Consumer Financial Data Aggregation & the Potential for Regulatory Intervention

By: Brian Hurh, Adam Maarec and Christopher M.A. Chamness – June 2017

Introduction

A confluence of regulatory activity and policy debates seem to be laying the groundwork for future regulation of consumer financial data aggregation activities. The outcome of these activities could significantly affect how financial data may be shared by financial institutions, controlled by third-party data aggregators, and used by financial technology companies (“fintechs”) in the future.

Last fall, the Bureau of Consumer Financial Protection (the “CFPB” or “Bureau”) brought this issue to the forefront in the United States when it issued a request for information (the “RFI”) on the varied ways that consumer financial data aggregators obtain, maintain, use, and disclose consumers’ financial data. The number of responsive comments filed by stakeholders, including financial institutions, data aggregators, fintechs, and consumer advocates highlight the diverse perspectives that exist regarding the adequacy and application of existing regulations to data aggregation activities. In addition to regulatory scrutiny from the Bureau, at least one member of the Federal Reserve Board (the “FRB”) has stated that the FRB ought to be concerned with data aggregation activities from a bank safety and soundness perspective. At the same time, regulations in the European Union and United Kingdom governing access to consumer financial data are being implemented, both of which provide an interesting juxtaposition for U.S. regulators and companies to consider.

This article provides background information on the growing number of participants involved in data aggregation activities, summarizes the RFI and commentators’ responses, and discusses select regulatory changes in the European Union and United Kingdom affecting the aggregation of consumer financial data. We then conclude with issues that the involved parties should consider in this uncertain regulatory environment.

The Consumer Finance Aggregator Ecosystem

For roughly two decades, “data aggregators” have sought to collect consumers’ financial account information from various financial institutions, including transaction, balance, and fee information relating to credit cards, auto loans, mortgages, and securities. This data is typically obtained with the consumer’s permission by either screen scraping or application program interfaces (“APIs”). Screen scraping occurs when the data aggregator has automated systems to log in to a particular financial institution as a consumer using the consumer’s username and password, and the company takes (or “scraps”) the account information that is made available online. On the other hand, APIs allow an aggregator to directly connect to a financial institution’s systems and obtain the desired information through an orderly exchange protocol.

On a separate but related track, “product aggregators” primarily obtain consumer financial product information, as opposed to financial account information, to provide a platform that allows consumers to comparison shop for credit cards, auto loans, mortgages, personal loans, and other consumer financial products from multiple providers. These product aggregators have recently evolved to also aggregate consumer financial data, typically by either obtaining a consumer’s express permission to access credit report information and/or by obtaining a consumer’s username and password to access the online banking portals of various financial institutions via screen scraping or APIs. With this access, the
product aggregator can use consumers’ detailed personal financial data to make more targeted and tailored offers for financial products and services to the consumer.

Fintechs are increasingly purchasing and using consumer financial data made available through aggregators in creative ways, for example, to alleviate pain points in personal financial management by providing automatic savings programs, budgeting tools, and investment analysis. Aggregators have also created efficiencies for banks and other financial services providers by providing back-end services, including verification of account numbers, consumer information, and transaction histories.

**Catalyst for Regulatory Intervention: Diverging Interests Between Banks, Aggregators, Fintechs, and Regulators**

In 2015, several large banks shut off aggregators' access to consumers' financial account information. The banks pointed to a series of concerns raised by the aggregators' business models, ranging from internal data security and the enhanced complexities that could arise in the event an aggregator suffers a data breach, to operational limitations on the ability of bank servers to respond to an overwhelming number of aggregator data requests. Following negative feedback from consumers, the banks reversed course days later and allowed aggregators to resume accessing consumers’ data.

The CFPB initially showed interest in the sharing of consumer data with aggregators as part of its “Project Catalyst Initiative.” In a report titled “Promoting consumer-friendly innovation: Innovation Insights,” the CFPB stated that consumer-permissioned access to financial data forms the “basis for personal financial management tools and mechanisms [that can] reduce the time to verify consumers” accounts and provide other consumer benefits. The report notes that the loss of access to consumer data by these third parties “could cripple or even entirely curtail the further development of such products and services.” CFPB Director Richard Cordray reiterated in a speech that the CFPB is “gravely concerned by reports that some financial institutions are looking for ways to limit, or even shut off, access to financial data rather than exploring ways to make sure that such access, once granted, is safe and secure.”

The CFPB subsequently issued the RFI in an effort to better understand the consumer benefits and risks associated with market developments that rely on access to consumer financial account information. The RFI states that its objectives are to: (1) help the industry develop best practices to deliver benefits to consumers and address potential consumer harms; and (2) evaluate whether any guidance or future rulemaking is needed. It remains to be seen whether the RFI will be the CFPB’s opening salvo into future public action, such as the issuance of guidance, regulations, or enforcement actions relating to the sharing, collection, and use of consumer financial data among fintechs, aggregators, and financial institutions.

**CFPB’s RFI on Consumer Financial Records**

**Statutory Authority to Write Rules Affecting Consumer Access to Electronic Financial Records**

The CFPB relies on two distinct provisions of the Consumer Financial Protection Act (“CFPA”) for the potential regulation of consumer financial data aggregation activities and aggregators themselves. Section 1033 of the CFPA gives a consumer the right to request and receive electronic records related to a consumer financial product or service obtained from a financial institution, including transaction, cost, and usage data. The statute exempts certain records from being provided, including: confidential commercial information; information collected to prevent fraud or money laundering; information required to be kept confidential by law; and information that a consumer “cannot retrieve in the ordinary course.” This provision grants the CFPB authority to write implementing rules.

The CFPB’s authority over data security issues is also based on the prohibition of unfair, deceptive, or abusive acts or practices under sections 1031 and 1036 of the CFPA. The RFI cites to the CFPB’s recent data-security case against Dwolla and the Federal Trade Commission’s (FTC) past data security activities as relevant precedent to generally assert that “[a]n entity’s consumer data privacy or security practices can violate UDAAP standards.” While the CFPB has filed only one enforcement action involving data security claims, the FTC has similarly used its unfairness authority (under section 5 of the Federal Trade Commission Act) to regulate specific data security practices.
Concerns & Challenges Expressed in the CFPB’s RFI

In the RFI, the CFPB expressed concern that some financial institutions may restrict consumer-permissioned access to financial records in ways "that undermine consumer interests identified in section 1033 [of the Act]." At the same time, the CFPB recognized that, despite the many consumer benefits of financial data sharing that it seeks to foster, legitimate risks need to be addressed, including data security and privacy.

The RFI’s reference to FTC precedent could indicate the CFPB’s willingness to rely on its UDAAP authority to address problematic data security practices involved in consumer financial data aggregation activities. If the CFPB were to go further and propose rules in this area, that regulatory initiative would be the first use of section 1033 and the first use of sections 1031 and 1036 with respect to consumer financial data aggregation.

Data Gathering: Questions in the CFPB’s RFI

The RFI asks twenty questions on how aggregators operate, including current market practices and how those practices will likely change over time. The following is a summary of the questions posed by the RFI.

- **Product Structures & Use**: How many consumers are using these services and what are their characteristics? How is financial and non-financial information used to assess eligibility for products? How are offers based on this data being made and by whom?

- **Provision of Data**: What incentives or disincentives exist for companies to provide consumer-permissioned data? Why might companies, consumers or aggregators not provide data, e.g., operational costs, risks, and actual or potential losses, and their specific causes?

- **Data Security**: How long is data stored? What security and other risks are incurred by consumers? How are these risks communicated to consumers and mitigated by companies or aggregators?

- **Consumer Understanding**: What consumer-facing disclosures are provided? Are consumers told what data are accessed, how often such data are accessed, how such information is used, whether access continues after a consumer stops using a given product, how sharing occurs and under what terms and conditions? Do consumers understand these practices and how does comprehension impact their willingness to consent?

- **Consumer Control**: Can consumers control how aggregators use their data, and if so, how? May consumers ask for data about themselves to be deleted?

- **Vendor Management**: Do financial institutions vet aggregators before granting access? If so, under what procedures?

- **Adequacy of Industry Standards**: Do industry standards currently comply with section 1033? Are they actually adopted by the industry?

- **Expected & Desired Change**: How are the current market practices expected to change? How should those practices change?

Responses to the RFI

Responses to the RFI predominantly came from three populations: (1) financial institutions; (2) data aggregators and fintechs; and (3) consumer groups.

**Financial Institution Comments.** Financial institutions generally argued that the CFPB should define data aggregators as “larger participants” and subject such larger participants to regular supervision. Several financial institutions noted that Regulation E limitations on consumer liability for “unauthorized transactions” should not apply with respect to a bank if improper transactions are initiated as a result of a data aggregator breach or other misconduct. For example, some commentators argued that a consumer who has given an aggregator their log-in credentials has “furnished [an] access device” to the aggregator and thereby assumed any risk from the aggregator exceeding the
authority granted to it. Commentators also argued that banks should not be liable for unauthorized transactions initiated by or through data aggregators acting as an “electronic fund transfer service provider” under Regulation E.

Additionally, several financial institutions raised questions regarding when a data aggregator might be considered a bank “service provider” subject to enhanced oversight requirements. Financial institutions also indicated that the Gramm-Leach-Bliley Act (GLBA) should apply to aggregators and fintechs holding consumer data. Noting that Section 1033 standards should cover data security, authentication, and access, financial institutions argued that access to consumer financial data should be limited to aggregators with whom they have contractual privity, and that the data retrieved by the aggregator must be identified and disclosed to the financial institution. Financial institutions also asked whether the financial institution or the aggregator ought to bear the costs associated with compliance, and indicated that while access to data should remain free to consumers, if aggregators are monetizing data provided by a financial institution, that some of those proceeds should be routed back to the financial institution. Lastly, financial institutions urged the CFPB to consult with the FTC and prudential regulators before issuing any guidance or rulemaking.

Aggregator & Fintech Comments. While the responses from data aggregators, fintechs and their industry groups focused on different issues, one common theme included a plea that banks should not filter or monopolize access to consumer financial information. These companies stated that the liability for unauthorized transactions under Regulation E that might result from improper use of a consumer’s access credentials should not rest with aggregators or fintechs, but rather that liability should remain with banks. Moreover, if liability does shift from banks, that liability should rest with consumers who assumed the risk involved in using their services. They also argued that both aggregators and fintechs obtaining data from banks are not, in the ordinary course, service providers to banks and are not subject to the regulatory burdens associated with bank vendor management programs. When responding to concerns about data security, aggregators and fintechs argued that technology could solve many data security challenges, citing authentication and tokenization protocols as examples.

Consumer Group Comments. Comments from consumer groups identified safe and secure data sharing as a goal that should be shared by financial instructions, data aggregators and fintechs. Consumer groups argued that certain privacy principles should govern the sharing of all consumer data, including: 1) the disclosure of aggregators’ data use and sharing practices; 2) limited storing and use of the data to the specific purpose for which it was obtained; 3) allowing data sharing only where there is authenticated access; and 4) consumer control over data sharing and rights to revoke access. They argued that consumers should not lose Regulation E liability protections for unauthorized transactions when sharing credentials with aggregators, since improper transactions would still be considered “unauthorized” under the regulation. Finally, consumer groups stated that banks should not be permitted to prevent data access for purposes of stifling competition.

From All Sides: Oversight of Data Aggregator Activities as a Safety and Soundness Concern, and Analysis of Regulatory Approaches to Data Access in the EU & UK

In addition to potential oversight from the CFPB, FRB Governor Lael Brainard indicated in an April 2017 speech that the FRB has a stake in overseeing bank relationships with consumer financial data aggregators. She described banks as one of a number of entities in “the fintech stack,” whereby fintechs are able to build upon the core deposit, lending, and payment activities of banks, much like app developers are able to build various applications that use iPhone or Android mobile platforms. Acknowledging current consumer financial data flows from a bank either to an aggregator via screen scraping or API and then to a fintech, or from a bank directly to a fintech via API, Governor Brainard indicated that the FRB has an interest in ensuring the viability and quality of aggregator arrangements from a safety and soundness perspective, presumambly along with other prudential regulators. Governor Brainard noted that the importance of “getting these connectivity questions right, including the need to manage the consumer protection risks, is critically important. It could make the difference between a world in which the fintech wave helps community banks become the platforms of the future, on the one hand, or, on the other hand, a world in which fintech instead further widens the gulf between community banks and the largest banks.”

The prudential banking regulators, and the CFPB, could also be influenced by trends in European banking regulation favoring greater access to and sharing of consumer financial data. Indeed, there is a statutory requirement that any rules issued by the CFPB must “take into account conditions under which covered persons do business both in the United States and in other countries.” In her April 2017 speech, Governor Brainard noted the varied approaches to data access being taken by regulators around the world. For example, in the European Union, rules implementing the revised Payment
Services Directive ("PSD2") proposed by the European Banking Authority would require banks to permit licensed third parties to access consumer bank account information via API and ban screen scraping. And the United Kingdom recently required the nine largest banks to share pricing, fees, and terms information via API this year, and will require open-access APIs for consumer transaction data and payment information in 2018. However, Governor Brainard indicated that regulators in the United States may not be ready or able to implement regulations demanding a similar degree of openness, in part because of the way regulatory authorities are broadly distributed (e.g. between multiple federal agencies and states with jurisdictions over different sectors of the financial services industry and actors within the consumer financial data aggregator ecosystem) and certain statutory limitations that predate the current technology, fintech, and aggregator ecosystems.

Unlike in the US, the implementation of open banking in Europe must take into account the EU’s strict data protection laws, which require informed consent from customers before their account information can be shared with third parties through APIs. Under the new General Data Protection Regulation, banks will be responsible not only for informing customers of how their data may be used by these third parties but also for putting in place specific contractual and technical protections to ensure that third parties do not disclose or re-use the data without additional approval from customers.

Operating in an Uncertain Regulatory Environment in the Near Term

The CFPB’s RFI suggests that only basic principles of contract and limited regulatory obligations currently apply to aggregators, and that individual transactional solutions could care for consumer protections and control identified risks, but might not do so in a sufficiently uniform manner.

While regulatory bright lines might be helpful, participants in the consumer data aggregation ecosystem should consider how regulation might help clarify the rights and responsibilities of the involved parties, and allow for greater access to financial data, address data security risk, but at the same time potentially limit or slow technological innovations. Following are only some of the issues that financial institutions, aggregators, and fintechs currently engaged in data aggregation activities may want to consider in the near-term:

Trend Towards Bilateral Agreements Presents an Opportunity to Self-Regulate & Identify Applicable Consumer Protection Laws

A trend towards bilateral agreements between banks and aggregators or fintechs can present an opportunity for participants to demonstrate that regulatory intervention is not necessary and that the industry can self-regulate. Key components of an effective self-regulatory system may include, among other things, a degree of uniformity in bilateral agreement terms that accurately reflect the compliance obligations of the parties under applicable consumer protection laws, including GLBA and the Fair Credit Reporting Act. Notwithstanding the ambiguities regarding the application of those laws to aggregators and fintechs, consumers should be provided clear disclosures describing the ways in which their financial data will be collected, used, and shared by the parties, and be provided with a method to control and perhaps stop those activities.

Privacy & Data Security Protections Are Paramount

With respect to privacy and data security, financial institutions may need to more closely consider the scope of their duty to monitor and protect customer information, and identify responsibilities that should be placed upon aggregators so that their mutual customers’ data is protected, including limitations on the use, disclosure, and sale of such data. The technology used by aggregators for authentication and data protection should be thoroughly vetted, and the consequences of a data breach should be defined, including who is responsible for providing data breach notifications under various state laws and how liability stemming from a data breach might be distributed.

Product Recommendations Using Consumer Data Present UDAAP Risk

With respect to the use of aggregated consumer financial data by product aggregators, companies should consider whether the use of such data creates a perception that products recommended to a consumer by the aggregator have been selected based on the consumer’s individual circumstances. If a particular experience places a consumer in a position of “reasonable reliance” on a product aggregator to “act in the interests of the consumer,” then – to follow the
terms of section 1031 of the CFPA – certain conduct by the aggregator, such as product recommendations that are not suitable for the consumer, might be considered “abusive.”

**Limits on the Requirement to Make Electronic Data Available**

The RFI appears to assume that section 1033 of the CFPA grants aggregators, as a consumer’s agent, largely unfettered access to the consumer’s financial data. But section 1033 only grants “a consumer” the right to request records. Recent case law from the Ninth Circuit indicates that a third party’s access to another company’s computer systems without proper authorization may be prohibited by the Computer Fraud and Abuse Act (CFAA), which carries civil and criminal penalties. In *Facebook v. Vachani*, a social media aggregator attempted to use Facebook’s systems at the request of Facebook users. Facebook attempted to block the aggregator from accessing its site through an IP block and a cease and desist letter, but the aggregator continued to access the Facebook database despite this explicit restriction on access. The court found the aggregator’s conduct to be a violation of the CFAA. The court provided the following analogy involving a retail bank branch to demonstrate the difference between user and agent access under the CFAA:

Suppose that a person wants to borrow a friend’s jewelry that is held in a safe deposit box at a bank. The friend gives permission for the person to access the safe deposit box and lends him a key. Upon receiving the key, though, the person decides to visit the bank while carrying a shotgun. The bank ejects the person from its premises and bans his reentry. The gun-toting jewelry borrower could not then reenter the bank, claiming that access to the safe deposit box gave him authority to stride about the bank’s property while armed. In other words, to access the safe deposit box, the person needs permission both from his friend (who controls access to the safe) and from the bank (which controls access to its premises). Similarly, for [the aggregator] to continue its campaign using Facebook’s computers, it needed authorization both from individual Facebook users (who controlled their data and personal pages) and from Facebook (which stored this data on its physical servers). Permission from the users alone was not sufficient [under the CFAA] to constitute authorization after Facebook issued the cease and desist letter.

The defendants in this case have filed a petition for certiorari with the U.S. Supreme Court to appeal the decision.

**Conclusion**

As consumer financial data and product aggregation services become more complex and the attendant data security and other risks become correspondingly higher, financial institutions may want to consider whether enhanced contractual protections and more rigorous oversight of aggregators are necessary. At the same time, aggregators and fintechs might consider supporting this additional level of scrutiny to the extent it is necessary to mitigate identified risks, ensure compliance with applicable laws, and demonstrate that regulatory intervention is not necessary. While there seems to be momentum for new regulations affecting consumer financial data and product aggregation activities, policymakers could permit the currently-developing self-regulatory system to develop and monitor the market for weaknesses before intervening. At the same time, the regulatory approaches being developed in the EU and UK can be viewed as test cases for potential consumer financial data policy in the US.

**Disclaimer**

This article is a publication of Davis Wright Tremaine LLP. Our purpose in publishing this article is to inform our clients and friends of recent legal developments. It is not intended, nor should it be used, as a substitute for specific legal advice as legal counsel may only be given in response to inquiries regarding particular situations. Attorney advertising. Prior results do not guarantee a similar outcome. Davis Wright Tremaine, the D logo, and Defining Success Together are registered trademarks of Davis Wright Tremaine LLP. © 2017 Davis Wright Tremaine LLP
Direct access to a bank’s APIs typically involves a negotiated, bilateral agreement between the financial institution and the aggregator obtaining the consumer financial records, by which the bank will define the data fields to be shared, identify the technology used to share the data, and obtain rights to exercise appropriate oversight to ensure the aggregator does not pose any undue risk to the bank. This is in contrast to open-access APIs, whereby third-parties are generally able to use a widely available API to access financial data held by a financial institution after consenting to a set of standard terms imposed by the bank.

The CFPB sought information on product aggregators (referred to as “third-party comparison sites”) in its 2017 Request for Information Regarding Consumer Credit Card Market. See 82 Fed. Reg. 13313, 13314 (March 10, 2017) (The CFPB asked the following questions related to product aggregators: “To what degree do consumers understand the benefits and risks of using third party comparison sites? To what degree do existing standards, practices, and disclosures protect consumers from unfair, deceptive, and abusive acts and practices? Where, if anywhere, do opportunities for improvement exist, and how would any such improvements most appropriately be realized?”).


Id. at 22.

Id. at 22-23.


Id. § 1033(a) (codified at 12 U.S.C. § 5533(a)) (“Subject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers.”).

Id. § 1033(b)(1)-(4) (codified at 12 U.S.C. § 5533(b)(1)-(4)).

While section 1033(a) of the CFPA appears to indicate that the consumer right to financial records springs into effect only when rules are prescribed by the CFPB, it could be argued that the statute is self-effectuating and applicable to covered persons now. When effective, the right to consumer financial records is enforceable by the CFPB, state attorneys general, and state regulators. See id. §§ 1042(a)(1) (codified at 12 U.S.C. § 5552(a)(1)); 1053(a)(1) (codified at 12 U.S.C. § 5563(a)(1)), and 1054(a) (codified at 12 U.S.C. § 5564(a)).


See RFI at 83807.

See e.g., Federal Trade Commission v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2015).

See RFI at 83809.
which the NPPI was initially disclosed. § 1016.14(a)). At the same time, recipients of NPPI are generally prohibited from using such information for purposes beyond that for which the financial institution that transfers that person are no longer authorized.

19 See 12 C.F.R. § 1005.14(a)(1) (“A person that provides an electronic fund transfer service to a consumer but that does not hold the consumer’s account is subject to all requirements of this part if the person: (1) Issues a debit card (or other access device) that the consumer can use to access the consumer’s account held by a financial institution; and (2) Has no agreement with the account-holding institution regarding such access.”). But see OCC Bulletin 2001-12, Bank-Provided Account Aggregation Services. (Feb. 28, 2001) (noting that, if a bank is accessing and aggregating consumer financial data using a consumer’s login credentials, “it is unclear under the current regulation which party would bear responsibility for an unauthorized transfer” and that in “the absence of guidance, bank management should be conservative when interpreting possible Regulation E compliance obligations in connection with aggregation services”).


21 GLBA is applicable to “financial activities” identified in Section 4(k) of the Bank Holding Company Act. Financial activities include activities determined by the FRB to be so closely related to banking as to be a proper incident thereto. A list of such activities under the FRB’s Regulation Y generally includes processing, storing and transmitting financial, banking or economic data. 12 CFR 225.28(b)(14). The FTC has previously opined that aggregators fall within this definition, stating that this section of the regulation “brings into the definition of financial institution an Internet company that compiles, or aggregates, an individual’s on-line accounts (such as credit cards, mortgages, and loans) at that company’s web site as a service to the individual, who may then access all of its account information through that Internet site.” 65 Fed. Reg. 33646, 33655 (May 24, 2000).


23 Id. (“[If] agreements between data aggregators and banks are structured as data aggregators performing outsourced services to banks, the bank should be able to conduct the appropriate due diligence of its vendors, whose services to those banks may be subject to examination by safety and soundness regulators.”).

24 Id.


26 European Banking Authority, Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) (Feb. 23, 2017). The ban on screen scraping appears to be supported by banks but opposed by fintechs. See European Banking Federation, EBF asks Commission to support ban on screen scraping (May 16, 2017), available at http://www.ebf.eu/ebf-asks-commission-to-support-ban-on-screen-scraping/; (last accessed May 24, 2017) (banking trade association supports the European Banking Authority’s proposed ban on screen scraping, equating aggregator logins using consumer user names and passwords to “impersonating” consumers); and Huw Jones, EU executive asks bank watchdog to rethink ‘screen scraping’ ban, Euronews (May 19, 2017), available at http://www.euronews.com/2017/05/19/eu-executive-asks-bank-watchdog-to-rethink-screen-scraping-ban (last accessed May 24, 2017) (citing the European Commission Vice President Valdis Dombrovskis indication that the European Commission, which must approve the proposed technical standards, will “ask the European Banking Authority to have another look at the draft standards for data interfaces, and at proposals to allow fintechs access to the customer facing interface, whenever the dedicated interface breaks down or is not performing properly…”).

27 Competition and Markets Authority, Making Banks Work Harder for You, United Kingdom (Aug. 9, 2016).


29 For example, a financial institution is generally restricted from disseminating consumers’ non-public personal information (“NPPI”) to third parties except in limited circumstances, including, for example, with the consumer’s consent and subject to the consumer’s right to revoke that consent (see 12 C.F.R. § 1016.15(a)(1)) or as necessary to effect a transaction requested by the consumer (see 12 C.F.R. § 1016.14(a)). At the same time, recipients of NPPI are generally prohibited from using such information for purposes beyond that for which the NPPI was initially disclosed. See generally 12 C.F.R. § 1016.11.
Although the communication of account information from a financial institution to an aggregator may not be subject to the Fair Credit Reporting Act because such a communication would presumably not be deemed a “consumer report”, an aggregator’s subsequent disclosure of that information to a third party (other than the consumer requesting the information) may cause the aggregator to be deemed a “consumer reporting agency.” See 15 U.S.C. § 1681 et seq.


Id. § 1030(c)(2).

844 F.3d 1058 (9th Cir. 2016).

Id. at 1068 (emphasis added).

About the Authors

**Brian J. Hurh** // PARTNER // WASHINGTON, D.C.
Brian Hurh counsels clients on financial regulatory, transactional, and privacy matters involving traditional lending products as well as mobile, prepaid, and other emerging consumer payment solutions. As a former systems engineer and computer programmer for an Internet payment startup company, Brian has both legal and technical knowledge of the financial and business needs of clients that include global financial services companies, international technology providers, online retail and commercial marketplaces, alternative payment service providers and local and national startup ventures.

brianhurh@dwt.com
202.973.4279

**Adam D. Maarec** // ASSOCIATE // WASHINGTON, D.C.
Adam Maarec concentrates his practice on financial services. He advises financial institutions on regulatory compliance matters regarding consumer protection, data privacy and information sharing, and joint marketing. Adam has experience with a broad range of financial protection laws, including Dodd-Frank, the Truth in Lending Act, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Real Estate Settlement Procedures Act, the Telephone Consumer Protection Act, and the CARD Act, as well as state telemarketing and insurance regulations. His regulatory practice includes drafting rulemaking comment letters, meeting with government agencies, and responding to regulatory investigations.

adammarrec@dwt.com
202.973.4217

**Christopher M.A. Chamness** // ASSOCIATE // WASHINGTON, D.C.
Admitted to practice only in Maryland.

Chris Chamness concentrates on financial services. Chris has experience with state licensing and usury issues, and state-law disclosure requirements for closed-end credit products. He has advised on a broad range of regulatory and transactional matters, including state and federal consumer finance protection laws and business lending compliance issues. He also has advised clients on alternative business finance products, including merchant cash advance. Chris also has experience with consumer privacy and fair lending rules and regulations.

chrischamness@dwt.com
202.973.4231