the address listed above. Comments may also be submitted by facsimile to (301)713–0376, or by email to *NMFS.Pr1Comments@noaa.gov*. Please include the File No. in the subject line of the email comment.

Those individuals requesting a public hearing should submit a written request to the Chief, Permits and Conservation Division at the address listed above. The request should set forth the specific reasons why a hearing on this application would be appropriate.

FOR FURTHER INFORMATION CONTACT: Amy Hapeman or Sara Young, (301) 427–8401.

SUPPLEMENTARY INFORMATION: The subject amendment to Permit No. 18016 is requested under the authority of the Marine Mammal Protection Act of 1972, as amended (16 U.S.C. 1361 *et seq.*), the regulations governing the taking and importing of marine mammals (50 CFR part 216), the Endangered Species Act of 1973, as amended (16 U.S.C. 1531 *et seq.*), and the regulations governing the taking, importing, and exporting of endangered and threatened species (50 CFR 222–226).

Permit No. 18016, issued on May 29, 2014 (79 FR 41991), authorizes the permit holder to conduct vessel surveys in Cook Inlet, Alaska for photo-identification and observations of Cook Inlet beluga whales (*Delphinapterus leucas*). The purpose of the research is to identify individual whales and to provide information about movement patterns, habitat use, survivorship, reproduction, and population size. The permit holder is requesting the permit be amended to increase the number of whales that may be approached during surveys from 72 to 340 whales annually. Animals may be taken up to 10 times per year during surveys. The amendment is needed to increase the effectiveness of photo-identification studies and to decrease the total time spent operating the survey boat around whales. No other details of the permit would change.

In compliance with the National Environmental Policy Act of 1969 (42 U.S.C. 4321 *et seq.*), an initial determination has been made that the activity proposed is categorically excluded from the requirement to prepare an environmental assessment or environmental impact statement.

Concurrent with the publication of this notice in the **Federal Register**, NMFS is forwarding copies of this application to the Marine Mammal Commission and its Committee of Scientific Advisors.

Dated: November 16, 2016.

Julia Harrison,

Chief, Permits and Conservation Division, Office of Protected Resources, National Marine Fisheries Service.

[FR Doc. 2016–28022 Filed 11–21–16; 8:45 am]

BILLING CODE 3510–22–P

BUREAU OF CONSUMER FINANCIAL PROTECTION

[Docket No.: CFPB–2016–0048]

Request for Information Regarding Consumer Access to Financial Records

AGENCY: Bureau of Consumer Financial Protection.

ACTION: Notice and request for information.

SUMMARY: The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) provides for consumer rights to access financial account and account-related data in usable electronic form. The Bureau of Consumer Financial Protection (Bureau or CFPB) is seeking comments from the public about consumer access to such information, including access by entities acting with consumer permission, in connection with the provision of products or services that make use of that information. Submissions to this Request for Information will assist market participants and policymakers to develop practices and procedures that enable consumers to realize the benefits associated with safe access to their financial records, assess necessary consumer protections and safeguards, and spur innovation.

DATES: Comments must be received on or before February 21, 2017.

ADDRESSES: You may submit responsive information and other comments, identified by Docket No. CFPB–2016–0048, by any of the following methods:

- *Electronic:* Go to *http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Email: FederalRegisterComments@cfpb.gov.* Include Docket No. CFPB–2016–0048 in the subject line of the message.
- *Mail:* Monica Jackson, Office of the Executive Secretary, Consumer Financial Protection Bureau, 1700 G Street NW., Washington, DC 20552.
- *Hand Delivery/Courier:* Monica Jackson, Office of the Executive Secretary, Consumer Financial Protection Bureau, 1275 First Street NE., Washington, DC 20002.

Instructions: Please note the number associated with any question to which you are responding at the top of each response (you are not required to answer all questions to receive consideration of your comments). The Bureau encourages the early submission of comments. All submissions must include the document title and docket number. Because paper mail in the Washington, DC area and at the Bureau is subject to delay, commenters are encouraged to submit comments electronically. In general, all comments received will be posted without change to *http://www.regulations.gov.* In addition, comments will be available for public inspection and copying at 1275 First Street NE., Washington, DC 20002, on official business days between the hours of 10 a.m. and 5 p.m. eastern standard time. You can make an appointment to inspect the documents by telephoning 202–435–7275.

All submissions, including attachments and other supporting materials, will become part of the public record and subject to public disclosure. Sensitive personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. Submissions will not be edited to remove any identifying or contact information.

FOR FURTHER INFORMATION CONTACT: For general inquiries, submission process questions or any additional information, please contact Monica Jackson, Office of the Executive Secretary, at 202–435–7275.

Authority: 12 U.S.C. 5511(c); 12 U.S.C. 5512(c).

SUPPLEMENTARY INFORMATION: The Bureau is seeking public comment through this Request for Information (RFI) to better understand the consumer benefits and risks associated with market developments that rely on access to consumer financial account and account-related information. This RFI generally refers to such information as ''consumer financial account data.'' [1] It further refers to consumer access to such information, including access by entities acting with consumer permission, as ''consumer-permissioned'' access. The RFI also labels account information that is obtained via consumer-permissioned access as ''consumer-permissioned account data.''

[1] The RFI sometimes distinguishes ''consumer financial account data'' from ''non-financial'' consumer account data, the latter being held by companies that offer consumers non-financial products and services. The RFI uses the term ''consumer account data'' to refer collectively to both kinds of consumer account data, financial and non-financial.

The information obtained in response to this RFI may help industry develop best practices to deliver benefits to consumers and address potential consumer harms. It may also help the Bureau in prioritizing resources. For example, the Bureau may use the information obtained to evaluate whether any guidance or other action by the Bureau is called for, including future rulemaking.

The Bureau encourages comments from all members of the public. The Bureau anticipates that the responding public may encompass the following groups, some of which may overlap in part:

- Individual consumers;
- Consumer and civil rights groups;
- Privacy advocates;
- Consumer financial product and service providers that control or possess data about consumer use of their products and services (for purposes of this RFI, ''consumer financial account providers'');
- Consumer financial product and service providers that rely, at least in part, on consumer-permissioned access to consumer financial account data (for purposes of this RFI, ''consumer-permissioned providers'' or ''permissioned parties'');[2]
- Entities that obtain consumer financial account data directly from consumer financial account providers for consumer-permissioned providers (for purposes of this RFI, ''account aggregators'');
- Consumer reporting agencies;
- Data brokers, processors and platform providers;
- Regulators;
- Providers of non-financial consumer products and services that may have knowledge of or experience in the use of consumer-permissioned account data to provide products and services to consumers;
- Participants in non-U.S. consumer markets with knowledge of or experience in the use of consumer-permissioned account data to provide products and services to consumers; and
- Any other interested parties.

Part A: Regulatory Framework Applicable to Consumer-Permissioned Access to Account Information

General Background

In the Dodd-Frank Act, Congress instructed the Bureau to implement and enforce consumer financial law ''for the purpose of ensuring that all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive.'' [3] Congress further instructed the Bureau to exercise its authorities so that ''markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation.'' [4]

The Bureau has jurisdiction with respect to a number of Federal statutes and regulations that establish rights and protections related to consumer financial account-related information. These well-established statutory and regulatory frameworks cover a broad range of entities, including traditional providers of consumer financial products and services and newer entrants. In some cases, they may cover service providers to such entities as well.

Many of these frameworks impose requirements that consumer financial account providers disclose certain information to their customers about their accounts. Disclosure requirements may include, for example, periodic statements with account information on transactions and fees or disclosures about the collection, sharing, use, and protection of consumers' non-public personal information.[5] A consumer also has the right to access information about himself or herself held by certain entities, such as information in a consumer reporting agency's file on the consumer.[6]

These and other legal frameworks also establish substantive consumer protections with respect to certain types of consumer information. Such protections include limitations on the use of such information, limitations on the disclosure of such information to third parties, and requirements relating to the security of such information.[7] Other protections include limitations on consumer liability if a consumer's information is lost or stolen and the consumer suffers a loss from unauthorized use or an erroneous electronic debit.[8] The Bureau also has authority under Title X to take action to prevent covered persons and service providers from committing or engaging in unfair, deceptive, or abusive acts or practices (UDAAPs). An entity's consumer data privacy or security practices can violate UDAAP standards.[9]

Consumer-Permissioned Access to Consumer Financial Account Information

In the context of this existing statutory and regulatory landscape, section 1033 of the Dodd-Frank Act provides for consumer rights to access information.[10] More specifically, section 1033 requires that ''[s]ubject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of such person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, or series of transactions, to the account including costs, charges,

[2] For purposes of this RFI, consumer-permissioned providers are *third-party* providers. Thus, consumer financial account providers do not themselves count as consumer-permissioned providers by virtue of using the account data that they already hold to deliver additional services to customers.

[3] 12 U.S.C. 5511(a).

[4] 12 U.S.C. 5511(b)(5).

[5] *See, e.g.,* Regulation Z, 12 CFR 1026.5(b)(2) and 1026.7(b) (implementing the Truth in Lending Act with respect to periodic statements for credit cards); Regulation E, 12 CFR 1005.9(b) (implementing the Electronic Fund Transfer Act with respect to periodic statements for traditional bank accounts and other consumer asset accounts); Regulation DD, 12 CFR 1030.6(a)(3) (implementing the Truth in Saving Act with respect to periodic statements for deposit accounts held at depository institutions); Gramm-Leach Bliley Act, 15 U.S.C. 6803, and its implementing regulations. Further, on October 5, 2016, the Bureau issued a final rule amending Regulations E and Z for prepaid accounts. For prepaid accounts, the final rule provides that as an alternative to providing the periodic statement, a financial institution must, among other things, make an electronic history of a consumer's account transactions available to the consumer that covers at least 12 months preceding the date the consumer electronically accesses the account. The requirement will become effective on October 1, 2017.

[6] Fair Credit Reporting Act, 15 U.S.C. 1681g(a).

[7] *See, e.g.,* Fair Credit Reporting Act, 15 U.S.C. 1681 through 1681x, Gramm-Leach-Bliley Act, 15 U.S.C. 6801 through 6809, and their implementing regulations.

[8] TILA, as implemented by Regulation Z, protects credit card consumers from unauthorized credit card use. *See* TILA section 133; 15 U.S.C. 1643; 12 CFR 1026.12(b). EFTA, as implemented by Regulation E, does the same with respect to EFTs. *See* EFTA section 909(a); 15 U.S.C. 1693g(a); 12 CFR 1005.6(b)(2).

[9] In March 2016 the Bureau entered into a consent order with a provider of a consumer-facing, online payment network. Among other things, the Bureau found that the entity falsely represented to consumers that it employed reasonable and appropriate measures to protect data obtained from consumers from unauthorized access. (*See http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf.*) Relying on section 5 of the Federal Trade Commission Act, which makes unlawful all ''unfair or deceptive acts or practices in or affecting commerce,'' *see* 15 U.S.C. 45(a)(1), the FTC has also taken action against companies that fail to take reasonable measures to protect the security of consumer data. *See, e.g.,* FTC Matter/File Numbers 1023142–X120032 (Wyndham Worldwide Corporation); 052–3148 (CardSystems Solutions, Inc.); 052–3136 (Superior Mortgage Corp.); 052–3096 (DSW Inc.); 052–3117 (Nations Title Agency, Inc.); 062–3057 (Guidance Software, Inc.); 072–3046 (Life is good, Inc.); 072–3055 (TJX Companies); and 052–3094 (Reed Elsevier, Inc.).

[10] 12 U.S.C. 5533.

and usage data.'' [11] Section 1033 further provides that the information must be in an electronic form usable by the consumer, although it does not impose any duty to maintain or keep any information about a consumer. Additionally, section 1033 applies only to information that the consumer financial account data holder can ''retrieve in the ordinary course of its business with respect to that information.'' [12]

Part B: Current Market Practices in Connection With Consumer-Permissioned Access to Account Information

General Market Practice

In recent years, the availability of consumer financial account data in electronic form, often in real-time or near-real-time, has made possible a range of benefits to consumers. When made readily available, such data foster consumer convenience, and they can help consumers understand and control their financial lives, make useful decisions, monitor spending and debt, set and achieve savings goals, communicate effectively with their financial service providers, and solve financial problems in timely ways.[13]

Many providers of consumer financial products and services, from traditional providers like banks and credit unions to newer entrants such as online lenders, make available to consumers extensive electronic data about their accounts at that firm. Many consumers, however, maintain accounts with several financial service providers. As a result, by the late 1990s, market participants began to offer consumers services that depended, at least in part, on broader, consumer-permissioned access to data across a consumer's financial accounts—sometimes combined with other information about the consumer. Traditional account providers like banks have been the predominant users of such consumer account data. By obtaining data about the consumers' other accounts, banks and other traditional market participants have been able to supplement their use of existing in-house data for online advisory and account management services.[14] Over time, however, newer entrants have also begun to provide products and services to consumers using consumer-permissioned, electronically-sourced account data.[15]

Some consumer-permissioned providers have used their own proprietary technology solutions to access data from consumer financial account providers. However, given the large number of potential data sources and the transaction costs associated with obtaining consumer account data (sometimes on a recurring basis), other providers have relied on third-party ''account aggregators'' to provide the necessary technology. (Some entities have provided both account aggregation services to third parties and direct services to consumers using permissioned data.) In either case, the process of accessing consumer account data is often referred to as account or data aggregation.[16]

Technology advances have facilitated the development of aggregation services and the associated delivery of products and services that rely on consumer account data access. The Bureau understands that methods to access consumer account data—and to obtain consumer permission to do so—are technically complex and actively evolving. To enable access, consumers are often prompted to provide their online account credentials, including user name and password, and other forms of authentication such as knowledge-based security questions. Depending on the product or service, consumers may be asked to permit access only to a single account with an individual company or financial institution, or to multiple accounts held by a number of financial institutions and other companies.

Typically, consumers provide their account credentials for a particular company or financial institution where they hold an account. Those credentials are then used to obtain their account data through either: (1) A structured data feed or an application program interface (API) hosted by the company or financial institution, or (2) the company or financial institution's consumer-facing Web site in a process known as screen-scraping.[17] If an account aggregator is an intermediary in this process, it will generally transmit the consumer's data to permissioned parties through an API. The Bureau understands that account aggregators, as well as product and service providers that use consumer-permissioned data, sometimes store consumer account data for a range of uses, including those discussed further below. In addition, they sometimes obtain updated consumer account data on a recurring basis.

Consumer Benefits From Specific Market Uses

The Bureau is aware of a number of types of products and services provided to consumers that make use of consumer financial account data on a consumer-permissioned basis, including the following:

- *Personal financial management:* Many personal financial management (PFM) tools allow consumers to view their account information from many accounts and financial service providers in a single, consolidated view.
- *Automatic or motivational savings:* Some companies provide automatic savings mechanisms for consumers to choose as well as messages to encourage savings. These companies may use algorithms that rely on permissioned account data to determine how much a consumer can afford to save or, at the transaction level, to ''round-up'' transaction amounts to the next dollar and save the remainder.
- *Budgeting analysis and advice:* Many providers allow consumers to set budgets and analyze their spending activity based on the classification of transaction data into categories like entertainment, food, and health care. Some services send a mobile or email notification when a consumer is over-budget or close to being over-budget. Consumers may be provided with other budgetary advice based on analysis of their transaction data, including comparisons with peer groups.

---

[11] 12 U.S.C. 5533(a). The Dodd-Frank Act defines ''covered person'' in detail at 12 U.S.C. 5481(6). The Act defines a ''consumer'' as ''an individual or an agent, trustee, or representative acting on behalf of an individual.'' 12 U.S.C. 5481(4).

[12] *See id.,* 5533(c), & 5533(b)(4). Section 1033 contains a number of other exceptions. *See* 5533(b)(1)–(3). In addition, it requires the Bureau to prescribe standards to promote the development and use of standardized formats for information to be made available to consumers, including through the use of machine readable files. *See* 5533(d).

[13] *See, e.g.,* Aite Group, *Personal Financial Management: A Platform for Customer Engagement* (Feb. 24, 2010).

[14] As far back as 2001, the Office of the Comptroller of the Currency (OCC) issued guidance to depository institutions under its supervision about using third parties to provide data aggregation services. *See* Office of the Comptroller of Currency, OCC Bulletin 2001–12, *Bank-Provided Account Aggregation* Services (February 28, 2001), *available at https://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-12.html#.*

[15] *See, e.g., https://www.mint.com/terms* (''The Mint Service is a personal finance information management service that allows you to consolidate and track your financial information. The Mint Service is provided to you by Intuit without charge[.]'') Intuit is Mint's parent company.

[16] This RFI generally uses the terms ''account aggregation'' or ''aggregation.''

[17] For example, Yodlee, an account aggregator, reports that 75 percent of the data it aggregates from over 14,500 sources is collected through structured feeds from its financial institution customers and other financial institutions. *See* Envestnet, 2015 Annual Report, at 14 (Feb. 29, 2016), *available at http://ir.envestnet.com/phoenix.zhtml?c=235783&p=irol-IRHome.* Yodlee was an independent company until it was acquired by Envestnet in 2015.

• *Product recommendations:* Some advisors or providers may make product recommendations based on consumer financial account data. For example, if checking account data show the consumer incurring ATM fees, a provider might recommend other checking accounts with lower or no ATM fees.

• *Account verification:* Many consumer financial and non-financial products and services require consumers to verify their identity and bank account information. Account aggregation technology may be used for near-instant verification of account ownership. When used in this manner, such technology eliminates any need for the consumer to enter their account and routing number, a manual process that carries the possibility of typographical error. Account aggregation technology used for verification purposes can also eliminate the use of ''micro-deposits,'' which is a verification method that can take significantly longer to confirm account ownership.

• *Loan application information verification:* Some lenders may access consumer financial account data, such as the account's deposit history, to verify income and other stated loan application data. Aggregation can make this kind of verification process more efficient and more reliable.

• *Credit decisioning:* Some lenders may be using or considering using consumer or small business owner account data for underwriting or credit scoring purposes.

• *Cash flow management:* Some third-party providers notify consumers when transactions occur, when funds clear, or when an account balance approaches or dips below zero. These alerts can help consumers manage their cash flow and, in some cases, transfer money into their account to avoid NSF and overdraft fees.

• *Funds transfer and bill payment:* Some providers may obtain consumer authorizations to transfer funds for other purposes, such as timely bill payment or automatic transfers to retirement plans, and use information based on consumer financial account data to inform decisions about the transfer, such as its size and timing. Some companies also receive available funds data to verify account balances before initiating an account debit. Using that data they can avoid debiting an account that has insufficient funds and triggering NSF or overdraft fees for the consumer. In addition, some providers may retrieve bill information for consumers and allow the consumer to pay their bills, a process sometimes known as EBPP (for electronic bill presentment and payment).

• *Fraud and identity theft detection:* Some service providers may analyze consumer transactions across various financial accounts to identify and alert consumers to potential fraudulent or erroneous transactions.

• *Investment management and other non-consumer business services:* Some product and service providers rely on consumer financial account data to provide individuals with investment management services. In a similar manner, non-consumer data (such as data from a small business's checking account) may be used to provide accounting and expense management services to small business owners, their investors, or lenders.

Current Market Issues and Risks

Market developments to date speak to the consumer benefits associated with consumer-permissioned account data access. However, such access may also present risks to market participants, including consumers. Public discussion of access to consumer financial account data has focused significant attention on data security and privacy issues.[18] In particular, some consumer financial account providers have raised concerns about whether account aggregators or permissioned parties employ adequate security and privacy procedures with respect to consumers' online account credentials and consumer account data obtained through aggregation.[19]

Privacy and security concerns have also been raised about whether account aggregators and permissioned parties obtain or retain more consumer information than is necessary for the specific product or service being provided, as well as the extent to which—and terms under which—they may use the data for purposes other than providing the requested product and service and may make data available to other entities.[20] A number of parties have also raised concerns about the application of the Fair Credit Reporting Act in this area.[21] In addition, some consumer financial account providers have expressed concern about their liability for unauthorized transactions that may result from a breach of consumer credentials or consumer financial account data held by an account aggregator or a permissioned party.[22] The Bureau understands that discussions among market participants surrounding these and other security and privacy-related issues are ongoing.

The Bureau also understands that market participants, including financial institutions that provide consumer deposit and other financial accounts, non-financial providers of consumer products and services, account aggregators, and permissioned parties continue to address their working arrangements, often bilaterally, with respect to consumer account data. Those efforts encompass the sharing of technical burdens, the frequency and volume of data provision, counterparty vetting, consumer protection obligations (particularly in the event of a data breach), compensation and indemnity arrangements, and other concerns. The Bureau believes, however, that such market participants do not necessarily share common views about consumer protection and other consumer interests.

More fundamental still, the Bureau does not believe that consumer views have been adequately represented in this area. The Bureau is concerned, therefore, that some market participants may decide to restrict consumer-permissioned access to data in ways that undermine consumer interests identified in section 1033—and that are broader than necessary to address legitimate privacy and security concerns.

[18] In a different context, commenters have told the Bureau that such concerns—what data will be retrieved, how securely it will be stored, and with whom it will be shared—may cause consumers not to adopt new, potentially beneficial products and services. *See* Consumer Financial Protection Bureau, *Report on Mobile Financial Services,* at 54–64 (November 2015) (listing ''security'' and ''privacy'' as the top two challenges or risks to adoption of mobile financial services by the underserved), *available at http://files.consumerfinance.gov/f/201511_cfpb_mobile-financial-services.pdf.*

[19] *See* Peter Rudegeair, *J.P. Morgan Warns It Could Unplug Quicken and Quickbooks Users,* Wall St. J. (Nov. 24, 2015), *available at http://www.wsj.com/articles/j-p-morgan-may-unplug-some-customers-access-to-account-data-1448375950?alg=y.*

[20] *See, e.g.,* Bradley Hope, *Provider of Personal Finance Tools Tracks Bank Cards, Sells Data to Investors,* Wall St. J. (Aug. 6, 2015) (reporting that Yodlee sells some of the data it collects to investment firms but that Yodlee has not publicly disclosed that it does so, and that Yodlee has stated that individuals' identities cannot be discerned from its data set), *available at http://www.wsj.com/articles/provider-of-personal-finance-tools-tracks-bank-cards-sells-data-to-investors-1438914620.*

[21] *See, e.g.,* Federal Reserve Bank of Philadelphia, Compliance Corner (Q4 2001), *On-line Aggregation: Benefits and Risks,* at CC4, *available at https://www.philadelphiafed.org/bank-resources/publications/compliance-corner/2001/q4cc_01.pdf.*

[22] *See, e.g.,* Jamie Dimon, *Letter to Shareholders,* at 21 (April 6, 2016) (expressing ''extreme concern'' over, among other things, data security and privacy, because customers have let aggregators access their bank accounts and account information); *see also,* Robin Sidel, *Big Banks Lock Horns with Personal-Finance Web Portals,* Wall St. J., Nov. 4, 2015, *available at http://www.wsj.com/articles/big-banks-lock-horns-with-personal-finance-web-portals-1446683450.*

Part C: Questions Related to Consumer-Permissioned Access to Account Information

This request for information is intended to cover practices—and potential practices—concerning consumer-permissioned access to consumer financial account data. The Bureau is interested in learning more about how consumer products and services may rely on such data, regardless of whether the products or services that make use of such data are technically ''consumer financial'' products or services, or whether such products also rely on consumer-permissioned data from non-financial accounts or on data from other sources. So long as submissions shed light on the use of consumer-permissioned access to consumer financial account data, they will be responsive. Except where specifically noted, therefore, these questions use consumer ''products'' and ''services'' to refer to consumer products or services that are financial or non-financial, *but that rely at least in part on consumer-permissioned access to consumer financial account data.*

Questions 1 through 17 below seek information about current market practices. Questions 18 through 20 enable commenters to describe how they believe market practices may or should change over time. Questions use ''consumer-permissioned access'' to cover direct access by the consumer upon request and access by the consumer's permissioned designees, but, where they deem it appropriate, respondents may provide different answers for these two forms of consumer access.

Current Practices

1. What types of products and services are currently made available to consumers that rely, at least in part, on consumer-permissioned electronic access to consumer financial account data? What benefits do consumers realize as a result? This question covers the use of such data to deliver products or services or to assess eligibility for a given product or service.

2. How many consumers are using or seeking to use such products or services? What demographic or other aggregate information is available about these consumers?

3. To provide or assess eligibility for these products and services, what kinds of consumer *financial* account data are being accessed, by what means, under what terms, and how often? How long is accessed data stored by permissioned parties or account aggregators?

4. To provide or assess eligibility for these products and services, what kinds of *non-financial* consumer account data are being accessed by parties that also access consumer financial account data? By what means, under what terms, and how often? How long is accessed data stored by permissioned parties or account aggregators?

5. What types of companies offer products and services that rely, at least in part, on consumer-permissioned electronic access to consumer financial account data, either to deliver the product or service or to assess eligibility for the product or service? To what extent are such products and services offered by entities that offer transaction accounts? To what extent are they offered by other market participants?

6. In what ways, if any, do consumer products and services that rely, at least in part, on consumer-permissioned electronic access to consumer financial account data differ according to whether the offering company provides or does not provide transaction accounts to consumers? Do any such differences impact consumers? If so, how?

7. To what extent do market participants compete to offer consumer products and services that rely, at least in part, on consumer-permissioned access to consumer financial account data? How does such competition impact consumers?

8. What incentives or disincentives exist for consumer financial account providers to facilitate or discourage consumer-permissioned access to the account data that they hold by permissioned parties or account aggregators? In what ways do consumer financial account providers directly or indirectly facilitate or restrict consumer-permissioned access to account data? What are the associated impacts to consumers and other market participants?

9. What impediments, obstacles or risks do consumer financial account providers currently face in providing data to or allowing access to data by permissioned parties or account aggregators? Describe specific operational costs, risks, and actual or potential losses, and identify their specific causes.

10. What impediments, obstacles or risks do permissioned parties or account aggregators currently face in obtaining such data? Describe specific operational costs, risks, and actual or potential losses, and identify their specific causes.

11. What impediments, obstacles or risks do consumers currently face in obtaining—including permitting access to—such data?

12. What security and other risks do consumers incur if they permit access to their financial account data in order to obtain a particular product or service? What steps have consumer financial account providers, account aggregators, permissioned parties and other users of consumer-permissioned account data taken to mitigate such risks? What information do these parties communicate to consumers about associated risks?

13. In what ways, do account aggregators or permissioned parties use consumer-permissioned account data for purposes other than offering or facilitating the delivery of a specific product or service to the permissioning consumer? Do such companies continue to access or store data after the consumer ceases to use the product for which the permissioned data use was intended by the consumer? Do such companies share the data with other parties and, if so, under what terms and conditions? What are the associated impacts to consumers?

14. When consumers permit access to their financial account data, what do they understand about: what data are accessed; how often they are accessed; for what purposes the data are used; whether the permissioned party or account aggregator continues to access, store or use such data after the consumer ceases to use the product or service for which the permissioned data use was intended by the consumer; and with which entities a permissioned party or account aggregator shares the data and on what terms and conditions? What drives or impacts their level of understanding? What impact does their level of understanding have on consumers and on other parties, including on consumers' willingness to permit access?

15. To what extent are consumers able to control how data is used by permissioned parties or account aggregators that obtain that data via consumer-permissioned access? Are consumers able to control what data are accessed, how often they are accessed, for what purposes and for how long the data are used, and with which entities, if any, a permissioned party or account aggregator may share the data and on what terms and conditions? Are they able to request that permissioned parties, account aggregators, or other users delete such data? Is such data otherwise deleted and, if so, when and by what means? To what extent are consumers consenting to permissioned party and account aggregator practices with respect to access, use and sharing of consumer financial account data?

16. Do consumer financial account providers vet account aggregators or permissioned parties before providing

data to them? Do consumer financial account providers perform any ongoing vetting of account aggregators or permissioned parties? If so, for what purposes and using what procedures? What are the associated impacts to consumers and to other parties?

17. What industry standards currently exist, in development or otherwise, to enable consumer-permissioned access to financial account data?

Potential Market Developments

18. What changes are or may be expected to happen to any market practice described in response to questions 1 through 17, why, and with what impacts to consumers, consumer financial account providers, permissioned parties, and account aggregators? Responses to this question may be integrated into responses to questions 1 through 17 if commenters prefer.

19. What changes *should* happen to any market practice described in response to questions 1 through 18, why, and with what impacts to consumers, consumer financial account providers, permissioned parties, and account aggregators? Responses to this question also may be integrated into responses to questions 1 through 17 if commenters prefer.

20. Are ''industry standard'' practices that provide consumers with data access comparable to that envisioned by section 1033 of the Dodd-Frank Act likely to be broadly adopted by consumer financial account providers, permissioned parties and account aggregators in the absence of regulatory action? If not, how will ''industry standard'' practices be insufficient? What marketplace considerations are likely to bear on such developments? Generally, how will the advent of standard practices for consumer-permissioned access to consumer financial account data affect competition and innovation in various consumer financial service markets?

Dated: November 14, 2016.

Richard Cordray,

Director, Bureau of Consumer Financial Protection.

[FR Doc. 2016–28086 Filed 11–21–16; 8:45 am]

BILLING CODE 4810–25–P

BUREAU OF CONSUMER FINANCIAL PROTECTION

Supervisory Highlights: Fall 2016

AGENCY: Bureau of Consumer Financial Protection.

ACTION: Supervisory highlights; notice.

SUMMARY: The Bureau of Consumer Financial Protection (CFPB) is issuing its thirteenth edition of its Supervisory Highlights. In this issue of *Supervisory Highlights,* we report examination findings in the areas of auto originations, automobile loan servicing, debt collection, mortgage origination, student loan servicing, and fair lending. As in past editions, this report includes information about a recent public enforcement action that was a result, at least in part, of our supervisory work. The report also includes information on recently released examination procedures and Bureau guidance.

DATES: The Bureau released this edition of the Supervisory Highlights on its Web site on October 31, 2016.

FOR FURTHER INFORMATION CONTACT: Adetola Adenuga, Consumer Financial Protection Analyst, Office of Supervision Policy, 1700 G Street NW., 20552, (202) 435–9373.

SUPPLEMENTARY INFORMATION:

1. Introduction

In this thirteenth edition of *Supervisory Highlights,* the Consumer Financial Protection Bureau (CFPB) shares recent supervisory observations in the areas of automobile loan origination, automobile loan servicing, debt collection, mortgage origination, mortgage servicing, student loan servicing and fair lending. The findings reported here reflect information obtained from supervisory activities completed during the period under review. Corrective actions regarding certain matters remain in process at the time of this report's publication.

CFPB supervisory reviews and examinations typically involve assessing a supervised entity's compliance with Federal consumer financial laws. When Supervision examinations determine that a supervised entity has violated a statute or regulation, Supervision directs the entity to implement appropriate corrective measures, such as refunding moneys, paying of restitution, or taking other remedial actions. Recent supervisory resolutions have resulted in total restitution payments of approximately $11.3 million to more than 225,000 consumers during the review period. Additionally, CFPB's supervisory activities have either led to or supported two recent public enforcement actions, resulting in over $28 million in consumer remediation and an additional $8 million in civil money penalties.

This report highlights supervision-related work generally completed between May 2016 and August 2016 (unless otherwise stated), though some completion dates may vary. Please submit any questions or comments to *CFPB_Supervision@cfpb.gov.*

2. Supervisory Observations

Recent supervisory observations are reported in the areas of automobile loan origination, automobile loan servicing, debt collection, mortgage origination, mortgage servicing and student loan servicing. Worthy of note are the beneficial practices centered on good compliance management systems (CMS) found during the period under review in the areas of automobile loan origination (2.1.1), debt collection (2.3.7), and mortgage origination (2.4.1).

2.1 Automobile Origination

The Bureau's rule defining larger participants in the auto loan market went into effect in August 2015.[1] The consequence was that the Bureau now has supervisory authority over auto lending not only by the largest banks, but also by various other large financial companies. Examinations completed in the period under review focused on assessing CMS and automobile financing practices to determine whether entities are complying with applicable Federal consumer financial laws.

2.1.1 CMS Strengths

During the period under review at one or more entities, examiners determined that the overall CMS of their automobile loan origination business was strong for its size, risk profile, and operational complexity. These institutions effectively identified inherent risks to consumers and managed consumer compliance responsibilities. They maintained: Strong board and management oversight; policies and procedures to address compliance with all applicable Federal consumer financial laws relating to automobile loan origination; current and complete compliance training designed to reinforce policies and procedures; adequate internal controls and monitoring processes with timely corrective actions where appropriate; and processes for appropriately escalating and resolving consumer complaints and analyzing them for root causes, patterns or trends.

These entities also showed strength in their oversight programs for service providers. In particular, they defined processes that outlined the steps to assess due diligence information, and their oversight programs varied commensurate with the risk and

[1] 12 CFR 1090.108.