October 30, 2023

CFPB Proposes "Open Banking" Rule Requiring Covered Entities to Provide Consumers Access and Transferability of Financial Data

On October 19, 2023, the Consumer Finance Protection Bureau ("CFPB") issued a 299-page proposed rulemaking that would require covered entities—generally, providers of checking and prepaid accounts, credit cards, and digital wallets—to provide consumers and consumer-authorized third parties with access to consumers' financial data free of charge.[1] Covered entities would be required to comply with uniform standards to provide access to this financial data through consumer and developer interfaces.[2] The proposed rule would also impose requirements on authorized third parties (such as fintechs), as well as data aggregators that facilitate access to consumers' data, including required disclosures to consumers regarding the third parties' use and retention of the requested data and a requirement that the data only be used in a manner reasonably necessary to provide the requested product or service (thus foreclosing selling the data or using it for targeted advertising or cross selling purposes).[3]

The proposed "Personal Financial Data Rights" rule is the latest step in a yearslong regulatory process to implement Section 1033 of the Dodd-Frank Act.[4] The proposal reflects Director Chopra's goal of "shift[ing] toward open and decentralized banking."[5] The CFPB estimates that at least 100 million Americans have authorized a third-party company to access their account data, and the proposal is aimed at further facilitating this process by giving consumers a legal right to readily transfer their financial data from one financial provider to another.[6] According to the CFPB, this would promote consumer choice, incentivize financial service providers to provide better service because customers can more easily switch providers, and allow newer providers to compete more easily.[7] In addition to allowing consumers to switch providers more readily, the CFPB cites the main use cases for sharing

1 The proposed rule is available here.

2 Proposed § 1033.301(a).

3 Proposed §§ 1033.421, 1033.431.

4 *See* Preamble to the Proposed Rule, pp. 23–26, 182–83.

5 CFPB, *CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking* (Oct. 19, 2023), available here.

6 *See* Preamble to the Proposed Rule, pp. 10, 16–18.

7 *See* Preamble to the Proposed Rule, pp. 18–22.

this data as facilitating "personal financial management tools of all kinds, payment applications and digital wallets, credit underwriting (including cashflow underwriting), and identity verification."[8]

Comments on the proposed rule are due by December 29, 2023, and the CFPB's goal is to issue a final rule by fall 2024. Below, we provide a high-level overview of the proposal and offer some observations.

Requiring Covered Entities to Provide Consumers and Authorized Third Parties with Access to Covered Financial Data

Subpart B of the proposed rule requires covered entities to provide covered data to consumers and authorized third parties. Covered data providers are any entities—including banks and digital wallet providers—that control or possess covered data concerning the following consumer financial products and services:[9]

- Personal checking, savings, and other consumer asset accounts held directly or indirectly by a financial institution;[10]
- Prepaid accounts, including payroll card accounts, certain government benefit accounts, and an account which is capable of being loaded with funds and whose "primary function is to conduct transactions with multiple, unaffiliated merchants for goods or services, or at automated teller machines, or to conduct person-to-person transfers, and . . . [t]hat is not a checking account, share draft account, or negotiable order of withdrawal account;[11]
- Credit cards;[12]
- Other products or services that facilitate payments from the asset accounts or credit cards described above—such as when a digital wallet facilitates a payment from a linked credit card in what are "sometimes referred to as pass-through payments."[13]

The CFPB intends for "neobanks, digital wallet providers, and similar nondepository entities," among others, to be covered data providers.[14] The agency stated that this initial scope of covered products is intended to "prioritize the most beneficial use cases for consumers and leverage data providers' existing capabilities," and that it intends to cover additional products and services through supplemental rulemaking.[15]

---

8 *See* Preamble to the Proposed Rule, pp. 12–13.

9 The CFPB summarizes these products as Regulation E asset accounts, Regulation Z credit cards, and products or services that facilitate payments from the foregoing. *See* Proposed rule p. 31.

10 This does not include accounts for "an occasional or incidental credit balance in a credit plan" or accounts held under a "bona fide trust agreement"; Proposed § 1033.111; 12 CFR 1005.2(b).

11 This generally does not include, among other things, HSAs, gift certificates, store gift cards, and loyalty, award, or promotional gift cards; Proposed § 1033.111; 12 CFR 1005.2(b)

12 Proposed §§ 1033.111; 1026.2(a)(15)(i).

13 Proposed § 1033.111; Preamble to the Proposed Rule, p. 31.

14 Preamble to the Proposed Rule, p. 33 ("The CFPB requests feedback on the proposed definitions, including whether any further clarification is needed to demonstrate that entities that refer to themselves as neobanks, digital wallet providers, and similar nondepository entities would qualify as data providers.").

15 Preamble to the Proposed Rule, p. 33; The CFPB cited mortgage, automobile, and student loans as products as to which data is generally shared through consumer interfaces and that would support a "variety of beneficial use cases," but stated that such data typically do not support "transaction based underwriting across a range of markets or payment facilitation." *Id.*

Depository institutions that do not have a consumer interface by the compliance date would be exempted, but those that stop providing a consumer interface after the effective date would not be exempted.[16] The CFPB estimates that exempt depository institutions without consumer interfaces hold only 0.64 percent of all deposit accounts.[17] The CFPB recognized that this exception would treat depository data providers differently than nondepository ones and noted that "nondepository data providers within scope of this proposed rule tend to use business models built on the ability to innovate with respect to technology and move quickly to implement technological changes and solutions, in contrast to depository institutions that have not established a consumer interface for their customers."[18]

Under the proposal, covered data would include:

- Account balance information and at least 24 months of transaction information, which includes "amount, date, payment type, pending or authorized status, payee or merchant name, rewards credits, and fees or finance charges";[19]
- Information allowing the receiving entity to initiate payments to or from a Regulation E account (generally a consumer asset or prepaid account);[20]
- Terms and conditions such as an "applicable fee schedule, any annual percentage rate or annual percentage yield, rewards program terms, whether a consumer has opted into overdraft coverage, and whether a consumer has entered into an arbitration agreement";[21]
- Upcoming bill information, including, for example, the minimum amount due on the data provider's credit card billing statement, and also scheduled payments to third parties, such as a utility company;[22]
- Basic account verification information, which is limited to "the name, address, email address, and phone number associated with the covered consumer financial product or service."[23]

Exceptions would apply for:

- Any confidential commercial information, including an algorithm used to derive credit risk or other risk scores or an underwriting model;[24]
- Any information collected only to prevent fraud or money laundering, or to detect, or make any report regarding other unlawful conduct;[25]

16 Proposed § 1033.111; Preamble to the Proposed Rule, p. 37.

17 *See* Preamble to the Proposed Rule, p.39.

18 *See* Preamble to the Proposed Rule, p. 39.

19 Proposed § 1033.211(a)–(b).

20 Proposed § 1033.211(c); Under the proposal, a data provider would be permitted to make available tokenized account and routing numbers instead of the actual numbers. *See* Preamble to the Proposed Rule, pp. 61–62.

21 Proposed § 1033.211(d); *See* Preamble to the Proposed Rule, p. 62.

22 Proposed § 1033.211(e).

23 Proposed § 1033.211(f).

24 Proposed § 1033.221(a).

25 Proposed § 1033.221(b).

- Any information required by law to be kept confidential;[26]
- Any information that cannot be retrieved in the ordinary course of business by the data provider. [27]

Requiring Covered Data Providers to Establish and Maintain Interfaces to Provide Consumers and Authorized Third Parties Access to Covered Data for Free Upon Request

Subpart C of the proposed rule would impose obligations on covered data providers to establish and maintain interfaces that allow authenticated consumers and authorized third parties to access covered data.

The CFPB noted that it is not aware of "significant concerns" regarding current consumer interfaces and intends for the proposed rule to generally ensure the continuation of current data provider practices in this regard.[28]

The proposed rule would prohibit data providers from imposing fees or charges in connection with data access services provided under the proposed rule, though the provider may charge fees for other services available through the consumer interface that are not covered by the proposed rule.[29] For example, banks would still be able to charge account maintenance or wire transfer fees.

Subpart C distinguishes between consumer interfaces (e.g. online banking applications) and developer interfaces (e.g. application programming interfaces or APIs), and requires data providers with existing consumer interfaces to establish and maintain developer interfaces in order to comply with third-party requests for consumer data. The requirement of a separate developer interface is intended to prevent data providers from relying on screen scraping to comply with the proposal's data sharing obligations. The CFPB believes that this would "help the market move away from screen scraping, even outside of the product markets covered under the proposed rule."[30] In the preamble to the rule, the CFPB included an ambiguous warning to data providers about blocking the use of screen scraping during implementation of the rule or for products outside the rule's coverage:

> During the rule's implementation period, and for data accessed outside its coverage, the CFPB plans to monitor the market to evaluate whether data providers are blocking screen scraping without a bona fide and particularized risk management concern or without making a more secure and structured method of data access available (e.g., through a developer interface). If so, the CFPB would consider using the tools at its disposal to address this topic in advance of the proposed compliance dates.[31]

Both consumer interfaces and developer interfaces would be required to produce requested consumer data as machine-readable files that could be retained and transferred to a different information system.[32] Developer interfaces, specifically, would be required to provide consumer data in a format that is established as a "qualified industry standard" or, in the absence of a qualified industry standard, a widely-used format to facilitate an easier transfer of data between different institutions.[33]

---

26 Proposed § 1033.221(c).

27 Proposed § 1033.221(d).

28 Preamble to the Proposed Rule, p. 67.

29 Proposed § 1033.301(c).

30 Preamble to the Proposed Rule, p. 19.

31 *Id.*

32 Proposed § 1033.301(b)

33 Proposed § 1033.311.

Covered data providers may have additional non-compliant consumer interfaces such as mobile banking phone applications so long as they maintain a compliant consumer interface.

The proposed rule would require the performance of developer interfaces to be "commercially reasonable" according to two indicia of reasonableness. The first indicator is compliance with a "qualified industry standard"[34] and the second is whether the interface meets the performance specifications of the interfaces of similarly situated data providers.[35] The proposed rule would also establish a minimum response rate of 99.5%, excluding requests and responses during scheduled maintenance.[36] The proposed rule establishes that there will be requirements for scheduled downtime for interfaces and other industry standard performance and technical specifications.[37] The exact technical specifications are defined with respect to "qualified industry standards" that do not yet exist.

Data providers also may not unreasonably restrict the frequency of requests for data or responses to those requests, including by imposition of a cap.[38] Frequency restrictions must not be discriminatory, and they must comply with the provider's own written policies and procedures. The proposed rule suggests that a frequency restriction's compliance with a "qualified industry standard" is one indicator that it is reasonable. The CFPB requested comment on whether the final rule should include: (i) a presumption of unreasonableness unless the denial of data access is time-limited for the purpose of preventing interruption of other data requests, (ii) a cap on the total amount of data that a particular third party could request over a period of time, and (iii) different treatment for data providers according to the size of the data provider. [39]

Subpart C also requires data providers to undertake security measures, including disallowing third parties from accessing consumer data using tokenized versions of the consumer's credentials.[40] The Bureau noted that, while tokenized screen-scraping may be more secure than screen-scraping with consumer credentials in their original, unmodified form, it still poses risks to consumer privacy and does not yield data in a standardized format.[41] The proposed rule would require Gramm-Leach-Bliley Act ("GLBA") financial institutions to apply to their interfaces a data security program that complies with that Act.[42] The Bureau anticipates that most existing consumer and developer interfaces already comply with the proposed rule's technical requirements.

Under the proposal, covered data providers would be obligated to provide requested data to authenticated consumers and authorized third parties. However, covered data providers may deny requests if they cannot verify the identity of the consumer or third party, if they cannot confirm the third party followed authorization procedures (described below), or if they cannot identify the scope of the data requested.[43] To clarify the scope of the data requested, the provider is permitted to ask the

---

34 Many of the Proposed Rule's technical specifications are defined with reference to "qualified industry standards." Proposed § 1033.141 would empower the Bureau to recognize standard-setting bodies as issuers of qualified industry standards upon request by the standard-setting body. The Bureau does not set forth an exact process it would use to recognize standard-setting bodies, but it lists criteria that it would take into account. These criteria include: whether it is open to all interested parties, whether decision-making is balanced across interested parties, whether it has written and publicly available policies and procedures, whether it has an appeals process, whether decisions are made by consensus, and whether its standard-setting process is transparent.

35 Proposed § 1033.311(c)(1).

36 Proposed § 1033.311(c)(1)(i).

37 Proposed § 1033.311.

38 Proposed § 1033.311.

39 Preamble to the Proposed Rule, pp. 84-85.

40 Proposed § 1033.311(d)(1).

41 Preamble to the Proposed Rule, p. 69.

42 Proposed § 1033.311(d)(2).

43 Proposed § 1033.331.

consumer to confirm the account to be accessed and the scope of the data requested. But data providers are not required to confirm third party authorization with the consumer directly, although they are not prohibited from doing so.[44] Additionally, the proposed rule provides that a data provider can reasonably deny a consumer of third-party access to its interface based on "risk management concerns."[45] This must be applied in a consistent and non-discriminatory manner, and must be directly related to a specific risk of which the data provider is aware, such as a "failure of the third party to maintain adequate data security."[46] The proposed rule provides that, when a third party does not present evidence that its data security practices are adequate to safeguard the covered data, the data provider may deny access without vetting the third party.[47] The CFPB requests comment on whether it should specify the types of evidence a third party would need to present about its data security practices, such as certifications or evidence of vetting by a third-party risk assessment firm.[48]

Providers may also deny access when required to comply with safety and soundness requirements or data security requirements under Federal law.[49]

The proposed rule allows data providers to establish a reasonable method for consumers to revoke any third party's authorization to access consumer data, where reasonableness of the revocation method is defined with respect to "qualified industry standards."[50] The revocation method must be "unlikely to interfere with, prevent, or materially discourage consumers' access to or use of the data, including access to and use of the data by an authorized third party."[51] Upon receipt of a revocation request, the data provider must inform the affected third party.[52] The revocation cannot be partial; it must be for all data previously authorized to be disclosed to the third party.[53]

Covered data providers must also maintain policies and procedures that ensure compliance with Subparts B and C of the proposed rule and that ensure retention of records that evidence compliance.[54]

Requiring Third Parties to Comply with Authorization Procedures and Obtain Informed Consent from Consumers

Subpart D establishes authorization procedures for third parties that retrieve financial data on behalf of consumers, including additional requirements when third parties use data aggregators. Subpart D broadly defines an authorized third party as a third party that seeks covered data from a covered provider and complies with certain consent, certification, and disclosure procedures.[55] Data aggregators are not third parties under the proposed rule, though they may perform authorization procedures on behalf of third parties. Third parties would be required to provide an authorization disclosure to consumers

44 Proposed § 1033.331(b)(2).

45 Proposed § 1033.321(a).

46 Preamble to the Proposed Rule, p. 94.

47 Proposed § 1033.321(d)(1).

48 Preamble to the Proposed Rule, p. 97.

49 Preamble to the Proposed Rule, p. 93.

50 Proposed § 1033.331(e).

51 *Id.*

52 *Id.*

53 Preamble to the Proposed Rule, p. 111.

54 Proposed § 1033.351.

55 Proposed § 1033.401.

explaining the purpose for which the consumer's data would be used.[56] Third parties would also need to certify that they will comply with the limitations on collection, use, and retention imposed on them by the proposed rule; that they will employ certain data security and privacy measures; and that they will ensure that consumers are aware of both the third party's authorized access and the consumers' ability to revoke authorization.[57] Third parties must obtain consumers' express consent to the authorized disclosure via electronic or written signature.[58] The authorization disclosure must be presented to consumers in a form that is "segregated" from other disclosure materials.

The third party would provide a signed authorization form to the data provider to prove that it has the consumer's authorization and that it complied with the authorization procedures. The authorization disclosure form must include:

- the name of the authorized third party;
- the name of the data provider;
- a description of the consumer's requested product or service to be provided by the third party, including a statement that the third party will use the requested data for that purpose only;
- the categories of data that will be accessed;
- a certification that the third party will comply with consent, certification, and disclosure procedures; and
- a description of the mechanism for revoking authorization.

Third parties may only use consumer financial data for practices that are part of, or reasonably necessary to provide, the product or service requested by the consumer. The Bureau stated that targeted advertising, cross-selling, and data sales are not part of, or reasonably necessary to provide, any other product or service, effectively prohibiting the use of consumer data for those purposes. The Bureau's rationale is that these practices are not primarily intended to benefit the consumer, consumers often do not understand the breadth of their authorization to include these practices, and many consumers consider these practices invasive.[59] The proposed rule would allow third parties to collect data for a one-year period after receiving authorization, after which it would require third parties to obtain new authorization.[60] If reauthorization is not provided, the third party must no longer use or retain covered data that was previously collected unless use or retention remains reasonably necessary to provide the consumer's requested product or service.[61] The proposed rule would require third parties that are GLBA financial institutions to apply an information security program to their data collection systems that satisfies the GLBA requirements.[62]

Under the proposed rule, third parties would be required to provide, without fee or penalty to the consumer, an authorization revocation mechanism that is as easy to access as the authorization mechanism itself.[63] Upon a revocation of authorization request from the consumer, the third party must notify "the data provider, any data aggregator, and other third parties to whom

56 Proposed § 1033.411.

57 Proposed § 1033.421.

58 Proposed § 1033.421(g).

59 Proposed § 1033.421(a).

60 Proposed § 1033.421(b)(3).

61 Proposed § 1033.421.

62 Proposed § 1033.421(e)(1).

63 Proposed § 1033.421(h).

it has provided the consumer's covered data."[64] Upon receipt of a revocation request or upon notice from a data provider of a revocation, the third party must stop collecting data pursuant to the most recent authorization. Further, third parties must stop using and retaining data collected pursuant to the most recent authorization unless using or retaining that data remains reasonably related to providing the consumer's requested product or service.[65]

Subpart D acknowledges that many institutions use data aggregators to access and process consumer financial data, and it allows but does not require data aggregators to perform the third-party authorization procedures on behalf of the third party.[66] The third party would still bear the ultimate responsibility for compliance with authorization procedures.[67] Regardless, if a data aggregator will be used, the disclosures to the consumer must include the name of the data aggregator and a certification from the data aggregator to the consumer that it will comply with the requirements for authorized third-party access to consumer financial data.[68] The proposed rule would also amend 12 CFR § 1001 to explicitly include data aggregators and similar financial data processing products in the definition of a financial product or service.[69]

Compliance Timeline

Subpart A proposes a four-tiered compliance timeline for covered data providers based on the total asset holdings (for depository institutions) or revenues (for nondepository institutions).[70] The regulation would apply:

- Six months after publication of the final rule in the Federal Register for depository institutions holding at least $500 billion in total assets and nondepository institutions with revenue of at least $10 billion;
- One year after publication of the final rule in the Federal Register for depository institutions holding at least $50 billion but less than $500 billion in total assets and nondepository institutions with less than $10 billion in revenue;
- Two and one-half years after publication of the final rule in the Federal Register for depository institutions holding at least $850 million but less than $50 billion in total assets; and
- Four years after publication of the final rule in the Federal Register for depository institutions holding less than $850 million in total assets.

Director Chopra stated that the Bureau's goal is to finalize the rule by fall 2024.[71]

Observations

The proposed rule is the latest step in a lengthy process that the CFPB has engaged in to develop its policy around section 1033 of the Dodd-Frank Act, which became law more than a decade ago. The steps in this process include the following: the CFPB released and received comments on a request for information on consumer rights to access financial data in 2016; released principles around data sharing in 2017; and then held a symposium, released a summary of proceedings, and released and

64 Proposed § 1033.421(h)(2).

65 Proposed § 1033.421(h)(3).

66 Proposed § 1033.431(a).

67 *Id.*

68 Proposed § 1033.431(b) and (c).

69 Proposed § 1001.2(b).

70 Proposed § 1033.121.

71 CFPB, *Prepared Remarks of CFPB Director Rohit Chopra on the Proposed Personal Financial Data Rights Rule* (Oct. 19, 2023), available here.

received comments on an Advanced Notice of Proposed Rulemaking in 2020.[72] It then issued an outline for the SBREFA process in October 2022, inviting other stakeholders to submit feedback on the outline by January 25, 2023.[73] The CFPB also issued CFPA section 1022(c)(4) market monitoring orders to data aggregators and large data providers to collect information related to personal financial data rights in January 2023.[74] Following a SBREFA panel, the CFPB issued a SBREFA panel report in April 2023 and then this proposed rule in late October 2023.[75] While the substance of the proposed rule largely tracks the SBREFA outline released in October 2022,[76] the proposal reflects some notable changes, including:

- Requiring that data providers only provide 24 months of historical financial information (rather than requiring providers to provide information for as far back in time that is available to the consumer on the consumer interface);[77]
- Prohibiting a third party from using the consumer data it obtains for targeted advertising, cross-selling of other products or services, and sale of covered data;[78]
- Requiring that third parties obtain reauthorization from a consumer each year following the prior authorization.[79]

Furthermore, certain types of information that were under consideration in the outline to be included as covered data are not required in the proposed rule, including consumer reports and information about transactions not typically shown on periodic statements or portals such as card networks, ATM networks, ACH networks, check-collection networks, and real-time payment networks.[80] Also, certain account identity information is not required by the proposed rule due to privacy and discrimination risks, such as age, gender, marital status, number of dependents, race, ethnicity, citizenship or immigration status, veteran status, date of birth, social security number, and driver's license number.[81] But terms and conditions, including any annual percentage rate or annual percentage yield, are considered covered data in the proposed rule.[82]

Other notable aspects of the proposed rule include:

- The absence of a prohibition on screen scraping of data by a third party from a data provider using consumer credentials when that data provider offers a compliant developer interface, although it appears that the CFPB may have intended to include such a prohibition. The CFPB observed that "screen scraping as a whole presents risks to consumers and the market," and it rejected the notion of allowing data providers to rely on screen scraping as a means of complying with the proposed

72 *See* Preamble to the Proposed Rule, pp. 182–183; *See* CFPB, *CFPB Outlines Principles for Consumer-Authorized Financial Data Sharing and Aggregation* (Oct. 17, 2023), available here.

73 *See* Preamble to the Proposed Rule, p. 24.

74 *See* Preamble to the Proposed Rule, p. 25.

75 *See* Preamble to the Proposed Rule, p. 24.

76 The SBREFA Outline is available here.

77 Proposed § 1033.211(a); *See* Preamble to the Proposed Rule, pp. 58–59.

78 Proposed § 1033.421; *See* Preamble to the Proposed Rule, pp. 138–141.

79 Proposed § 1033.421; *See* Preamble to the Proposed Rule, pp. 151–152.

80 *See* Preamble to the Proposed Rule, pp. 54–57; *See* SBREFA Outline pp. 20, 23.

81 *See* Preamble to the Proposed Rule, pp. 62–64; *See* SBREFA Outline p. 22.

82 Proposed § 1033.211(d).

rule.[83] The proposal does include a prohibition on data providers from granting third parties access to developer interfaces using consumer credentials;[84]

- The failure to specify the assignment of liability for errors;
- The requirement that the data provided to authorized third parties is the "most recently updated covered data" the provider has;[85]
- The provision empowering data providers to "reasonably" deny consumers and third parties access to interfaces based on "risk management concerns," which are "directly related to a specific risk of which the data provider is aware."[86]

Under CFPA Section 1022(b), the CFPB engaged in an analysis of potential benefits and costs of the proposed rule.[87] Benefits the CFPB expects of the proposed rule for data providers include an increase in the value of first party covered data held by providers, which are not subject to the same use restriction applicable to third-party collected data.[88] For example, according to the CFPB, data providers would be able to use first party covered data they possess for purposes which are proscribed for third parties such as for "marketing and for the development of new products," thereby increasing the value of such data to providers.[89] The CFPB also stated that data providers would benefit from reductions in screen scraping-generated security risks and web traffic.[90] Notable costs the CFPB expects for data providers include the costs of establishing and maintaining developer interfaces, digital infrastructure costs generated by increased data requests, and informational advantage costs as a result of increased third-party access to first party data.[91]

Notable benefits the CFPB expects for third parties include opening access to data from covered data providers and prohibitions against data provision fees and unreasonable access caps by providers.[92] Notable costs the CFPB expects for third parties include loss of revenue generated from use of covered data for internal marketing of other products and services and sharing covered data with fourth parties.[93]

Given the lengthy policy development process thus far and the controversies section 1033 has engendered, as well as the complexity of various aspects of the proposed rule, we expect a fulsome comment process and that the Director's fall 2024 finalization goal will be challenging to reach.

* * *

83 Preamble to the Proposed Rule, p. 68.

84 Proposed § 1033.311(d).

85 Proposed § 1033.201(b).

86 Proposed § 1033.321.

87 *See* Preamble to the Proposed Rule, pp. 180–181.

88 *See* Preamble to the Proposed Rule, p. 226.

89 *See* Preamble to the Proposed Rule, p. 226.

90 *See* Preamble to the Proposed Rule, pp. 222–224.

91 *See* Preamble to the Proposed Rule, pp. 191, 204–205

92 *See* Preamble to the Proposed Rule, pp. 227–228.

93 *See* Preamble to the Proposed Rule, pp. 215–216.

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Jessica S. Carey
+1-212-373-3566
jcarey@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Katherine B. Forrest
+1-212-373-3195
kforrest@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Brad S. Karp
+1-212-373-3316
bkarp@paulweiss.com

Legal interns Naji Alabed and Josh Stallings contributed to this Client Memorandum.