Statement of Natalie S. Talpas, Senior Vice President and Digital Product Management Group Manager, PNC Bank

Consumer Financial Protection Bureau Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act

Wednesday, February 26, 2020

I. Introduction and Executive Summary

PNC Bank, National Association (PNC) appreciates the opportunity to participate in the Consumer Financial Protection Bureau's (Bureau) symposium regarding data aggregators and consumer access to financial records.

PNC is a Main Street bank focused on serving the financial needs of our customers and communities. We have employees in more than 40 states across the country and a retail branch network located primarily in the Mid-Atlantic, Midwest and Southeast, with approximately 2,300 branches and 9,100 ATMs. We are proud of our longstanding history of supporting our customers, communities and employees while operating a sustainable long-term business.

We are committed to providing our customers with access to convenient technology tools and the financial applications of their choice, while protecting the personal and financial information they entrust to us and maintaining the integrity of our systems. We support our customers' use of financial applications (apps) and informed consumer choice in accessing and sharing their financial data. In fact, we process millions of trouble-free logins by financial apps, and the data aggregators that support these apps, each week.

What are data aggregators? Data aggregators are nonbank financial services companies that gather financial data on consumers from banks and other financial institutions, such as broker-dealers, and make this information available to financial apps and, potentially, other purchasers of consumer data. They also act as an intermediary between financial apps and financial institutions, essentially providing the "pipes" through which financial apps connect and gain access to information regarding a consumer's financial accounts or effect transactions through

such accounts. Today, the largest data aggregators hold the sensitive financial information of millions of U.S. consumers.

We are concerned with several aspects of how data aggregators currently operate. First, the manner in which most data aggregators receive customer authorizations lacks transparency. As a result, most customers lack a fundamental understanding of who is collecting their sensitive financial information, how that information is being collected, how long that information will be stored, and with whom the information may be shared.

Second, most data aggregators collect customer information using outdated "screen scraping" methods. This puts sensitive customer financial information at risk and limits the ability of consumers to exercise informed consent about what, when, and how information is shared. Screen scraping also places enormous demands on the infrastructure of financial institutions, increasing cost and operational risk to the financial institutions.

Third, data aggregators currently are not subject to any comprehensive regulatory regime to ensure that their systems for maintaining the privacy and security of the consumer information they hold is robust and effective. Thus, unlike banks and broker-dealers, which are subject to regular cyber-security reviews by federal regulators, there is no governmental body charged with ensuring that data aggregators have and maintain strong cyber-security programs. This puts the sensitive information of millions of U.S. consumers, as well as the U.S. financial system, at risk.

As discussed further below, PNC supports several actions to address these deficiencies in the current system. First, we believe it is critical for data aggregators to shift their information collection practices away from "screen scraping" to secure Application Programming Interfaces (APIs) supported by tokenized authentication. Doing so will allow the secure distribution of data without the sharing of personally identifiable information. APIs also will enable *consumers* to control the amount of financial information they share with financial apps and data aggregators.

PNC has already signed a secure data access agreement with one of the largest data aggregators, and we and other banks are in active discussions with numerous data aggregators and other interested parties to implement APIs and tokenized access. We also support the efforts of FDX and The Clearing House to develop API standards and a utility, respectively, that

would facilitate the migration of data aggregators to APIs and tokenized access. In the meantime, we have taken important steps to protect the security of our customers' most sensitive information that is often used to facilitate account takeovers and fraud.

The Bureau can play a positive role in encouraging rapid industry migration to this new, more secure and transparent model for customer-authorized data sharing, which is necessary if the principles the Bureau outlined for Consumer-Authorized Financial Data Sharing and Aggregation in 2017 (the "2017 Principles") are to be achieved. At the same time, the Bureau, together with other policymakers, should consider how best to ensure that the millions of consumer records held by data aggregators are secure from cyber-attacks. We look forward to working with you and others on these consumer protection priorities.

II. Obscure and Insecure—The Current State of Data Aggregation

Financial institutions, financial technology applications and data aggregators all have different roles in the current financial ecosystem. Data aggregators enable financial applications to link customer bank accounts to their platform, providing account and transaction details, balance and identity information. Data aggregators power financial technology applications like Venmo, Mint and Acorns which offer various financial services and tools – person-to-person payments, budgeting and saving – that allow customers to manage their personal finances. In this digitally driven financial environment, it is critical that customers authenticate and provide access to their financial data from their financial institution to these financial data parties in a convenient, secure and reliable manner.

A. Consumers Lack an Understanding of How Their Information Is Being Collected and Shared

Consumer authorization plays an important role in giving consumers control of their personal and financial information. Prior to using a digital product or service, customers generally must agree to the financial app's Terms of Use language and, where applicable, Privacy Policy. Similarly, customers are often presented with a link to the data aggregator's Terms of Use when linking the financial app to their financial account. Ostensibly, data aggregators obtain a consumer's authorization to access the consumer's information at her financial institution through the Terms of Use the aggregator or a supported app provides the consumer.

In practice, though, consumers in many cases are not provided clear and conspicuous disclosures about the type and amount of financial information that may be collected by a data aggregator when the consumer signs up for a financial app, or how that information might be used or shared by the data aggregator. In fact, some practices of data aggregators or the apps that they support appear designed to confuse consumers about who is collecting information from them and how that information will be stored.

For example, in some cases the login and/or authorization screen used by a financial app or aggregator is designed to resemble the consumer's banking institution by using the bank's coloring, stylized font and logo. This can easily confuse the consumer, who may assume that the application is sponsored by their bank or that they are providing their bank account login and passwords to their bank, rather than a nonbank financial app or data aggregator. Some applications likewise state that they "never store bank login credentials", but fail to inform consumers at the same time that such credentials may be stored by a data aggregator acting on behalf of the financial app.

In addition, while the relevant Terms of Use and Privacy Policy may broadly authorize the app (or a data aggregator acting on its behalf) to access information at the consumer's financial institution, the customer in many cases is *not* required to read the document. In some cases, they do not even have to click on the link to the document to proceed with establishing the account. Even if a consumer were to click on the link to the Terms of Use, the authorization for the data aggregator to obtain the consumer's financial information typically is buried in fine print, and the wording used is difficult for the average user to understand. In our view, this is not the type of informed consumer authorization and consent contemplated by the Bureau's 2017 Principles.

As a result, it is not surprising that a significant number of consumers do not fully grasp the extent to which their information is being accessed, shared, stored and retained – or by whom – when they use financial apps. A November 2019 survey conducted by The Clearing House (TCH), a banking association and payments company that supports industry collaboration and development, found that 80% of financial app users are not fully aware that apps or third parties may store their bank account username and password, and more than 80% are not aware that apps may use third parties to access consumers' personal and financial information.[1]

[1] The Clearing House, Consumer Survey: Financial Apps and Data Privacy, November 2019.

Moreover, only 11% of consumers claimed to have read and understood the terms and conditions presented by the financial app governing its services. This is alarming given how financial apps have become a key component of the financial ecosystem and consumers' day-to-day lives. In fact, 54% of U.S. banking consumers use financial apps to engage in personal financial management.[2]

Simply put, we believe most consumers do not understand that, by signing up to use a financial app, they may be authorizing a data aggregator to access *all* of the consumer's sensitive financial information that may appear on the consumer's online banking page at her financial institution—even information that may be completely unrelated to the service provided by the financial app. Most consumers also do not realize that the aggregator may continue to obtain this information even if the consumer stops using or deletes the financial app. Rather, to cease the aggregator's collection of information, the consumer must affirmatively revoke the authorization provided to the aggregator. However, the means of doing so often are not clear or easy. The current state of consumer authorizations, therefore, seems fundamentally at odds with the Data Scope and Usability and Control and Informed Consent principles within the 2017 Principles.

These concerns were highlighted by Lauren Saunders, Associate Director of the National Consumer Law Center, in her recent testimony before the U.S. House of Representatives Committee on Financial Services Task Force on Financial Technology:

> Consumers may believe that they are providing access only for purposes of a narrow range of transactions or services. But the third party can gain access to a wealth of information about the consumers' income, where they shop and what they buy, their spending patterns and a variety of other sensitive personal information. Some services harvest this information for marketing purposes and even at times may reserve the right to share it with or sell it to other parties that the consumer does not contemplate. …
>
> Consent alone is also insufficient because the vague privacy policies that consumers receive do not give them any real idea of how their information may be used. Consumers should not be expected to decipher privacy policies to hunt for inappropriate uses. Consumers also may have used a service once or twice to try it out and long forgotten about it, not realizing their information is still being collected and potentially disseminated. While consumers have the right to limit data sharing with unrelated third

[2] The Clearing House, Consumer Survey: Financial Apps and Data Privacy, November 2019.

parties, they are often unaware of those rights, and may have difficulty knowing how to change their preferences.[3]

The TCH 2019 consumer survey confirmed that, once consumers realize the scope of information that third parties have access to through their use of financial apps, they share these concerns. Indeed, 68% of consumers expressed discomfort with the level of access third parties have to their financial information once they learned about these practices.[4]

B. Current Screen Scraping Practices Are Outdated and Insecure

"Screen scraping" refers to the automated process of collecting the content that appears on a website. In the world of consumer-permissioned data sharing, data aggregators predominately use screen scraping to retrieve data from online banking websites, store this information, and share it with a financial application for storage and display within the application.

Screen scraping typically relies on "credential-based access," meaning consumers are required to share their online banking login credentials (e.g., usernames, passwords, and any challenge questions and answers) with the financial app and/or its data aggregator partner. The data aggregator or financial app then stores these credentials and uses them to routinely access the consumer's online banking website. Through credential-based access and screen scraping, the data aggregator or app is able to read any data elements that are visible on the financial institution's online banking website for the consumer, including the consumer's account balances, a list of recent financial transactions (including where purchases were made), customer account numbers (if displayed), individualized offers and terms for additional financial services products, the consumer's contact information, and other sensitive information about the consumer.

The current screen scraping practices of data aggregators suffer from three inherent flaws. First, this method does not allow for consumer control over the amount of data they share with third parties, and there is no way to ensure that the information "scraped" and maintained by the aggregator does not go beyond what is necessary for the financial app to deliver the services

---

[3] National Consumer Law Center Testimony before the U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES Task Force on Financial Technology, "Banking on Your Data: The Role of Big Data in Financial Services," November 21, 2019.

[4] National Consumer Law Center Testimony before the U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES Task Force on Financial Technology, "Banking on Your Data: The Role of Big Data in Financial Services," November 21, 2019.

sought by the consumer. Indeed, as noted above, there is the risk that the data (and the consumer's credentials) may continue to be collected and maintained by the aggregator or financial app even after the consumer ceases using the financial app.

Second, screen scraping, and the credential-based access on which it is based, creates opportunities for bad actors to gain access to a consumer's accounts at a financial institution and commit fraud, or even take over the consumer's account. As FinCEN Director Kenneth A. Blanco noted in his speech at the Federal Identity (FedID) Forum and Exposition on September 24, 2019:

> FinCEN has … seen a high amount of fraud, including automated clearing house (ACH) fraud, credit card fraud, and wire fraud, enabled through the use of synthetic identities and through account takeovers via fintech platforms. In some cases, cybercriminals appear to be using fintech data aggregators and integrators to facilitate account takeovers and fraudulent wires. By using stolen data to create fraudulent accounts on fintech platforms, cybercriminals are able to exploit the platforms' integration with various financial services to initiate seemingly legitimate financial activity while creating a degree of separation from traditional fraud detection efforts. Some criminals are also monetizing stolen credit card information through fraudulent merchant accounts to charge victims' cards or are simply creating fraudulent user accounts on fintech platforms as part of identity theft or synthetic identity fraud.[5]

These concerns echoed an earlier Investor Alert issued by the Financial Industry Regulatory Authority (FINRA) on March 29, 2018, which warned consumers of the risks presented by the credential-based access currently used by data aggregators:

> Many customers value the convenience of financial data aggregation and appreciate having a single snapshot of multiple accounts. But sharing security credentials for financial account information can come with some risks. Foremost, you can potentially expose yourself to privacy and security risks. These include potential vulnerability to cyber fraud, unauthorized transactions and identity theft. A key risk is that the aggregators could be storing all consumer financial information or security credentials in one place, creating a new and heightened security risk for consumers.[6]

Third, screen scraping can divert the cyber-security resources of regulated financial institutions away from preventing unauthorized access by criminals and nation-states. This is because it may be difficult for a financial institution to distinguish "legitimate" data aggregator log-ins from

---

[5] Prepared remarks of FinCEN Director Kenneth A. Blanco, delivered at the Federal Identity (FedID) Forum and Exposition, titled, "Identity: Attack Surface and a Key to Countering Illicit Finance" in Tampa, Florida on September 24, 2019.

[6] Know Before You Share: Be Mindful of Data Aggregation Risks, Investor Alert, FINRA, March 29, 2018.

illegitimate traffic, a problem compounded by the fact that some data aggregators have actively mimicked the digital profile of threat actors or worked to bypass security controls used by financial institutions to authenticate customer log-ins (such as by auto-populating the security questions posed when a new connection is sought to be established with a consumer's account). As the Basel Committee on Banking Supervision found, "Screen scraping or reverse engineering can undermine a bank's ability to identify fraudulent transactions, as banks cannot always distinguish between the customer, data aggregator, and an unauthorised third party that is logging in and extracting sensitive data."[7]

C. Data Aggregators Currently Are Not Subject to Systematic Cyber-Security Oversight

Banks are subject to regular cyber-security examinations by the Federal banking agencies. These examinations are designed to ensure that banks have robust systems and controls to maintain the security of consumer financial information and protect such information against unauthorized access. The Federal Financial Institutions Examination Council (FFIEC), which includes the Bureau, has published a detailed handbook to guide these examinations.[8] Likewise, broker-dealers registered with the Securities and Exchange Commission (SEC) are subject to cyber-security examinations by the SEC. In fact, the SEC's Office of Compliance Inspections and Examinations has made cyber-security an area of focus in recent years and recently published a report on its cyber-security examinations at broker-dealers, as well as other institutions supervised by the SEC.[9]

Nonbank data aggregators, though, are not subject to systematic and comprehensive federal oversight for cyber-security. As FINRA noted in its March 2018 Investor Alert:

> Many data aggregators may operate under limited regulatory oversight and are not subject to the same regulation that registered financial institutions are subject to, particularly in areas of data privacy and security.[10]

Thus, while large data aggregators maintain the sensitive financial information of millions of U.S. consumers — perhaps even more than held by the largest banks — there is no framework for

[7] Basel Committee on Banking Supervision, Report on open banking and application programming interfaces, November 2019.

[8] FFIEC IT Examination Handbook, available at https://ithandbook.ffiec.gov/.

[9] OCIE, *Cybersecurity and Resilience Observations*, Jan. 2020, available at https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

[10] Know Before You Share: Be Mindful of Data Aggregation Risks, Investor Alert, FINRA, March 29, 2018.

the federal oversight of these entities to ensure that they have and maintain the systems and controls necessary to protect that information from unauthorized access and theft. This puts consumers and the financial system at risk.

III. The Path Forward – Enabling Informed Customer Consent and Information Security

Fortunately, there is a path forward that will enable informed customer authorization and facilitate the secure exchange of information when properly authorized. Specifically, the widespread implementation of application programming interfaces (APIs) and tokenization would be an important step in bringing the entire financial ecosystem more in line with the Bureau's 2017 Principles.

Simply stated, APIs enable direct, real-time communication between different software systems. For instance, ridesharing apps communicate simultaneously with Google Maps and the user's choice of payment method, allowing a customer to use one app to hail a ride to a specific location and pay for it. APIs provide a dedicated data portal where consumer-permissioned data is provided directly from a database containing the required permissioned data elements.

APIs have multiple benefits compared to the credential-based access and screen scraping currently employed by data aggregators. First, APIs can give consumers more control over what aspects of their financial data is shared. For example, through the use of an API, the customers of a financial institution can limit the types of data shared with a financial app or data aggregator to just the information needed to obtain the service desired. Thus, a consumer that signs up for a payment, financial management, or tax preparation app could authorize the sharing of only the data needed to support that service, limiting risk to the consumer and giving consumers greater control over what kinds of information they share. No longer would a data aggregator be able to obtain, on an ongoing basis, *all* of the information on a consumer's online banking portal simply because the consumer used a payment app once to send a payment.

APIs also permit financial institutions to directly authenticate consumers that are seeking to connect their financial institution accounts to a financial app or its data aggregator intermediary. This facilitates the application of the financial institution's fraud detection and authentication tools, thereby reducing the potential for fraud and account takeover.

Additionally, APIs may be used in concert with tokenized access, which obviates the need for the consumer to provide their sensitive online banking credentials to data aggregators and financial app developers. With tokenized access, a consumer is taken to their financial institution during the app enrollment/sign-up process to log in and authenticate with the bank, review what data is being requested and permission which accounts they would like to grant such access. A token, or string of characters up to 1,000 characters long, is then generated and sent to the data aggregator or financial app. Then, for data retrieval, the token is presented to the consumer's financial institution through an API so that the consumer's permissioned data elements can be shared with the data aggregator or financial app. Tokens contain no personally identifiable information, only work with the single financial institution the consumer uses and often expire in a short period of time.

APIs and tokenized authentication make consumer-permissioned data sharing easier, more accurate and more secure. Not only do they remove sensitive credential sharing and provide a dedicated data access portal for data access providers and companies not affiliated with a consumer's financial institution, but they also lay out the rules for how to request data and what data will be returned.

In light of the risks of screen scraping as a method of access, the UK and the European Union have issued rules that will eventually ban the use of screen scraping for the purpose of accessing payments account data and require the use of a dedicated interface based on APIs or a modified customer interface. Providers have a transition period that will last until March of this year during which they may continue in some circumstances to use screen scraping, but from March onward, fintech platforms will be required to comply with new strong customer authentication (SCA) standards to provide access to account data and payment functionality.

PNC, together with The Clearing House, is taking several steps to speed the necessary transition away from credential-based access and screen scraping in the U.S. and toward an API-supported ecosystem of informed customer-permissioned information sharing. We have already signed a secure data access agreement that enables the use of an API and tokens with one of the largest data aggregators in the United States. We are currently in discussions with

numerous other data aggregators to implement more secure data exchange practices, including the implementation of APIs.

In addition to these bilateral activities, we are strong advocates for an industry-wide transition to APIs and tokenization, which we believe will improve efficiencies and create an overall safer, more reliable consumer-permissioned financial data access ecosystem. PNC Bank and TCH, of which PNC Bank is a member, are founding members of Financial Data Exchange (FDX), a non-profit, technical-standards body whose mission is to unify the financial industry around a common, interoperable, royalty-free standard for secure and convenient consumer and business access to their financial data – namely the FDX API. FDX is a subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC).

FDX's members include financial institutions, fintech companies, consumer advocacy groups, financial data services companies and major financial industry groups involved in consumer-permissioned financial data access. FDX believes there are five core principles that should govern the consumer-permissioned financial data access ecosystem.

1.) Control: Consumers should be able to permission their financial data for services or applications.
2.) Access: Account owners should have access to their data and the ability to determine which financial data parties will have access to their data.
3.) Transparency: Individuals using financial services should know how, when, and for what purpose their data is used. Only data that is required to provide such services should be shared with the organizations providing the services.
4.) Traceability: All data transfers should be traceable. Consumers should have a complete view of all financial data parties that are involved in the data-sharing flow.
5.) Security: Financial data parties need to ensure the safety and privacy of data during access and transport and when that data is at rest.

In addition to an industry standard API, FDX is currently working on standards for secure authentication and authorization, a certification program, and user-experience, consent guidelines and best practices. FDX has convened industry stakeholders to achieve the shortest critical path to realizing the benefits of secure, consumer-permissioned data sharing and encouraging the widespread adoption of the FDX API. FDX and its members believe that the

widespread adoption of an industry standard API will benefit consumers through consistent and secure access to the data they need to make better financial decisions, improve their financial lives, and use the financial applications they choose.

TCH and its member banks also have developed a model agreement to expedite and streamline the process for financial institutions and financial application developers to better serve joint customers. Further, TCH is working to streamline and accelerate required compliance processes to help evaluate the safety and security of financial apps and data aggregators through a common registration and assessment process.

We believe this Symposium is an important step in accelerating the migration to tokenized data access via secure APIs when sharing consumer financial information. By educating policymakers on the dangers posed by the current credential-based, screen scraping practices of data aggregators, we can solidify the momentum necessary to move data aggregators away from these practices. As a nation, we should aim to eliminate all credential-based screen scraping information collection by data aggregators as quickly as possible. Active engagement by the Bureau and other government agencies can help ensure that the financial system as a whole expeditiously moves away from screen scraping and toward APIs and tokenized access.

IV. Cyber-Security Oversight of Data Aggregators

While APIs and tokenization will, if implemented, help make information shared *in the future* more secure, these technologies will not address the potential security risks associated with the vast quantities of sensitive customer information that has already been collected and stored by data aggregators. It is difficult to estimate the quantity of data held by data aggregators, of which there are approximately 120 in the United States. According to one report, data aggregator Acxiom provided up to 3,000 attributes on 700 million people in 2017, and by 2018, it collected 10,000 attributes on 2.5 billion consumers.[11] While these figures are difficult to verify, we can be certain that the largest data aggregators hold the sensitive financial information of millions of U.S. consumers.

[11] https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.

We believe it is important for all data aggregators that have access to, or maintain, a significant volume of customer financial information to be subject to regular, comprehensive information security examinations by a federal agency with expertise in this area, just as banks and SEC-registered broker-dealers are today. Threat actors, including cyber-criminals and nation states, are adept at finding the "weak link" within the financial ecosystem, and then exploiting that weakness to obtain access to consumer financial information that can be used to divert funds or disrupt the U.S. financial system. Indeed, as FinCEN Director Blanco noted in his September 2019 speech, cyber-criminals have already exploited the connections maintained by data aggregators with financial institutions to commit fraud and account takeover. We should not wait until the first confirmed, large-scale intrusion of a data aggregator to put in place a framework for the federal oversight of these firms' information security practices. We would be pleased to work with the Bureau, data aggregators and other interested parties to achieve this important objective.

V. Conclusion

PNC appreciates the opportunity to participate in this Symposium and other discussions regarding the current state of practice and regulation regarding data aggregators and customer-authorized information sharing. We support our customers in securely connecting their PNC accounts to the apps of their choice. However, protecting our customers and the personal and financial information that they entrust to us is, and will remain, a top priority for PNC. For these reasons, we strongly support the migration of connections between financial institutions and data aggregators to secure APIs that can support informed customer consent and the secure transmission of properly permissioned information.

We would welcome the opportunity to continue discussions with the Bureau and other interested parties to achieve this goal and, thereby, promote safety and security for consumers and the financial services sector.