

December 28, 2023

FINANCIAL DATA RIGHTS  
c/o Legal Division Docket Manager  
Consumer Financial Protection Bureau  
1700 G Street NW  
Washington, DC 20552



1050 Fulton Avenue  
Suite 120  
Sacramento, CA 95825

Sent via: Federal eRulemaking Portal: <https://www.regulations.gov>

Re: Section 1033 Personal Financial Data Rights  
CFPB-2023-0052  
RIN 3170-AA78

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 Notice of Proposed Rulemaking (“NPRM”).

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 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”)<sup>1</sup> 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.”<sup>2</sup>

---

<sup>1</sup> RMAI, *RMAI Receivables Management Certification Program*, <https://rmaintl.org/certification/>.

<sup>2</sup> 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](http://files.consumerfinance.gov/f/documents/20160727_cfpb_Outline_of_proposals.pdf).

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:

- (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.<sup>3</sup>

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.<sup>4</sup> Many vendors to debt buyers and debt collectors would also fall within the U.S. Small Business Administration's (SBA) small business threshold.

---

<sup>3</sup> RMAI Certification Standard A7, v11.

<sup>4</sup> 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

## II. COMMENTS

### **General comment regarding § 1033 and the Fair Debt Collection Practices Act**

If the Bureau's definition of "covered entity" is expanded to include financial institutions subject to the federal Fair Debt Collection Practices Act, 15 U.S.C § 1692g, *et seq.* ("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..."<sup>5</sup> 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 verification. The information required in connection with a response to a consumer's request for verification is the subject of extensive decisional law and recent rulemaking developed to provide accuracy and integrity in the provision of information in response to a consumer's verification 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 verification as a § 1033 request and to provide information not suitable for verification 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 complying with 15 U.S.C. § 1692g and 12 C.F.R. § 1006.34 complies with § 1033.

### **Excluded data providers (§ 1033.111(d))**

- *The CFPB requests comment on whether there are nondepositories that do not provide an interface for their customers, and if so, whether an exemption should include them.*<sup>6</sup>
  - There are many nondepository entities that do not provide a consumer interface. For example, if the rulemaking is expanded to include financial institutions subject to the FDCPA, passive debt buyers that do not directly undertake collection activities and have no contact with consumers would have to create a consumer interface. Additionally, smaller collection agencies often do not have a consumer interface, preferring instead to

---

[https://www.sba.gov/sites/default/files/2022-12/Table%20of%20Size%20Standards\\_Effective%20December%2019%2C%202022.xlsx](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.

<sup>5</sup> 15 U.S.C. § 1692c(b) (emphasis added).

<sup>6</sup> NPRM, p. 37.

take payments by phone or check. Those that do take online payments frequently use a third-party payment processing vendor and lack any interface that allows exportation of data. Small businesses without interactive websites would incur significant expense developing portals for consumer and developer access to data in human-readable and machine-readable formats. 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.<sup>7</sup> Further, providing such a portal involves added costs to maintain data security over such a portal and increases the risk of exposure to a data breach. For these reasons, RMAI suggests there is no reason to treat nondepositories differently than depositories with regard to the §1033.111(d) exclusion.

### **Qualified industry standard (§§ 1033.131 and 1033.141)**

- *The CFPB requests comment on the adequacy of these proposed attributes for ascertaining whether an open banking standard-setting body is fair, open, and inclusive. In this regard, the CFPB emphasizes that it intends the proposed attributes to pertain only to industry standards and standard-setting bodies; the attributes would not be pertinent with respect to standards issued by governmental standard-setting bodies such as the National Institute of Standards and Technology.*<sup>8</sup>
  - Data providers, as defined in § 1033.111(c), are subject to a myriad of laws and regulations. The Bureau has stated it “intends to implement CFPB section 1033 with respect to other covered persons and consumer financial products or services through supplemental rulemaking.”<sup>9</sup> This will bring into consideration additional laws and regulations not at issue in the current rulemaking. To ensure any qualified industry standard is consistent all applicable laws and regulations, RMAI suggests that § 1033.141(a) include this additional attribute: “The decision-making body ensures that all qualified industry standards issued do not conflict with and remain consistent with the laws and regulations to which covered entities are subject.”<sup>10</sup>

### **Obligation to make covered data available (§ 1033.201)**

- *The CFPB requests comment on whether the provision regarding current data would benefit from additional examples or other clarifications.*<sup>11</sup>
  - RMAI believes the description “the most recently updated covered data that it has in its control or possession at the time of a request” is sufficient.

---

<sup>7</sup> 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.>

<sup>8</sup> NPRM, p. 49.

<sup>9</sup> NPRM, p. 33.

<sup>10</sup> Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, §5.a(iv) (2016).

<sup>11</sup> NPRM, p. 54.

### **Covered data (§ 1033.211)**

- *The CFPB requests comment on whether additional data fields should be specified to minimize disputes about whether the information would fall within the proposed covered data definition.<sup>12</sup>*
  - RMAI appreciates the goal of minimizing disputes but recommends that safe and commercially reasonable solutions be considered when contemplating additional data fields. Further, the more data that is included, the greater the harm to consumers in the event of a data breach.

### **Transaction information § 1033.211(a)**

- *The CFPB requests comment on whether the transaction information examples are sufficiently detailed and consistent with market practices.<sup>13</sup>*
  - RMAI believes the current description and example are sufficient, subject to the limitation of that which is “in the control or possession of the data provider.”
- *The CFPB also requests comment on whether to retain the safe harbor for historical transaction data and whether a different amount of historical transaction data would be more appropriate.<sup>14</sup>*
  - RMAI supports the inclusion of the safe harbor and does not object to the timeframe subject to the limitation that the information is restricted to that which is “in the control of possession of the data provider.” A data provider should not lose the safe harbor because some historical information described in the example has been deleted or deidentified pursuant to data minimization policies and procedures adopted in the ordinary course of business.

### **Account Balance § 1033.211(b)**

- *The account balance category would include available funds in an asset account and any credit card balance. The CFPB requests comment on whether this term is sufficiently defined or whether additional examples of account balance, such as the remaining credit available on a credit card, are necessary.<sup>15</sup>*
  - Account balance is commonly considered the amount owed on an account, i.e., “the difference between debit and credit sides of an account.”<sup>16</sup> If the Bureau seeks to expand its interpretation of the definition to information beyond this, for example to include “the remaining credit available on a credit card,” it should add additional subsections to § 1033.211.

---

<sup>12</sup> NPRM, p. 57.

<sup>13</sup> NPRM, p. 59.

<sup>14</sup> *Id.*

<sup>15</sup> *Id.*

<sup>16</sup> Black’s Law Dictionary (5th ed. 1983).

### **Terms and conditions § 1033.211(d)**

- *The CFPB requests comment on whether the final rule should include more examples of information that must be made available under terms and conditions.*<sup>17</sup>
  - RMAI believes the example provides sufficient guidance.

### **Basic account verification information § 1033.211(f)**

- *Given privacy and security concerns about unintentionally covering other kinds of information that are not typically shared today, the CFPB also requests comment on whether it is appropriate to limit this category to only a few specific pieces of information.*<sup>18</sup>
  - RMAI agrees that this information should be limited due to privacy and security concerns, and special consideration should be given before adding information that would commonly be considered “sensitive” in nature.

### **Exceptions (§ 1033.221)**

- *The CFPB requests comment on whether it should include additional examples of data that would or would not fall within the exceptions, and whether this provision sufficiently mitigates concerns that data providers may cite these exceptions on a pretextual basis.*<sup>19</sup>
  - RMAI believes that additional examples could be helpful.

### **Format of covered data (§ 1033.311(b))**

- *Proposed § 1033.311(b)(2) would apply only in the absence of a qualified industry standard. The CFPB requests comment on whether proposed § 1033.311(b)(2) should also be available if there is a qualified industry standard. Alternatively, the CFPB requests comment on whether it should omit proposed § 1033.311(b)(2), meaning that in the absence of a qualified standard only the general requirement under proposed § 1033.311(b) to make available covered data in a standardized format would apply.*<sup>20</sup>
  - RMAI supports the development of a qualified industry standard but believes small businesses may benefit from being able to satisfy the developer interface requirement if the interface meets a qualified industry standard *or* is in a format that is widely used by the developer interfaces of other similarly situated data providers. To encourage the use of a qualified industry standard while still allowing the option of widely used formats, RMAI recommends the Bureau provide a safe harbor for the former or, in the absence of such standard, for the latter.

---

<sup>17</sup> NPRM, pp. 61-62.

<sup>18</sup> NPRM, p. 64.

<sup>19</sup> NPRM, p. 66.

<sup>20</sup> NPRM, p. 76.

### **Security specifications (§ 1033.311(d))**

- *The CFPB declines to propose a general policies-and-procedures requirement for data security but seeks comment on such a requirement.*<sup>21</sup>
  - RMAI agrees with the proposal that an information security program must comply with the Gramm-Leach-Bliley Act and Safeguards Rule requirements.

### **Interface access (§ 1033.321)**

- *The CFPB requests comment on additional ways to harmonize the risk management obligations of data providers with CFPB section 1033's data access right for consumers and authorized third parties.*<sup>22</sup>
  - The data access rights must take into consideration data providers' obligations under federal laws, such as the Gramm-Leach-Bliley Act and Safeguards Rule, state laws such as the New York Cybersecurity Regulations, and approved industry standards.
- *The CFPB requests comment on the extent to which CFPB rule or guidance, or other sources, should address whether a data provider's denial of third party access to a developer interface under § 1033.321(a) would be reasonable with respect to any particular risk management practices.*<sup>23</sup>
  - RMAI is concerned that a third party could request information that is not relevant and reasonably necessary for the product or service sought by a consumer. Data minimization is an important risk management obligation, and the Bureau should consider how it can ensure a third party does not seek data beyond what is relevant and reasonably necessary. The inability of a third party to demonstrate data minimization should be considered a reasonable denial under § 1033.321(b).

### **Denials related to lack of information—evidence of data security practices (§ 1033.321(d)(1))**

- *The CFPB requests comment on whether to specify the types of evidence a third party would need to present about its data security practices that would give a data provider a reasonable basis to deny access under proposed § 1033.321(d)(1), and what types of evidence might provide such a basis. For example, the CFPB requests comment on whether such evidence could consist of certifications or other credentials representing compliance with data security standards, or evidence of vetting by a third party risk assessment firm.*<sup>24</sup>
  - RMAI believes certifications and credentials representing compliance with data security standards are necessary, as well as risk assessments performed by an independent third party.

---

<sup>21</sup> NPRM, p. 89.

<sup>22</sup> NPRM, pp. 94-95.

<sup>23</sup> NPRM, p. 95.

<sup>24</sup> NPRM, p. 97.

- *The CFPB requests comment on whether developing such a credential could reduce diligence costs for both data providers and third parties and increase compliance certainty for data providers with respect to the proposed rule.*<sup>25</sup>
  - RMAI believes such credentials could be helpful and that reliance on the credentials could reduce due diligence costs if data providers are afforded a safe harbor for their good faith reliance on the credentials.
- *The CFPB also requests comment on the steps necessary to develop such a credential and how the CFPB or other regulators could support such efforts.*<sup>26</sup>
  - RMAI suggests roundtables involving regulators, data security experts, industry representatives, and consumer advocates, similar to the “Life of a Debt” roundtables hosted by the Federal Trade Commission and the Bureau leading up to the Bureau’s development of Regulation F.

**Denials related to lack of information—certain information about the third party (§ 1033.321(d)(2))**

- *The CFPB seeks comment on whether it should indicate that conformance to a specific standard or a qualified industry standard would be relevant indicia for a third party’s machine-readability compliance.*<sup>27</sup>
  - RMAI supports this proposition and suggests that a data provider should have a safe harbor for its good faith reliance on a third party’s certification of conformance.
- *The CFPB seeks comment on whether it should issue regulations or guidance that would make it easier for data providers and other members of the public to identify a particular third party’s information.*<sup>28</sup>
  - RMAI believes that regulations or guidance on this issue would be helpful and reduce potential for conflicting interpretations.
- *The CFPB seeks comment on whether it should provide that a data provider is permitted to deny access if the third party does not submit to the CFPB the link to the website on which this information is disclosed.*<sup>29</sup>
  - Given the potential liabilities the Bureau’s proposal places on data providers, RMAI believes it is appropriate to provide as much assistance as possible to ensure the legitimacy of third parties.

---

<sup>25</sup> NPRM, p. 98.

<sup>26</sup> *Id.*

<sup>27</sup> NPRM, p. 100.

<sup>28</sup> *Id.*

<sup>29</sup> *Id.*



- *The CFPB also seeks comment on whether data providers should have to provide information or notice to the CFPB regarding their procedures and decisions to approve or deny third parties for access to their developer interfaces.*<sup>30</sup>
  - RMAI believes that given the records of denials required by § 1033.351(b) and the record retention requirements of § 1033.351(d), it would be an unnecessary burden on data providers to provide this “real time” reporting.

**Confirmation of third party authorization (§ 1033.331(b)(2))**

- *The CFPB seeks comment on whether the final rule should instead permit data providers to confirm this information with the consumer only where reasonably necessary.*<sup>31</sup>
  - As RMAI has previously commented, it would be preferable for the authorization to be given directly to the data provider rather than to a third party. That would give the data provider confidence as to the authenticity of the request and reduce the complexity of the current proposal. Nevertheless, under the current proposal the data provider is ultimately responsible for ensuring the sharing of data with a third party is appropriately authorized and that the information requested is relevant and reasonably necessary for the specific purpose product or service sought by a consumer. Therefore, a data provider should be given wide latitude to decide whether to seek consumer confirmation.

Additionally, a data provider should have a safe harbor for denying a third-party’s request if it is unable to receive confirmation from the consumer either because the consumer is unreachable or because of limitations imposed by law. For example, non-attorney debt settlement companies frequently send debt collectors several documents: 1) authorization given to the debt settlement company to request information regarding a consumer’s debt from the debt collector; and 2) a form signed by the consumer demanding the debt collector cease communicating with her or him directly and only communicate with the debt settlement company. The issue in this scenario is that a debt collector generally cannot communicate with a third party regarding a consumer’s debt “without the prior consent of the consumer *given directly* to the debt collector.”<sup>32</sup> Here, there was no authorization given directly to the debt collector to release information, only authorization given to the debt settlement company to make the request. Exacerbating the situation is the debt collector’s potential violation of the FDCPA if it seeks confirmation or authorization from the consumer.<sup>33</sup>

---

<sup>30</sup> *Id.*

<sup>31</sup> NPRM, p. 108.

<sup>32</sup> 15 U.S.C. § 1692c(b) (emphasis added).

<sup>33</sup> “If a consumer notifies a debt collector in writing that the consumer refuses to pay a debt or that the consumer wishes the debt collector to cease further communication with the consumer, the debt collector shall not communicate further with the consumer with respect to such debt . . .” 15 U.S.C. § 1692c(c).

### **Jointly held accounts (§ 1033.331(d))**

- *The CFPB seeks comment on whether other account holders should receive authorization disclosures or otherwise be notified, or should have an opportunity to object, when an account holder authorizes access to consumer information.*<sup>34</sup>
  - Due to the security risks inherent in the Bureau’s proposal, RMAI believes any authorization to a third party must be from all holders of a joint account unless the terms of the account or state laws provide otherwise. Also, the Bureau should consider the implications of divorce, death, bankruptcy, and minors with regard to multiple consumers holding the same account.
- *The CFPB also seeks comment on whether the rule should specifically address whether authorized users of credit cards should have similar access, even if they are not a joint holder of the credit card account.*<sup>35</sup>
  - An authorized user should not have similar access. An authorized user of a credit card has no legal responsibility with respect to the obligations incurred and has no contractual authority with the creditor to manage the account and should not have similar access. The Bureau should consider the implications of divorce, death, bankruptcy, and minors with regard to multiple consumers holding the same account.

### **Data provider revocation (§ 1033.331(e))**

- *The CFPB seeks comment on the implementation of this notification requirement, including, in cases where an authorized third party uses a data aggregator to access the authorized third party’s access, to which party or parties the data provider must provide the notice.*<sup>36</sup>
  - RMAI suggests that a data provider should have no responsibility to provide notification to any party other than that to which the authorization was provided.

### **Denials of requests for developer interface access and requests for information (§ 1033.351(b)(2) and (3))**

- *The CFPB requests comment on whether the final rule should provide examples or further clarify how data providers could reasonably design policies and procedures to account for data security or risk management concerns.*<sup>37</sup>
  - RMAI believes additional examples on this important aspect would be helpful.

---

<sup>34</sup> NPRM, p. 110.

<sup>35</sup> *Id.*

<sup>36</sup> NPRM, p. 113.

<sup>37</sup> NPRM, p. 122.

### **Policies and procedures for ensuring accuracy (§ 1033.351(c))**

- *The CFPB seeks comment on whether the final rule should include additional elements bearing on the reasonableness of a third party’s policies and procedures regarding accuracy.*<sup>38</sup>
  - Assuming the Bureau means “a *data provider’s* policies and procedures,” RMAI believes the proposed elements are sufficient.

### **Policies and procedures for record retention (§ 1033.351(d))**

- *The CFPB requests comment on proposed § 1033.351(d) regarding the length of the retention period and the date from which the retention obligation should be measured.*<sup>39</sup>
  - RMAI agrees with the length of the retention period to be measured from the time of the response.
- *The CFPB requests comment as to the types of records that should be retained to evidence compliance.*<sup>40</sup>
  - RMAI believes the four types of records described are sufficient to evidence compliance and, with the retention requirements of § 1033.351(d), eliminate the need for the real time reporting suggested by the Bureau.<sup>41</sup>

### **Third party authorization procedures (§ 1033.401)**

- *The CFPB requests comment on whether other account holders should receive authorization disclosures or otherwise be notified, or should have an opportunity to object, when an account holder authorizes a third party to access covered data from a jointly held account.*<sup>42</sup>
  - If the Bureau does not require the authorization from all account holders, the non-authorizing account holders should be notified and have an opportunity to object and prevent the authorization. The Bureau should consider the implications of divorce, death, bankruptcy, and minors with regard to multiple consumers holding the same account.
- *The CFPB requests comment on whether the authorization procedures in proposed § 1033.401 would be sufficient to ensure that a third party is acting on behalf of a consumer in obtaining access to covered data or whether the CFPB should consider alternative procedures.*<sup>43</sup>
  - The ability of a data provider to confirm the existence and scope of the third party’s authorization with the consumer, as currently provided in § 1033.331(b)(2), should be

---

<sup>38</sup> NPRM, p. 125.

<sup>39</sup> NPRM, p. 126.

<sup>40</sup> *Id.*

<sup>41</sup> “The CFPB also seeks comment on whether data providers should have to provide information or notice to the CFPB regarding their procedures and decisions to approve or deny third parties for access to their developer interfaces.” NPRM, p. 100.

<sup>42</sup> NPRM, p. 131.

<sup>43</sup> NPRM, pp. 131-132.

sufficient to ensure that a third party is acting on behalf of a consumer, though RMAI continues to maintain that the better approach is for the authorization to be provided by the consumer directly to the data provider.

- *The CFPB also requests comment on whether the authorization disclosure, including the statement that the third party will comply with certain third party obligations, is sufficient to ensure that the consumer would be able provide express informed consent for the third party to access covered data on behalf of the consumer.*<sup>44</sup>
  - As noted above, the “categories” of covered data that will be accessed can be described in broad and generic terms that may not fully apprise the consumer of the level of covered data being sought. The disclosure should, instead, recite the specific pieces of information that will be sought and provide confirmation from the authorized third party that the collection, use, and retention of those specific pieces of covered data are reasonably necessary to provide the consumer’s requested product or service.
- *The CFPB requests comment on whether the rule should include other protections or clarifications, such as express prohibitions on false or misleading representations or omissions to induce the consumer to consent to the third party’s access to covered data.*<sup>45</sup>
  - RMAI agrees that additional protections as suggested should be included to ensure each consumer’s authorization is informed and freely given. Additionally, RMAI agrees with the following recommendation submitted by the U.S. Chamber of Commerce:

Finally, the CFPB should specify in the final rule that responsibility and liability flow with the data. The CFPB should affirm through regulation that a data provider sharing data in compliance with the section 1033 rule cannot be held financially liable for a breach of a third-party provider. Addressing liability is key to data providers’ ability to appropriately manage third party risk while complying with the section 1033 rule. Including liability in the final rule would incentivize third parties to maintain security and privacy standards that meet applicable legal requirements, including the Gramm-Leach-Bliley Act regulations. Specifying that liability will flow with the data would also promote accountability and responsibility throughout the data flow. The risk management protections provided under the Proposed Rule would be significantly undermined if any entity receiving covered data lacks required safeguards to protect it.<sup>46</sup>

- *Additionally, the CFPB requests comment about whether the proposed authorization procedures described in proposed § 1033.401 should be streamlined for certain third parties.*<sup>47</sup>

---

<sup>44</sup> NPRM, p. 132.

<sup>45</sup> *Id.*

<sup>46</sup> Regulations.gov, Comment ID CFPB-2023-0052-0771 (Dec. 25, 2023); available at <https://www.regulations.gov/comment/CFPB-2023-0052-0771>.

<sup>47</sup> NPRM, p. 132.

- RMAI suggests that procedures for ensuring proper authorization and the safe and secure sharing of information should not be streamlined.
- *The CFPB also requests comment on whether there are certain circumstances involving the transmission of data to third parties for which proposed § 1033.401 would not be appropriate.*<sup>48</sup>
  - As noted above, data should not be transmitted to third parties unless all account holders have been notified and provided an opportunity to object and prevent the transfer, in the absence of contractual provisions or laws that provide otherwise. Additionally, if the Bureau moves forward with its alternative consideration to allow secondary use of data by third parties,<sup>49</sup> such use should be prohibited unless the consumer explicitly opts in.

### **Authorization disclosure content (§ 1033.411(b))**

- *The CFPB seeks comment on any obstacles to including the proposed authorization disclosure content and on whether additional content is needed to ensure consumers have enough information to provide informed consent. Specifically, the CFPB seeks comment on whether the rule should include any additional requirements to ensure: (1) the consumer can identify the third party and data aggregator, such as by requiring inclusion of legal names, trade names, or both; (2) the description of the consumer’s requested product or service is narrowly tailored and specific such that it accurately describes the particular product or service that the consumer has requested; (3) the consumer can locate the third party obligations, such as by requiring a link to the text of proposed § 1033.421; and (4) the consumer can readily understand what types of data will be accessed, such as by requiring third parties to refer to the covered data they will access using the categories in proposed § 1033.211.*<sup>50</sup>
  - As noted above, the “categories” of covered data that will be accessed can be described in broad and generic terms that may not fully apprise the consumer of the level of covered data being sought. The disclosure should, instead, recite the specific pieces of information that will be sought and provide confirmation from the authorized third party that the collection, use, and retention of those specific pieces of covered data are reasonably necessary to provide the consumer’s requested product or service.
- *The CFPB also seeks comment on alternative disclosures that would achieve the CFPB’s objective, and on whether the authorization disclosure should include additional content such as the names of other parties with whom data may be shared, the third party’s contact information, or how frequently data will be collected from the consumer’s account(s).*<sup>51</sup>
  - As noted above, the “categories” of covered data that will be accessed can be described in broad, generic terms that may not fully apprise the consumer of the level of covered data being sought. The disclosure should, instead, recite the specific pieces of information that will be sought and provide confirmation from the authorized third party that the

---

<sup>48</sup> *Id.*

<sup>49</sup> NPRM, pp. 154-156; 244-245.

<sup>50</sup> NPRM, p. 136.

<sup>51</sup> *Id.*

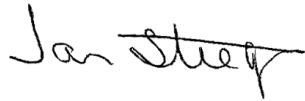
collection, use, and retention of those specific pieces of covered data are reasonably necessary to provide the consumer's requested product or service.

### III. CONCLUSION

RMAI appreciates the Bureau's thoughtful work on the Section 1033 Notice of Proposed Rulemaking, and for its consideration of these comments.

Please reach out to RMAI General Counsel David Reid at (916) 482-2462 or [dreid@rmaintl.org](mailto:dreid@rmaintl.org) if you have questions or if we can be of any assistance.

Sincerely,

A handwritten signature in black ink that reads "Jan Stieger". The signature is written in a cursive, slightly slanted style.

Jan Stieger  
RMAI Executive Director