February 4, 2021

Via E-Mail to 2020-ANPR-1033@cfpb.gov

U.S. Bureau of Consumer Financial Protection
1700 G Street, NW
Washington, DC 20552
Attn: Monica Jackson, Office of the Executive Secretary

**Re: Docket No. CFPB-2020-0034; RIN 3170-AA78**
**Bureau of Consumer Financial Protection Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records**

Dear Ms. Jackson,

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to submit this comment letter on the above-referenced advance notice of proposed rulemaking ("ANPR") issued by the Consumer Financial Protection Bureau ("CFPB").[2]

The ANPR invites comment and information to assist the CFPB in developing regulations to implement section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act"). In relevant part, section 1033 establishes, subject to rules to be prescribed by the CFPB, a consumer's right to access information in the control or possession of a "covered person,"[3] "including information relating to any transaction, series of transactions, or to the account including costs, charges and usage

---

1 SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate on legislation, regulation, and business policy affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association ("GFMA"). For more information, visit http://www.sifma.org.

2 85 Fed. Reg. 71003 (Nov. 6, 2020).

3 A "covered person" is defined in section 1002(6) of the Dodd-Frank Act, in part, as entities engaged in offering or providing consumer financial products or services. 12 USC § 5481(6).

data" and further provides that this information "shall be made available in an electronic form usable by consumers."[4]

SIFMA supports a consumer's right to access financial information in a safe and secure format and in a way that is designed to ensure responsibility and accountability for data aggregators and other parties that access such data, consistent with SIFMA's Data Aggregation Principles.[5] SIFMA also is encouraged by the CFPB's efforts to promote consumer-friendly innovation and competition in financial markets. At present, however, regulatory uncertainty over how, and under what conditions, data aggregators and data users may use, assemble, evaluate, or repackage a consumer's information once it leaves a data holder creates risk for consumers and data holders.[6] This dynamic highlights the necessity to ensure that regulatory obligations are clearly delineated for all actors in the financial data ecosystem, including data holders, data aggregators, data users, and other third parties.

As the CFPB develops regulations to implement section 1033, SIFMA recommends that the CFPB provide additional clarity concerning the application of the security and privacy provisions of the Gramm-Leach-Bliley Act ("GLBA") to data aggregators, in particular by (*i*) requiring that data aggregators comply with security standards that are no less protective than those applicable to institutions governed by the GLBA, and (*ii*) amending Regulation P to clarify that the section 1033 implementing regulations, when adopted, are the only regulations that govern a financial institution's obligations with respect to data shared pursuant to section 1033 once the financial institution has allowed access to that data in compliance with the section 1033 implementing regulations. The CFPB also should coordinate with other regulators to ensure conforming amendments to their respective GLBA implementing regulations. Such a regulatory scheme would help ensure that consumer data continues to be subject to sufficient legal protections throughout the data ecosystem, including by requiring data aggregators to implement appropriate security measures and to provide consumer disclosures concerning what the aggregator has retrieved and how it will be used or shared.

SIFMA also recommends that the CFPB coordinate with other federal financial regulators to seek consistency in regulation and guidance. In particular, SIFMA would welcome further clarity that financial institutions' arrangements with data aggregators or data users do not constitute third-party vendor relationships and, therefore, that financial institutions are not required to perform affirmative due diligence on such data aggregators. SIFMA also recommends that the CFPB coordinate with the Securities and Exchange Commission ("SEC") on issues specific to broker-dealers, investment advisers, and other SEC-regulated entities that are not subject to CFPB supervision. This includes coordinating with the SEC

---

4 Pub. L. 111-203, Title X, § 1033(a); codified at 12 USC § 5533(a).

5 *See* SIFMA Data Aggregation Principles (last accessed Jan. 18, 2021), available here.

6 The terms "authorized data," "authorized data access," "data aggregator," "data holder," and "data user" are defined in the ANPR, and should be understood to have the same meaning in this letter.

concerning the scope of data covered by 1033, including the implications of providing third-party access to brokerage and trading orders or other trading data that are regulated by the SEC.

## 1. Data Aggregators Should Be Subject to Security Requirements Commensurate with the GLBA.

SIFMA encourages the CFPB to prioritize the safeguarding of consumer financial data, regardless of how it is accessed or stored. Data aggregators generally store account log-in credentials and consumer data obtained by "scraping" consumers' online accounts at financial institutions, creating highly attractive targets for hackers and other malicious actors. Meanwhile, some aggregators do not use data security protocols or fraud monitoring systems that are commonplace for regulated financial institutions, rendering the aggregators vulnerable to cyberattacks. This vulnerability places both consumers and financial institutions at risk by exposing consumers' financial accounts and data to potential breach and theft.[7] In addition, cyberattacks may expose financial institutions to significant liability for unauthorized transactions, especially in the current fast payment environment.[8] These risks can be further exacerbated if data users or other clients of data aggregators ("fourth parties") also fail to provide sufficient protections for consumer financial data.

Moreover, unlike SIFMA's regulated members, which are subject to cybersecurity standards issued by the SEC and other federal financial regulators, most data aggregators are not subject to any comprehensive data security standards. As the Financial Industry Regulatory Authority ("FINRA") recently noted, "Many data aggregators may operate under limited regulatory oversight and are not subject to the same regulation that registered financial institutions are subject to, particularly in areas of data privacy and security."[9]

SIFMA therefore recommends that the CFPB provide greater clarity concerning the application of relevant security and privacy provisions to help ensure that data aggregators, rather than data holders, are subject to relevant legal obligations for any consumer data that the aggregator has obtained pursuant to section 1033. In particular:

- **SIFMA fully supports a consumer's right to access financial information pursuant to security standards that are no less protective than those required for consumer data held by financial institutions, accompanied by compliance programs commensurate to the data aggregators' security risks**. Such a regulatory scheme would ensure that sensitive

---

7 *See* SIFMA Response to CFPB Request for Information Regarding Consumer Access to Financial Records (Feb. 21, 2017), available here.

8 *See id*.

9 *See* Financial Industry Regulatory Authority, Investor Alert: "Know Before You Share: Be Mindful of Data Aggregation Risks" (March 29, 2018), available here.

consumer information is subject to similar protections, regardless of whether it is held by financial institutions or subsequently obtained by data aggregators or data users. Consumers also would be assured of the safe and secure treatment of their financial information. Accordingly, data aggregators that are not currently subject to the GLBA and the regulations promulgated thereunder (or equivalent regulatory standards) should be required by the CFPB's regulations to comply with such standards before accessing consumer financial data. The CFPB also should coordinate with the Federal Trade Commission ("FTC") to clarify when a data aggregator is subject to the GLBA.

- **SIFMA encourages the CFPB to clarify the interaction between section 1033 and the GLBA privacy provisions, including the CFPB's Regulation P.** Regulation P obligates "financial institutions" (as defined therein) to provide consumers with notices concerning privacy policies and practices, including with respect to the sharing of nonpublic personal information.[10] Under certain circumstances, Regulation P also requires financial institutions to provide consumers with the right to "opt out" of disclosures of their non-public personal information to non-affiliated third parties and places certain limitations on how third parties may use that data. As financial institutions often have only limited control and information concerning how consumers choose to share data with data aggregators and data users, these financial institutions should not separately be subject to the obligations and limitations under Regulation P pursuant to section 1033, including any consumer notification obligations or limitations on third-party data use. Accordingly, SIFMA urges the CFPB to amend Regulation P to clarify that the section 1033 implementing regulations, when adopted, are the only regulations that govern a financial institution's obligations with respect to data accessed pursuant to section 1033. The CFPB also should coordinate with other regulators to ensure conforming amendments to their respective GLBA implementing regulations.

## 2. The CFPB Should Consult with Other Regulators on Potentially Overlapping Legal Requirements and Obligations.

SIFMA encourages the CFPB to work with the primary financial regulators to ensure consistency in regulation and guidance. In particular, the CFPB should consult with the SEC on issues specific to broker-dealers, investment advisers, and other SEC-regulated entities that are not subject to CFPB supervision. Further, as directed by section 1033, the CFPB should consult with the federal banking agencies and the FTC. As discussed further below, the proprietary and confidential nature of certain consumer data may vary across industries, and the CFPB should coordinate with federal financial regulators to carefully define the scope of data covered by section 1033 in its rulemaking. The CFPB also

[10] 12 CFR part 1016.

should describe in detail these consultations and the input provided by the other agencies when proposing a rule, including the suggestions of other agencies and how the CFPB resolved those suggestions.

SIFMA further urges the CFPB and other federal financial regulators, including the Office of the Comptroller of the Currency, to clarify jointly that financial institutions' arrangements with data aggregators or data users do not constitute third-party vendor relationships and therefore, that financial institutions are not required to perform affirmative due diligence on such data aggregators or data users. Such clarification would eliminate any uncertainty facing data holders about their potential liability for simply allowing access to consumer data as required by section 1033. Data aggregators and data users are better positioned to ensure that their use of consumer data complies with relevant legal obligations than financial institutions, which often do not have direct contractual relationships with these third parties. Accordingly, as discussed above, consumer privacy and data security would be better safeguarded by clarifying that legal obligations rest on data aggregators or data users.

With respect to privacy and data security, SIFMA also recommends that the CFPB consult with other regulators concerning each agency's applicable legal frameworks. To that end, SIFMA encourages the CFPB to hold public roundtables or similar fora with the other agencies to receive feedback from industry participants and to help ensure that the CFPB's rulemaking is aligned with broader innovation efforts across the financial services regulatory community.

## 3. Consumers Should Be Provided With Clearer Disclosures Concerning Data Access and Sharing.

By disclosing their user credentials and account data to data aggregators, consumers may inadvertently subject themselves to privacy risks. Consumers may not appreciate the full scope of the data collected by data aggregators or data users, much of which may be unrelated to the consumer service for which authorization is provided. Similarly, consumers may not understand that data aggregators and data users often copy and store consumer data or use it for other commercial purposes including the development of new products and services.

The broad scope of data collected by aggregators and users across various sources may also raise particular privacy concerns. Data collected from one data holder is often sufficiently anonymized to protect individual consumers' privacy; once combined with other data elements in the aggregator's possession, however, it may be possible to re-identify particular individuals and ascertain sensitive personal attributes. In addition, certain sensitive data attributes, such as personal trading data, may be confidential to the data holder and particularly sensitive if obtained by third parties or aggregated across many consumers.

To help ensure consumer privacy, the CFPB therefore should require that consumers be provided with clearer disclosures about how their financial information will be used and shared. For example, consumers should be provided with information about what data is being retrieved by data aggregators, which data users or other entities are also receiving copies of their data, how frequently data is retrieved and received, which entities are handling the data, and those entities' regulatory obligations to safeguard the security of that data. Placing these affirmative obligations on data aggregators to disclose their intended use of the authorized data provides additional protections to consumers by ensuring that the aggregators take appropriate precautions to safeguard consumer privacy. Because data aggregators provide innovative products directly to consumers, they are better positioned to take such precautions than are financial institutions, which often have no direct contractual relationships with these third parties and cannot control how they use the accessed consumer data.

Accordingly, the CFPB also should impose consumer notification requirements on data aggregators that are no less protective than current federal regulatory notification requirements for financial institutions. Data aggregators' disclosures to consumers should include information about what consumer data has been collected by the data aggregators (including personally identifiable information, if any), as well as any subsequent uses of that data for commercial purposes unrelated to the consumer service under which authorization was provided (*e.g.*, creating and monetizing derivative data, combining consumer data with other data sets to re-identify individuals, etc.). The CFPB should also consider whether it would be appropriate to develop options for providing consumers with a clear and easy method of terminating access to their data.

## 4. The CFPB Should Support Industry Establishment of Standards for Consumer Data Access.

Data aggregators and data users generally employ two methods to collect financial information from data holders: (*i*) "screen-scraping" credential-based access; and (*ii*) application programming interface ("API") access. Although APIs require individual bilateral negotiations, and access to API technologies is not equally distributed across financial institutions (because smaller institutions may need to make significant investments in their cybersecurity and IT infrastructure to support the adoption of API technologies), APIs have benefits over screen-scraping. For example, screen-scraping creates security and privacy concerns by requiring consumers to turn over their log-in credentials to data aggregators and is more susceptible to inaccuracy. And screen-scraping can be a rather blunt tool. As compared to screen-scraping, APIs provide data holders with more control in managing data access, including by enabling data holders to minimize or restrict the scope of data transferred to data aggregators or data users to a subset of the data accessible to consumers themselves.

SIFMA supports the use of technologies that do not require consumers to turn over log-in credentials to data aggregators or users, including an eventual transition from credential-based access to API access.

Industry stakeholders are best suited to address and set appropriate standards for data access. Rather than prescribing the means of authorized access, SIFMA encourages the CFPB to support industry efforts to create interoperable standards that can accelerate innovation and adapt to future technological advances. SIFMA commends the Financial Data Exchange ("FDX") for bringing together leading financial institutions, fintech companies, data aggregators, trade groups, and consumer advocates to create an industry-standard API, a framework for security and certification, and user experience guidelines. The CFPB should endeavor to support such industry standard-setting efforts, including those of FDX, rather than prescribing rigid technical guidelines that quickly become outdated.

Accordingly, the CFPB should not require financial institutions to adopt either credential-based access or API-based access, but should allow industry stakeholders to collaborate in establishing a flexible framework best suited to facilitate consumer data access fitted to institutions', data users', and data aggregators' individual circumstances, consistent with the security and privacy standards SIFMA urges the CFPB to adopt. Moreover, as API technology continues to develop, this flexible framework will allow industry stakeholders to quickly adapt, thereby maximizing both benefits and protections for consumers.

## 5. The CFPB Should Carefully Limit the Scope of Data Subject to Section 1033.

Section 1033 covers a defined scope of information with several defined exceptions. Specifically, section 1033 applies to information "concerning the consumer financial product or service" obtained from a covered entity, "including relating to any transaction, series of transactions, or to the account including costs, charges and usage data."[11] Further, section 1033 does not apply to (*i*) "any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors" or (*ii*) "any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information."[12]

SIFMA encourages the CFPB to carefully define the scope of data covered by section 1033 so that all personal information collected directly from consumers by financial institutions is not within scope. As an initial matter, section 1033 does not provide a right for consumers to access all personal information that can be collected directly from the consumer by a financial institution and, therefore, financial institutions should not be required to make available to a consumer all personal information, such as the consumer's address, birthdate, employment information, or similar information that might be collected in connection with the opening and administration of an account. As one example, there may be consumer personal information that is subject to the GLBA's protections that falls outside the scope of section 1033.

---

[11] 12 USC § 5533(a).

[12] 12 USC § 5533(b).

SIFMA also encourages the CFPB to ensure that consumer data is no less protected after it is acquired by data aggregators or data users than when it is held by regulated financial institutions. Once consumer data is obtained by these third parties, data holders lack the ability to meaningfully control how it is used, aggregated, or shared. To this end, SIFMA recommends that the CFPB ensure that any downstream uses of consumer data comply with the scope of the consent obtained from consumers, including by tailoring the scope of accessible data to the consumers' consent.

Furthermore, consumer trading data, market data[13] obtained through third parties, derived data,[14] and third-party data generated by a user's participation in various activities[15] can reveal market movements when aggregated and, therefore, raise significant sensitivities and regulatory implications for data holders. For example, once aggregated with data from other sources, third parties can obtain a precise view into consumer trading patterns, lifestyle choices, and even their daily location. Accordingly, such sensitive data should be excluded from the scope of the section 1033 implementing regulations. As the CFPB develops its rulemaking, SIFMA urges the CFPB to consult with the SEC concerning the implications of providing third-party access to information—including brokerage orders, trading orders, and other trading data—that are regulated by the SEC.

Further consideration is needed concerning the potential risk of unfettered access by aggregators to financial institutions' websites or applications during times of market stress or volatility. During these times, financial institutions may experience significant stresses on their systems due to increased data access by data users and aggregators. SIFMA therefore encourages the CFPB to provide an exception to authorized access during times of market stress or volatility.

* * *

---

13 Market data is information about current stock prices, recent trades, and supply-and-demand levels sold by national securities exchanges. *See* SIFMA, "Market Data" (last accessed Jan. 18, 2021), available here.

14 Derived data generally consists of data that has been manipulated or combined with other data to create new information or products, such as an index, financial model, benchmark, or performance measurements.

15 Third-party data concerning user activities may include, among other information, how often a consumer accesses her account; data concerning her mobile device; and geolocation information, including GPS data.

SIFMA greatly appreciates the CFPB's consideration of the issues above and would be pleased to discuss these comments in greater detail. If you have any questions or need any additional information, please contact me at mmacgregor@sifma.org.

Sincerely,

Melissa MacGregor
Managing Director and Associate General Counsel

cc: Courtney Dankworth, Partner, Debevoise & Plimpton
David Portilla, Partner, Debevoise & Plimpton
Anna Gressel, Associate, Debevoise & Plimpton
Amy Aixi Zhang, Associate, Debevoise & Plimpton