FINANCIAL SERVICES

Building a consumer-first framework for modern technologies

PLAID

I. INTRODUCTION

Over the past several years, a new class of financial services applications has emerged that gives power and choice to the consumer.

These applications have improved the lives of millions of Americans, allowing them to gain control of and easily manage their financial information, by delivering new services and providing modern, consumer-friendly experiences. The impact these companies have had in a short amount of time has been significant—consumers rely on many of them on a daily basis. And the investment environment, where funding to the financial technology sector tripled from $4 billion in 2013 to more than $12 billion in 2014, suggests further opportunity for progress. (See ***Snapshot of the financial technology sector***.)

Yet none of these businesses could exist without a category of enabling technology companies called third-party data aggregators. These companies build the technological bridges that connect applications with established financial institutions, allowing consumers to access their information in the ways that work best for them.

Third-party aggregators give consumers financial choices

Aggregators are therefore key drivers of consumer choice and flexibility. Fundamentally, aggregators are technology- and security-centric businesses that facilitate new services while protecting consumers' financial data. By providing the platform that enables any bank account to work with any financial application, aggregators help consumers explore and benefit from new financial services. In this way, third-party aggregators give consumers financial choices that they would not otherwise have. And because they put security first, aggregators help ensure that this freedom is backed by the best protections possible.

As with any period of dramatic innovation, progress in financial services has raised difficult questions about the best way for traditional financial institutions—which sit at the heart of this ecosystem—and newer technologies to collaboratively deliver services to the consumer. At the root of these questions is whether and how consumers should be able to access their data, and the role aggregators ought to play in providing them this functionality.

These issues will take time to properly address. In the meantime, however, market uncertainty could dampen innovation and disrupt the way many consumers access the financial applications they have come to rely on. Without cooperation among key players in the financial and technology industries, many consumers could find themselves without the agency to

SNAPSHOT OF THE FINANCIAL TECHNOLOGY SECTOR

Despite the changes that have come to the financial industry, banks remain at the core of financial services. According to the Federal Reserve, 92% of Americans maintain at least one bank account.

Indeed, most of the emerging financial technologies are not designed to compete with and cannot displace banks. Instead, they provide complementary services and functionalities that enhance customer satisfaction. By helping consumers save more money, cut expenses, and invest—savings consumers then deposit into their primary bank accounts—financial technologies contribute to a more knowledgeable and sophisticated market that benefits the system overall.

The functionalities provided by legacy financial institutions and those supplied by upstarts are both essential. But it is only by working together that consumer expectations can be met. While banks' core competencies lie in finance, the core competencies of financial technology businesses are rooted in technology. Aggregators serve as the link between the two, making it possible for consumers to enable third-party access to their bank data in a secure way and for financial technologies to bring new functionalities to market.

own, access, and transfer their data.

As answers evolve and financial technology companies continue to fill gaps in the market, it is essential to build a secure, collaborative system that empowers consumers and enriches their choices.

This paper puts forward three recommendations to guide the development of an inclusive financial services ecosystem:

- Protect the ability to innovate and compete;
- Grant consumers control over their personal financial information; and
- Promote better security for personal financial information.

The leadership of traditional financial institutions, financial technology companies, consumers, and policymakers will shape the financial landscape. Addressing the inevitable challenges in a way that empowers consumers everywhere is an objective that should be shared by all.

II. CONSUMER CHOICE REQUIRES A RICH LANDSCAPE FOR INNOVATION

Consumer choice is strengthened by the existence of a range of options. Consumer agency therefore depends on a thriving financial technology landscape that supports innovation and product diversity.

Over the past decade, this landscape has begun to take shape through the democratization of services and user-friendly functionalities that aim to increase consumers' satisfaction with and overall participation in the financial system. These include personal financial management tools, modern payroll systems, mobile-optimized account management interfaces, and account security and fraud prevention services.

Specifically, nonprofits like EARN use aggregators to automatically match savings that low-income households set aside in their accounts. Companies like Digit rely on aggregators to underpin its automated savings solutions, making it easier for U.S. consumers—many of whom have less than $1,000 in their bank accounts and struggle to manage expenses—to start saving money. Businesses like Even turn to aggregators to provide insight into transaction flows to suggest improvements to spending habits. Applications like Betterment and Wealthfront, which were some of the first companies to democratize investment advice, rely on aggregators to draw insights from rich transaction data.

What's more, consumers who benefit from aggregators' technologies are not merely individuals. Owners of small companies rely on software that leverages aggregator data to run their businesses. For example, accounting software like Xero uses aggregators to make it easier to link account information and manage finances. Modern approaches to payroll like Gusto and Justworks turn to aggregators to seamlessly connect employee accounts for direct deposits.

These and other services make it easier for people to control their financial lives. They are the result of a healthy, competitive ecosystem that drives innovation by encouraging companies to develop better functionality, deliver seamless user experiences, and focus on pockets of the market that might not otherwise get attention.

This innovative environment is made possible by data aggregators. Their application programming interfaces, or APIs, connect traditional financial institutions and financial technology applications that seek to access and utilize data. (See ***How third-party data aggregators have evolved***.)

By providing this core platform, data aggregators effectively democratize financial services—so smaller upstarts can compete and consumers can access these useful services and improved functionalities.

With some 20,000 financial institutions in the United States alone, the level of interoperability

HOW THIRD-PARTY DATA AGGREGATORS HAVE EVOLVED

Data aggregation technology that links banking data with other platforms has been in use since the mid-1990s.

Twenty-five years ago, the previous generation of data aggregators implemented screen-scraping technologies to facilitate access to consumers' financial information. At the consumer's direction, screen-scraping data aggregators work by collecting visual screen data from the web portal for a consumer's bank account and transmitting that data to applications.

As the financial sector has evolved, data aggregation technology has undergone a generational shift. Today, aggregation technology makes data accessible in a more secure and convenient way.

Data aggregators also provide the tools that the financial technology sector relies on to bring new services to market. Instead of requiring companies to build multiple, discrete linkages with each financial institution—which would likely be prohibitive given the sheer number of financial institutions in the United States, let alone the different technology platforms used across the system—data aggregators provide a single point of contact for securely accessing data.

In this way, aggregators do the work of building and maintaining thousands of integrated connections with individual banks—helping existing financial services companies focus on developing and delivering their core products and services, as well as lowering barriers to entry for new firms.

This progress has created an inflection point in the development of this ecosystem, requiring financial institutions and third-party aggregators to clarify their roles and solidify their partnerships.

that aggregators enable is essential for this ecosystem to not only thrive, but simply to exist.

III. CONSUMERS SHOULD CONTROL ACCESS TO DATA

Consumers normally give permission to aggregators to access account, transaction, and user data. This data may include the type of account, name of account, and account and routing information; amount spent, name of merchant, and merchant categories; and the account owner's name and address. In general, this data is provided in a tokenized and encrypted format so that only necessary parties have access.

Consumers should expect reliable access to their data through applications they have authorized. But current market dynamics prevent consumers from realizing these reasonable performance expectations. In November 2015, for example, *The Wall Street Journal* reported that customers of some banks were unable to access their data through services they had authorized for several days.

Such situations frustrate and inconvenience individuals who have granted access to and depend on various financial applications to manage their daily finances. They impact the small businesses and innovators whose services rely on consumer access and aggregators. And they also create market uncertainty that may discourage innovators from investing resources into new products and services.

A compelling parallel exists in the healthcare industry, whose evolution illustrates the importance of protecting consumer choice and providing market confidence. As the healthcare industry transitioned to electronic medical records, questions surrounded the free exchange of patient health information and practical considerations arose around interoperability. However, with cooperation among healthcare providers, records companies, and other experts, the industry worked to enable protected exchange of information at the behest of patients. This not

only gives consumers more freedom to find the best care, but also encourages providers to deliver superior services at affordable prices.

The need to protect consumer access to data and innovation within financial services is not unique to the United States.

Earlier this year, the European Union Parliament adopted a framework that recognizes the important role aggregators play and the need for meaningful protections for consumer access to data. The United Kingdom is addressing these topics by bringing together government officials, industry stakeholders, consumer advocates, and open data experts to develop new standards to reconcile consumer control of their own data with business, security, and privacy concerns.

As technology-first businesses, aggregators are ideally positioned to be strong partners in pursuit of maximum systemic security and risk mitigation

In the United States, various players have begun collaborating to increase efficiencies and clarify uncertainties. In fact, some banks have embraced data aggregators as a means to modernize their own services and compete more effectively against their peers. These banks use aggregators to power opportunities for growth and facilitate the provision of additional services or functionalities, such as mobile-optimized bill pay, streamlined account opening, efficient credit card payments, easy payroll direct deposits, and comprehensive loan services. Working closely with aggregators reaps benefits while avoiding onerous, expensive, and distracting integration requirements.

Yet no consensus currently exists regarding the optimal relationship between financial institutions and the data aggregators that underpin innovation in the sector. Uncertainty surrounding the relationship between financial institutions and aggregators—and, by extension, the innovative services they power—only shortchanges consumers. It is imperative that clarity be reached, driven by consumers' right to access and control their own data.

IV. STRONG PARTNERSHIPS SUPPORT SECURITY

Any conversation about access to personal financial data quickly turns to security.

Indeed, many financial institutions argue that potential security issues underpin concerns related to third-party access to consumers' account information.

This is a worthy priority. Strong security is in the best interest of all parties involved in the financial ecosystem. With financial services in the crosshairs of increasingly sophisticated cyberattacks—most will remember the historic data breach at JPMorgan Chase in 2014, in which the personal information of more than 100 million customers was stolen—security must be top of mind.

As technology-first businesses, aggregators are ideally positioned to be strong partners in pursuit of maximum systemic security and risk mitigation. Aggregators are able to put forward—and implement—security best practices in real-time. Already, they implement advanced, layered levels of security that are commensurate with the capabilities of traditional financial institutions. (See ***Aggregators are on the leading edge of security***.)

Moreover, as gatekeepers in the financial technology system, aggregators can ensure that any party accessing, using, or storing personal financial information meets uniform minimum security standards.

This progress provides end-to-end encrypted authentication to every consumer—not just those who happen to bank with select partners.

Instead of having consumers share their banking credentials to permission multiple applications and platforms to access financial data—which results in a higher risk of their accounts being breached, misused, or abused—aggregators can serve as a secure intermediary to minimize exposure.

Many aggregators are actively working on efforts to build a more secure system. Aggregators can eliminate the need for consumers to manually enter account and routing numbers when linking bank accounts to other platforms. This not only creates added efficiency, it also reduces another common point of vulnerability.

Additionally, some aggregators are working to eliminate the use of credentials, instead working directly with banks to increase security while preserving developer-friendly approaches. This provides financial applications with the functionality they need to serve consumers—but without direct access to consumers' credentials or accounts.

AGGREGATORS ARE ON THE LEADING EDGE OF SECURITY

As technology businesses, data aggregators drive innovations that strengthen the security of personal financial information. They attract top engineering talent and are not constrained by legacy technologies, bureaucratic budget reviews, or outdated infrastructure. These advantages have allowed aggregators to build modern, nimble security systems that traditional financial institutions are less well positioned to pioneer.

Modern aggregators utilize layers of security technologies to keep personal information protected. These measures include forced two-factor authentication, tokenization of sensitive data, mechanisms for consumers to revoke control, and client-side encryption.

For example, instead of storing sensitive credentials, aggregators apply tokenization. Where financial institutions lack two-factor authentication—which has quickly become the standard in the security industry—aggregators have the potential to enforce it.

As such, long-term partnerships between traditional financial institutions and technology companies strengthen security best practices. By sharing expertise, a cooperative financial services industry could protect consumers in a way that better reflects the vital need to maximize the security of sensitive personal financial information.

V. RECOMMENDATIONS FOR BUILDING A SECURE SYSTEM DRIVEN BY CONSUMER CHOICE

A robust financial system should ensure that people have choices in how they interact with and understand their finances, can control their personal financial information, and feel confident that their decisions are supported by the best security possible.

Maximizing the empowerment of consumers and protection of personal information requires a strong partnership between traditional financial institutions, data aggregators, and financial applications.

As such, three key principles should guide the development of the financial services ecosystem that legacy financial institutions, data aggregators, startups, policymakers, and regulators must work together to build.

These principles are:

Protect the ability to innovate and compete. Innovation in the financial services industry benefits consumers, as consumers cannot be empowered if they do not have choice. New technologies offer consumers unprecedented opportunities to overcome traditional barriers in financial services with secure, user-friendly, affordable options.

As such, the ability for developers and

entrepreneurs to bring new services to market must be protected, as should their ability to access information and tools that data aggregation technologies are designed to provide. Anti-competitive practices or intentional barriers to entry should be identified and disallowed.

Consumers who choose to bank at small institutions should not be inadvertently denied access to financial technology products and services

In the same vein, new protocols should be adoptable by both large and small financial institutions. Any future system must preserve the ability of small community banks and credit unions to compete. Specifications and standards with large implementation costs unfairly favor larger players over smaller institutions that may lack such resources. Consumers who choose to bank at small institutions should not be inadvertently denied access to financial technology products and services. To protect innovation and consumer choice, it is essential to create a model that is inclusive of every financial institution with which a consumer chooses to bank.

Grant consumers control over their personal financial information. Empowered consumers should have access to—and control over—information across all of their accounts.

Consumers should have the ability to deploy their own information in order to benefit from new services or improved functionalities.

Additionally, they should expect transparency in terms of how financial institutions, aggregators, and applications are accessing and using their data. Consumers should also be able to easily revoke permission to any platform accessing their data. And they should have the right to opt out of their data being shared, even if it can no longer be linked to them.

Promote better security for personal financial information. Cooperation among stakeholders stands to strengthen the overall security of the system. Aggregators are a neutral party, without competitive self-interests, that can play a key role in developing and enforcing uniform security standards in partnership with developers and traditional financial institutions.

Financial institutions should formally recognize trusted third-party data aggregators. In turn, aggregators should help banks implement uniform minimum security standards among third parties accessing personal financial information.

Finally, the use of tokenization should be utilized more broadly in the future to minimize the exposure of credentials, account numbers, and routing numbers throughout the system.

VI. CONCLUSION

Traditional financial institutions and firms in the financial technology sector tend to agree on several key points. The interests of the consumer should be put first. Maximizing security in the financial system is an urgent priority. And leadership will be required to develop a clear framework to accomplish these important objectives.

The United States' breakthroughs in the healthcare system suggest that progress in financial services is within reach. Additionally, the attention these issues have received in the European Union and United Kingdom underscores the importance they play in promoting innovation and competition.

The United States should follow suit in designing and implementing a framework that guides the continued evolution of the financial services sector in a way that is balanced, secure, and competitive—and puts the consumer first.

A strong partnership between established financial institutions and technology firms will be critical to the success of any such effort.


PLAID