.

III. CONCLUSION

RMAI thanks the Bureau for its thoughtful work on the Section 1033 Rulemaking and SBREFA Outline, and for its consideration of these comments.

Please let us know if you have questions or if we can be of any assistance. I can be reached at (916) 482-2462 or jstieger@rmaintl.org.

Sincerely,



Jan Stieger
RMAI Executive Director