OPEN BANKING

Building Trust

May 2021

CENTER FOR DEMOCRACY & TECHNOLOGY

Open Banking: Building Trust

by Stan Adams & John B. Morris, Jr.

Introduction

The United States is the global leader in online innovation and in the development of online services and applications. But the U.S. significantly lags behind the European Union in the development and offering of open banking apps and services, reflecting the yet-to-be-realized promise of innovation in "fintech." Open banking services are products that securely connect with traditional banks to be able to offer innovative services to banking customers. Open banking offers significant potential benefits to consumers through competition, innovation, and increased convenience.

But to achieve those benefits for consumers, open banking must overcome significant hurdles in terms of trust, and most critically in terms of the privacy and security of customers' banking data. Like health information, financial information is very sensitive and users will need significant protections of their data for open banking products to be broadly embraced in the U.S. Americans are already hesitant to fully embrace the online world because of privacy concerns,[1] and they will be all the more cautious with financial apps and services.

This paper looks at the history and progress of open banking and identifies steps that policymakers and industry can take to ensure that the U.S. can catch up with Europe in terms of vibrant – but security- and privacy-respecting – open banking apps.

Overview of Open Banking

The phrase "open banking" refers to a suite of concepts and products based on the portability of financial data. That is, if banks and other traditional financial institutions facilitate customers' ability to authorize access to their own financial data, then other companies can offer new and useful products and services built around that data, inspiring competition and innovation in consumer banking services. Basically, in a robust open banking environment, banks make it easy for customers to share their own financial data – such as transaction history, purchases, and account balances – with third parties, which in turn can offer different kinds of information and financial services.

[1] *See* Andrew Perrin, Half of Americans have decided not to use a product because of privacy concerns, Pew Research Center (Apr. 14, 2020), https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/.

As seen in the more advanced open banking market in Europe, consumer-focused open banking apps and services generally fall into one of two broad categories: Information-focused apps and transaction-focused apps.

Information-focused apps provide users with additional ways to review, analyze, and understand their banking activities, such as by providing categorized summaries of spending, budgeting tools, or predictions about future impacts of financial decisions. These apps and services can aggregate information from multiple unrelated banks and financial institutions, to allow the users to see and understand the full range of their financial activities. Apps like Yolt and Money Dashboard (both focused on the United Kingdom market) aggregate and consolidate information from multiple accounts into a single interface offering budgeting and planning tools based on the user's goals.[2]

Transaction-focused apps can – with permission and instruction from the user – initiate banking transactions and send and receive money. These apps may build on the features of information-focused apps, but they can also provide investment services, credit cards, payment processing, and automated savings programs. Zeux and Moneybox are examples of European apps that go beyond information aggregation.[3] In addition to these examples of consumer-facing open banking apps and services, open banking will also have significant impacts on business-to-business transactional relationships.[4]

Many in the U.S. may be unfamiliar with the idea of open banking. The concept has been around for several years, but because it requires industry consensus and coordination, standard setting, the development of new kinds of infrastructure to support secure, multi-party access to sensitive information, and enough consumer buy-in to make all of that worthwhile, open banking is still in its early days in the U.S.[5]

Consumer-facing open banking applications hold the potential to improve the ways consumers interact with their finances by providing useful information and tools in a convenient, accessible interface.[6] The wide variety of products and services that open banking could support has the potential to create a more competitive banking environment for consumers, with many choices for handling basic to sophisticated banking arrangements. In Europe, where open banking is

---

[2]Yolt, https://www.openbanking.org.uk/customers/regulated-providers/yolt/, last visited May 26, 2021; Money Dashboard, https://www.openbanking.org.uk/customers/regulated-providers/the-one-place-capital/, last visited May 26, 2021.

[3] Zeux, https://www.openbanking.org.uk/customers/regulated-providers/zeux-limited/, last visited May 26, 2021; Moneybox, https://www.openbanking.org.uk/customers/regulated-providers/moneybox/, last visited May 26, 2021.

[4] Accenture, It's now open banking, Do you know what your commercial clients want from it? (2018) https://www.accenture.com/_acnmedia/PDF-90/Accenture-Open-Banking-Businesses-Survey.pdf.

[5] PWC, "Open banking: US is next," Apr. 2018, https://www.pwc.com/us/en/financial-services/financial-crimes/publications/assets/pwc-open-banking.pdf.

[6] *See* Financial Data and Technology Association (North America), "Opportunities in Open Banking," 2019, https://fdata.global/north-america/wp-content/uploads/sites/3/2019/04/FDATA-Open-Banking-in-North-America-US-version.pdf.

more well-established, providers highlight the convenience and technological benefits of their products. For example, some providers are using their access to data from many customers to build machine learning systems to predict when customers may incur overdraft fees.[7]

But to enjoy these new ways to manage their money, consumers must allow third parties to access and process their financial data, including possibly autonomously executing financial transactions in some circumstances (such as automatic bill payment or savings apps). For that to happen, however, consumers will need to be able to trust the new open banking apps and companies, and must have confidence that their information will be secure and protected as it flows between banks, app companies, merchants, and other players in the financial system. However, consumers' increasing concerns about privacy across the online ecosystem and the lack of baseline privacy protections in the U.S. will make achieving the needed levels of trust and security in open banking more difficult.

The challenge for both policymakers and the emerging open banking industry in the U.S. is to lay a foundation that ensures strong privacy and security protections for customers' sensitive financial information, builds strong technical standards that facilitate secure and private transfers of information, and provides a strong legal path for emerging fintech companies as well as traditional banks to offer innovative apps and services that are secure and privacy protective.

Methods of Access to Customer Banking Information

Most early open banking apps – both in Europe and the few that exist in the U.S. – were based on a dubious practice called "screen scraping," which requires customers to give an open banking app their individual login credentials (usernames and passwords) so that the app can access the customers' financial data through the customers' banks' websites.[8] Screen scraping allowed open banking startups to offer services without any agreements with or consent of the banks that the apps were accessing.

Screen scraping presents significant flaws from a security perspective. Sharing credentials increases the possibility of fraudulent account manipulation because anyone with access to a user's credentials can log in and manipulate the user's account as though they were the user. Because service providers must store these credentials (and must be able to use them in unencrypted form to log into the banks), credentials could be exposed as part of a data breach, thereby giving malicious actors full access to customer financial accounts. Moreover, if a customer decides to stop using an app, the only way to prevent future access by the app would be for the customer to change their login credentials with the bank. Additionally, the act of sharing login credentials is something security professionals have spent decades trying to *stop*

[7] Sanat Rao, "How banks can ride the artificial intelligence wave," Jan. 19, 2018, https://www.livemint.com/Opinion/mwj8mRPsoyXmxl597XKJ8H/How-banks-can-ride-the-artificial-intelligence-wave.html.

[8] GoCardless, "Screen scraping 101: Who, What, Where, When?," Jul. 9, 2017, https://openbankinghub.com/screen-scraping-101-who-what-where-when-f83c7bd96712.

Internet users from ever doing. Companies should not encourage this practice by building systems that depend on sharing credentials.

Fortunately, banks and open banking apps can establish much more secure and controllable access to customers' financial data through the creation of application programming interfaces (APIs). APIs allow banks to make data available in ways that are both more secure and more efficient. Through an API, banks can allow applications to read customer data directly while also controlling the application's ability to interact with or manipulate customer accounts. In some arrangements, users can exert more nuanced control over third parties' access to their accounts with "tokens" which serve as a kind of pre-approved authentication for access. With token-based systems, consumers can grant differing levels of access to multiple providers.[9] For example, a user could allow a financial aggregation application to read (but not manipulate) information from all of their accounts, while granting an open payments application the ability to transfer funds to or from only a single account.

Although the API approach to open banking is far more secure, more flexible, more auditable, and more privacy protective, traditional banking institutions have historically been very resistant to open banking apps, and to creating APIs to facilitate open banking.[10] This resistance stemmed from a range of concerns including competition, liability, and the security of the banks' own internal networks. A key question for open banking in any market will be whether the local banking regulators mandate that traditional banks offer standardized API access to customer data.

The European Approach

Europe provides a useful case study that can suggest paths toward the success of open banking in the U.S. In the mid-2000s, before the term "open banking" had been coined, Europe began to create an integrated, pan-European environment for seamless electronic banking. Europe's focus was not on promoting fintech innovation; instead the most critical goal was to lay the groundwork for flexible cross-border – within Europe – banking.[11] At that time, Europe was moving to a single currency and allowing Europeans to more easily cross borders for work. Thus, workers increasingly would be living and working in a country different from that of their "home" banks. Europe also sought to increase competition within – and with – the traditional banking sector on the continent. Building on earlier foundational directives, the European

[9] Joseph Lorenzo Hall, "The Beginning of the End of Sharing Banking Credentials," Jan. 25, 2017, https://cdt.org/insights/the-beginning-of-the-end-of-sharing-banking-credentials/.
[10] "How open banking will force banks to adopt the cloud," Sept. 1, 2020, https://bankinnovation.net/allposts/products/open-bank/how-open-banking-will-force-banks-to-adopt-the-cloud/.
[11] European Commission, "Payment Services," https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/payment-services_en.

Union set its open banking industry on a strong path in 2015 when it issued its updated Payment Services Directive (PSD2), which went into force in January 2018.[12]

To ensure strong consumer protections, and to overcome resistance from the traditional banking industry, Europe mandated that banks develop and provide secure interconnections – APIs – through which consumer-focused banking products could work together across Europe. The government mandates on banks, coupled with strong privacy mandates (including in Europe's broadly applicable General Data Protection Regulation), laid the foundation for a blossoming open banking environment. Even major European banks – initially resistant to open banking – are coming to embrace the value of the open system.[13]

As Europe moved towards an API mandate, some of the early European open banking apps sought to defend their ability to continue to use screen scraping, in part because they did not have confidence that traditional banks would in fact implement workable APIs.[14] Ultimately, however, Europe mandated that screen scraping would not be permitted, except in circumstances when a bank's mandated API ceased to function.[15]

Independent of the European Union, the United Kingdom also took the regulatory approach to mandate competition and facilitate innovation in banking through open banking across England, Scotland, Wales, and Northern Ireland.[16] Similarly, Australia has recently adopted regulations to securely open the banking industry to competition and innovation.[17]

Initial Paths Forward for Open Banking in the U.S.

Although the U.S. has begun to take some important initial steps toward a robust, secure, privacy-protecting open banking ecosystem, it remains far behind other markets. There remains no clear legislative or regulatory strategy to support and guide the development of open banking, and there are few legal protections to ensure appropriate privacy and security safeguards over consumers' financial information. The banking and fintech industries have begun to collaborate on standards to govern secure API access to data and other critical aspects of a robust open banking system. But without mandates to implement standards, open banking in the U.S. is likely to face greater obstacles than in Europe and elsewhere.

---

[12] European Commission, Payment Services Directive (EU) 2015/2366, https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en, last visited May 26, 2021.
[13] Banks with the most advanced open banking models, Consultancy.eu (Sept. 1, 2020) https://www.consultancy.eu/news/4811/banks-with-the-most-advanced-open-banking-models.
[14] GoCardless, "Screen scraping 101: Who, What, Where, When?," Jul. 9, 2017, https://openbankinghub.com/screen-scraping-101-who-what-where-when-f83c7bd96712.
[15] Skadden Arps Slate Meagher & Flom LLP, "Open Banking: Navigating the Emerging Regulatory Landscape," Oct. 28, 2020, https://www.jdsupra.com/legalnews/open-banking-navigating-the-emerging-15903/.
[16] "What is open banking?" Open Banking UK https://www.openbanking.org.uk/wp-content/uploads/OB_MediaPDF_FINAL.pdf.
[17] Deloitte, "Open Banking: Value Unlocked," https://www2.deloitte.com/au/en/pages/financial-services/articles/open-banking.html#.

The surest path toward a robust U.S. open banking ecosystem would be for Congress to take steps similar to those taken in Europe, the United Kingdom, and Australia – to enact legislation that squarely addresses open banking and ensures that (a) consumers' privacy and security interests are protected, (b) fintech innovators can fairly compete against traditional banking institutions, and (c) responsibility and liability are appropriately allocated and –where appropriate – shared between traditional institutions and fintech companies. Such legislation would directly address the full range of open banking services, from simple information sharing and aggregation to payment processing, automatic investing and savings services, and lending services, among others.

In 2010, Congress did – perhaps inadvertently – take the first step toward facilitating open banking. In enacting Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (commonly referred to simply as Dodd-Frank), Congress mandated that many financial institutions must make available account and transactional information to consumers "in an electronic form usable by consumers."[18] The language of Section 1033 does not on its face appear to envision a world of fintech apps directly accessing customers' financial data through APIs, but instead is phrased in language suggesting only that consumers must be able to download that data in machine readable format.

In the 2010 law, Congress mandated that the then-newly-created Consumer Financial Protection Board ("CFPB") implement Section 1033 through regulations. The CFPB has been slow to carry out that mandate, but the growth of fintech in the interim may convince the CFPB to use its Section 1033 authority to take steps toward enabling open banking. In 2016, the CFPB launched an inquiry into secure sharing of access to financial records, and could have taken steps to facilitate open banking in that process.[19] But by late 2017 – after a change in political administration and significant controversy surrounding the CFPB – the agency chose to only issue non-binding principles to encourage development of open banking. As described by the CFPB, its Consumer Protection Principles were:

> *"...intended to reiterate the importance of consumer interests to all stakeholders in the developing market for services based on the consumer-authorized use of financial data. The Principles express the Bureau's vision for realizing a robust, safe, and workable data*

[18] Dodd-Frank Section 1033(a), codified at 12 U.S.C. § 5533(a) ("IN GENERAL.—Subject to rules prescribed by the [Consumer Financial Protection] 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.").

[19] CFPB, "CFPB Launches Inquiry Into Challenges Consumers Face in Using and Securely Sharing Access to Their Digital Financial Records," Nov. 17, 2016, https://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-inquiry-challenges-consumers-face-using-and-securely-sharing-access-their-digital-financial-records/.

aggregation market that gives consumers protection, usefulness, and value."[20]

These 2017 non-binding principles focused on promoting a "data aggregation market" and did little to address additional questions around permitting open banking apps to initiate and execute payments, investments, and other actual financial transactions. With this continued lack of federal action, screen-scraping remains an insecure tool used by U.S.-focused open banking services.

In 2020, the CFPB returned to Section 1033 and the question of whether the agency should take any more concrete action regarding authorizing direct access to consumer financial data to facilitate open banking offerings.[21] The CFPB subsequently decided to take the initial step toward rulemaking by issuing an Advance Notice of Proposed Rulemaking ("ANPR") to address these issues.[22] Although the ANPR asked questions focused on payments and other uses of open banking to initiate financial transactions, it is unclear given the more limited scope of Section 1033 how far the CFPB can go to create the regulations needed for a strong, secure open banking ecosystem. Nearly 100 commenters responded to the ANPR, including many encouraging the agency to implement strong privacy and security protections for consumer data as well as calls to standardize the ways institutions make data available, such as through open APIs.[23]

The American fintech industry, as well as the traditional banking and financial industry, have not idly waited for federal regulation. As noted, in the absence of a mandate to use a secure API – and the absence of broad cooperation from traditional banks, U.S. open banking services have used screen-scraping to access customer data. And importantly, over the past 15 years, at least two significant – and competing – initiatives were created to develop secure standards and APIs for secure data access. As of mid-2019, the two leading efforts came under the same umbrella, with the Open Financial Exchange (OFX) initiative becoming a part of the Financial Data Exchange (FDX) group, with an express goal of moving toward a single standard based on the FDX framework.[24] The FDX consortium describes itself as a nonprofit organization that is:

---

[20] CFPB, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation," Oct. 18, 2017, https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.
[21] CFPB, "CFPB to Host Symposium on February 26," Feb. 20, 2020, https://www.consumerfinance.gov/about-us/newsroom/cfpb-hosts-symposium-february-2020/.
[22] CFPB, "Consumer Financial Protection Bureau Releases Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records," Oct. 22, 2020, https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-releases-advance-notice-proposed-rulemaking-consumer-access-financial-records/; Federal Register, "Consumer Access to Financial Records." Nov. 6, 2020, https://www.federalregister.gov/documents/2020/11/06/2020-23723/consumer-access-to-financial-records.
[23] Consumer Access to Financial Records, Proposed Rule, Docket CFPB-2020-0034, https://www.regulations.gov/document/CFPB-2020-0034-0001/comment.
[24] FDX, "Frequently Asked Questions about FDX US," https://www.financialdataexchange.org/FDX/About/FAQ-US/FDX/About/FDX_US_FAQ.aspx.

> *"...dedicated to unifying the financial industry around a common, interoperable and royalty-free standard for the secure access of user permissioned financial data, aptly named the FDX API. FDX has an international membership that includes financial institutions, financial data aggregators, fintechs, payment networks, consumer groups, financial industry groups and utilities and other permissioned parties in the user permissioned financial data ecosystem."* [25]

FDX, which is currently centered around fintech and financial companies in the U.S. and Canada, does have some of the larger industry players participating in their effort. In 2019, FDX released a White Paper on "Five Principles of Data Sharing," which reflect an industry recognition that instilling confidence and trust among potential customers will be critical for the success of open banking apps and services.[26] The principles cover many of the important bases for a secure system for open banking – control, access, transparency, traceability, and security – but the White Paper is very light on addressing a sixth critical topic, privacy.

The open banking status quo in the U.S. is not good:

- In the absence of a mandate to financial institutions to offer a secure API, apps and services still use screen scraping and other insecure approaches to access customer data;
- Congress has not directly acted on open banking, meaning that the only financial institutions that are moving toward adopting a secure API are a self-selected subset of major banks and other institutions;
- The efforts of the CFPB hold promise, but the scope of its future regulations is far from clear;
- The industry appears to have taken some important steps toward standardizing a secure API, but critical issues such as privacy and liability within an open banking ecosystem are far from resolved; and
- Consumers interested in using open banking apps have few concrete protections or assurances on critical privacy and security concerns.

We offer some recommendations below, first for Congress and regulators, and then for industry.

[25] FDX, "About," https://www.financialdataexchange.org/FDX/About/FDX/About/About.aspx.
[26] FDX, "Financial Data Exchange Refines Vision for Consumer-First Financial Data Sharing Practices," Aug. 29, 2019, https://www.financialdataexchange.org/FDX/News/Press-Releases/FDX_Refines_Vision.aspx.

Recommendations

For Congress and regulators:

To create a robust, innovative, and secure open banking environment in the U.S., Congress and regulators must step forward and lay a proper foundation of laws and regulations to address critical issues such as privacy, security, and liability.

- **Pass baseline privacy legislation as soon as possible.** Directly legislating on open banking is likely to be a multi-year effort, and Congress is early in its consideration of the issues raised. In contrast, Congress has been wrestling with baseline privacy legislation for years, and there is now bi-partisan support for such legislation. Baseline legislation now would go a long way toward protecting consumers in the open banking market.

- **Tackle open banking issues directly, and quickly.** Both Congress and financial industry regulators should work to require financial institutions to implement secure APIs to support open banking, and should work to prohibit (or, depending on legal authorities, at least limit and strongly discourage) screen scraping as an accepted method of open banking access to customer data. Beyond access and APIs, Congress should act to ensure that there is clear legal responsibility – and liability – among the various participants in the open banking ecosystem. Both financial institutions and fintech start ups must have responsibility to ensure that open banking data exchanges are secure and privacy-protecting, and it should be clear which entities consumers can look to for redress if security and privacy are not protected. Congress should consider adopting a program similar to deposit protection programs to limit the risk to users of open banking services in scenarios where one or more of the companies had security flaws leading to consumer losses.

- **The Consumer Financial Protection Bureau should seek to address many of these issues in its on-going rulemaking process.** Even if the CFPB's legal authority is limited in some areas, its analysis and actions may be able to help guide Congress where legislation is needed.

- **Regulators should conduct audits of data management and security practices in the open banking ecosystem.** Regulators should be able to verify that companies – both traditional financial institutions as well as fintech companies offering open banking products and services – comply with clear and strong data management and security policies. Regulators should further take additional regulatory or enforcement actions to ensure that companies meet industry standards and comply with federal regulations regarding data management, security, and use. To the extent regulators currently lack the authority to audit non-traditional companies, Congress should grant them that power.

For industry:

In the absence of strong leadership from Congress and regulators, industry should seek to create an environment that provides strong protections for consumers, specifically including strong privacy, security, and liability protections. Especially without strong national legislation addressing privacy and security, industry will have to work to gain the trust of consumers – and to avoid the privacy or security "disasters" that could greatly set back the acceptance of open banking in the U.S.

- **Continue development and increase availability of secure and interoperable technical standards and APIs for data access and user control.** Current efforts appear to be headed in a positive direction, but consumer advocates and representatives should be able to assess and test the security, transparency, access, control, and traceability of the technical standards. It is also vital that the APIs be made widely available to both financial institutions and fintech developers.

- **Address privacy head on, and work to ensure that any industry rules that govern open banking services provide meaningful and actionable privacy protections to users.** For open banking to succeed in the U.S., privacy must be protected, and privacy and security "disasters" must be avoided. Ideally Congress would act to mandate strong privacy rules, but in the absence of legislative action, the industry should step forward with strong rules Such a privacy regime would need to ensure (a) secure connections between banks and third party apps, (b) clear and binding limitations on secondary uses of data, with clear and effective consumer recourse for violations, (c) strong transparency about what open banking apps do with users' data, and (d) a range of other more detailed safeguards.

- **Similarly, address shared responsibility, allocated liability for security and privacy problems, and clear means for customers to obtain redress for such problems.** Compared to social networks, retail operations, and movie streaming systems, most users will be more sensitive to privacy and security risks involving their financial information and accounts. If the industry cannot squarely address those concerns, uptake of open banking offerings may lag.

- **Undertake a series of steps specifically designed to promote and build trust in open banking apps and services.** For consumers to be able to trust that open banking services are secure and meet their needs, they must know at a minimum that companies and their vendors will limit uses of consumers' data to only those necessary to provide the service, that they will be able to control access to and uses of their data, and what happens when something goes wrong. Companies should provide clear information addressing these points. Such disclosures serve at least three functions. One, the information itself helps consumers understand their options and make good choices. Two, the act of disclosing relevant and useful information signals a company's willingness to be open and honest with both

customers and potential customers – and helps to set strong business practices for open banking services. Three, disclosures create a public record of a company's commitments to which their actual practices can be compared. Steps to provide clear information to consumers, and promote trust, include:

- *Companies should limit their use of customer data to purposes necessary for the provision of services to customers, and any internal uses not directly connected to providing services should be clearly described to consumers.* Consumers prefer data uses that conform with their understanding of the data processing needed for the service.[27] Although many are willing to accept additional uses of their data, undisclosed data uses undermine trust.

- *Companies should not share customer data with third-party vendors, except as necessary to provide the promised service to customers.* Companies should not share customers' personally identifiable information with third parties unless necessary for the service, but where sharing is necessary, data shared with vendors should be accompanied by strong, enforceable measures to ensure use limitations.[28]

- *Companies should offer accessible, layered, granular options to enable customer control over access to and uses of data, allowing customer control as long as the company retains any of their data.* User-facing data controls will be simple to understand and easy to use, while still providing a comprehensive suite of granular controls.[29] Whether through a dashboard or other style of interface, users should be able to understand the default settings for data sharing, including what data is shared, with whom, and in what format. They should also be able to adjust those defaults as they choose. Such controls should be available for users in all jurisdictions, not just where required by law. Providing these controls to users demonstrates a company's openness in its data practices and its willingness to preserve users' ability to manage uses of their own data. Further, companies should explain what happens to the customers' data after the customer decides to stop using the service, and customers should be able to exert control over data in this context, including asking the company to delete all of the data acquired through the course of their relationship.

---

[27] The Clearing House, *Fintech Apps and Data Privacy: New Insights from Consumer Research*, (Aug. 2018) https://www.theclearinghouse.org/payment-systems/articles/2018/08/-/media/d025e3d1e5794a75a0144e835cd056b3.ashx.

[28] The EU's General Data Protection Regulation (GDPR) already requires strict controls on third-party data sharing agreements, but companies should adopt stringent data controls for vendors regardless of jurisdiction. See Complete Guide to GDPR Compliance, https://gdpr.eu/, last visited May 13, 2020.

[29] Joseph Jerome, Financial Dashboards: Enhancing User Control Outside a Traditional "Privacy Dashboard", (Sep. 17, 2017), https://cdt.org/insights/financial-dashboards-enhancing-user-control-outside-a-traditional-privacy-dashboard/.

- *Companies should require customers to use strong authentication methods to access their accounts.* Given the sensitivity of financial data, and following the European example,[30] companies should mandate customers' adoption of strong security practices, including multi-factor authentication processes for accessing accounts and initiating transactions.[31]

- *Companies should tell consumers how the harms of a security breach will be addressed and which parties are responsible in the various possible situations.* Companies must communicate what they will do to help their customers in the event of a breach, so that customers can factor how companies will take responsibility for security into their consumer choices about competing service providers.

Conclusion

The promise of open banking depends on building trust among consumers. Congress and regulators can take major steps to develop that trust. Both traditional financial institutions and newer fintech companies must also focus on building that trust. Clear, upfront, and thorough communications about the service offered and its terms show consumers that companies are being honest about what they offer and how they will provide the service, including how they will use customers' financial data.

Limiting the uses of customer data, including by third-party vendors, and demonstrating strong security practices shows consumers that a company will act responsibly on behalf of its customers. Finally, preserving customers' control over their own data and honoring their requests to correct, delete, or limit access to it shows consumers that companies respect their customers and their wishes to preserve the privacy and security of their data. Honesty, responsibility, and respect are fundamental to any long-term relationship. Consumers deserve no less in open banking.

[30] European Banking Authority, Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2), Final Report, (Feb. 23, 2017) https://eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf.

[31] CDT, What is Two-Factor Authentication? (Aug. 3, 2018) https://cdt.org/insights/election-cybersecurity-101-field-guide-two-factor-authentication/.