February 21, 2017

VIA ELECTRONIC SUBMISSION
Monica Jackson
Office of the Executive Secretary
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

Dear Ms. Jackson:

My name is Bill Harris, CEO of Personal Capital and former CEO of Intuit and PayPal. This letter is in response to the Consumer Financial Protection Bureau’s Request for Information Regarding Consumer Access to Financial Records. Our response can be summarized in four points:

• Our current ecosystem for data aggregation is not broken. It functions at huge scale with high security connecting 14,000 financial institutions with tens of millions of consumers.

• One reason it functions so well is the mix of methods used to collect the data, depending upon each circumstance. Any attempt to impose a single “standard” would disrupt the collaborative process that’s been built bank-by-bank over twenty years, and rob the system of its inherent resiliency.

• OAuth, the “standard” recently proposed by some banks and brokers, would restrict consumer access and seriously weaken the cybersecurity protecting the money in consumer bank accounts. Some banks like OAuth because it would switch control of the data from consumers to the banks.

• The system is not broken. Let’s be careful not to break it.
Digital Financial Tools for Consumers

Personal Capital is a financial advisory firm that provides free online tools using aggregated data to help consumers understand and improve their financial life. A few of those tools are described here:

• **Digital Dashboard.** A comprehensive summary of a family’s entire financial situation, including bank accounts, credit card accounts, investment accounts, loan and mortgage accounts and a variety of other accounts from any of the 14,000 financial institutions in the U.S. The average household has 15 different financial accounts.

• **Transaction Monitor.** A real-time record of all your transactions in all your accounts at all your financial institutions. Monitoring transactions on a regular basis is the best available means for protection against errors, hacking or fraud.

• **Retirement Planner.** A complete financial planning application that uses your current assets and liabilities and your historical income and spending to create an instant fifty-year projection of your financial health into retirement. This is the most important thing for every American family to do: plan and prepare for their financial security. Aggregated data is used to populate this financial planner.

• **Fee Finder.** An automated analysis tool that finds all fees charged on each account, including hidden fees, late penalties, overdraft charges, commissions, advisory fees and fees embedded in mutual funds.

• **Investment Checkup.** A health report on your investments identifying problems such as poor asset allocation, inappropriate investments and high fees. The checkup even uses the underlying holdings of each mutual fund to calculate your true exposure to asset classes, geographies, sectors and individual stocks.

• **401k Analyzer.** An online tool that assesses the allocation, holdings and fees in your 401k or 403b accounts and projects the amount that fees will subtract from your retirement account over the next thirty years. Most 401k providers are brokers, not fiduciaries, so they can sell whatever makes them the most money, without regard for your best interest. Fees on retirement accounts are stubbornly high – sometimes as high as 2% per year. And an AARP study revealed that 71% of employees in retirement plans believe there are no fees at all. This is one reason it’s so important for consumers to have easy access to their data and to tools that help them make sense of their data.
• **Stock Option Tracker.** A tool that tracks the daily value of unexercised stock options. 36% of Americans who work at companies with stock have stock options, and the value of options is often a significant part of their net worth.

Most Americans are living unexamined financial lives. They don’t know what’s happening to their money. If you have to go from website to website to collect all your financial information, it’s simply too cumbersome for most people to attempt. Even with the data, many people lack the time or expertise to make sense of it all.

Yet a complete view of a family’s financial situation is obviously necessary to provide meaningful financial advice, whether that advice is provided with digital tools, human advisors, or the combination of both. And easily-available aggregated data – the customer’s own data – is a necessary condition.

**Financial Data Aggregation**

Financial data aggregation has been available for twenty years, and tens of millions of American consumers now rely upon it. There has always been tension between big banks and data aggregators, because data aggregation loosens the banks’ control of their customers’ data and the use of that data. Over the years, there have been occasional instances of bank resistance, which have generally been quickly withdrawn when the banks’ best customers complained that they wanted access to their own financial records.

Today’s resistance comes in a subtler form: A few big banks are proposing a new authorization framework (“OAuth”) by which to provide the data, because this framework switches control over the data from the customers to the banks.

To understand why this is backwards, remember that an aggregator is not a third party, it’s an agent of the first party – the customer. In the desktop software era, the customer used software like Quicken to collect her data. In the cloud software era, the customer uses software like Personal Capital to collect her data. Either way, the customer is directing the software to perform a job, and the bank shouldn’t be the one to say whether that job is necessary or advisable.

The banks’ rationale for attempting to impose OAuth is that it will solve an urgent security problem in the existing ecosystem of data aggregation. In his annual shareholder letter, J.P. Morgan Chase CEO Jamie Dimon emphasized how concerned he is about protecting the security of his customers:

> “One item that I think warrants special attention is when our customers want to allow outside parties to have access to their bank accounts and their bank account information. Our customers have done this with payment companies,
aggregators, financial planners and others. We want to be helpful, but we have a responsibility to each of our customers, and we are extremely concerned.... We are now actively working with all third parties who are willing to work with us to set up data sharing the right way.”

Contrary to the professed intention of Mr. Dimon, this ‘right way’ – OAuth – would actually decrease customer access to their data and significantly weaken the cybersecurity protecting the money in customer accounts at his bank. To the extent there is an urgent security problem to be “extremely concerned” about, it’s not about data aggregation, it’s about passwords. Everyone agrees that password authentication is weak, but not everyone understands that aggregation services are the best way to make it stronger.

There are a number of secure methods for the collection of financial data in general use today. This is not a problem, it’s a strength. Different approaches are feasible or optimal for different Banks and Data Hubs under different circumstances. This array of secure options is what makes near-universal data availability possible today. If a new “standard” were to be imposed, that universal access would be shattered.

**Cybersecurity for Financial Accounts**

There are numerous people at Personal Capital, including myself, who have worked with data aggregation for many years. Both our Chief Technology Officer and our Chief Engineering Officer have deep security experience, and each of them formerly worked at two different cybersecurity companies. For twelve years, I served on the board of directors of Yodlee, the largest data aggregator in the world, and served on its Audit and Risk Committee responsible for overseeing the audits by federal bank regulatory agencies and the banks themselves. I founded three different cybersecurity companies – one of which built the online authentication system used by the majority of banks in the U.S. – and served on the board of RSA Security, the largest cybersecurity firm in the world. Finally, I founded multiple financial technology companies that use aggregated data to improve financial lives, including Personal Capital. We have ample experience and expertise to provide commentary.

To protect a password, three components involved in an online authentication must be secured: the server, the transport and the client. As always, securing the client – a consumer’s personal computer, smartphone or other device – is dramatically more difficult that securing the other two.

- **Transport.** Securing the transport channel for moving data between client and server is the easiest thing to do. The most widely used method is Hypertext Transfer Protocol Secure (HTTPS) which uses either Transport Layer Security
(TPS) or Secure Sockets Layer (SSL) to create an encrypted tunnel which is highly resistant to direct attack.

- **Server.** It requires a high level of technical sophistication to secure a server and to deploy and monitor the necessary encryption hardware, firewalls, DMZs, load balancers, traffic sniffers, penetration testing and software patching. But organizations with advanced cybersecurity skills can make servers highly resistant to external malware attack or data breach.

- **Client.** It is extremely difficult to secure a local computer. One third of the personal computers in the world are already infected by malware, according to the Anti-Phishing Working Group. And although it’s hard to place malware on a specific computer if the user practices good hygiene, it is easy to place malware on thousands of computers if you’re not targeting a specific machine.

There are four methods of electronic data collection in general use today, plus a new one being proposed by some banks. Each of these methods has strengths and weaknesses related to threat vectors directed against the server, the transport and the client.
Secure Channel. The vast majority of data requests today are made through a Secure Channel connection between a Data Hub and a Bank. To establish an ongoing data feed using a Secure Channel connection, the Bank password must be provided by the Consumer once and only once. This is a remarkably powerful improvement in security versus asking the Consumer to log into the Bank’s website every time – not only because it exposes the Bank’s password only once, but also because the channel is read-only (it allows data to be viewed but does not allow payment or transfer instructions to be made). This method is very secure.

OFX. OFX, the earliest method for collecting bank data, celebrated it’s twentieth anniversary last week. I built the coalition of financial technology companies that created OFX in 1997 – Intuit, Microsoft and Checkfree. Despite its age or perhaps because of it, it has been implemented by 7,000 financial institutions, and it works. The OFX method is very secure.

Server-Side Scraping. Server-Side Scraping offers most of the security benefits of the Secure Channel method, including the once-and-only-once exposure of the Bank password on the Consumer’s computer. It differs only in that the Data Hub navigates to the Bank website to collect the Consumer’s data. This method is highly secure.

Client-Side Scraping. Client-Side Scraping operates similarly to Server-Side Scraping in every way except the final step. Rather than enter the password directly on the Bank’s website, the Data Hub sends the password to the Consumer’s browser which redirects it to the Bank website. This method is sometimes used when a Bank attempts to block a Data Hub’s access to its website. Client-Side Scraping exposes the password on the Consumer’s computer but only via a local application, not entered manually where it can be captured by key-logging malware. This method is moderately secure.

OAuth. OAuth is an authorization framework initially developed for the web, but version 2.0 is now focused on internal enterprise deployment rather than high-scale web use. It is very complex and would be impossible to implement across a majority of the 14,000 financial institutions in this country in any meaningful timeframe. And it would result in the weakening of the cybersecurity protecting Consumer financial accounts. In addition, it would train Consumers to be more susceptible to phishing attacks. This method is less secure.

Bank Log-in. The most basic way a Consumer accesses her financial data is to log in to her Bank website. Ironically, this is the least secure way to access the data. First, it requires the Bank password to be exposed on the Consumer’s local computer every time data is requested – if the data is accessed through a data
aggregation service, the Bank password is exposed once and only once. Second, frequent use of the Bank password is more dangerous than frequent use of a Fin-Tech password, because the Fin-Tech password typically grants read-only access to data while the Bank password allows the legitimate or fraudulent holder of the password to make transfers and payments. This method is least secure.

The online financial services world has a password problem. Passwords are relatively easy to compromise, yet they often allow financial transactions to be done by whomever knows the password. In multiple ways, data aggregation services can reduce the risk associated with passwords.

Not only is data aggregation a more secure way to look at your bank data, it’s also the best available means to protect your accounts against fraud of all types. We recommend everyone monitor their accounts twice a week. With an aggregation service, you can see all transactions in all accounts at all banks and brokers in 30 seconds.

And using a data aggregation service to monitor your accounts is both easier and more secure than going website to website. When using an aggregation service, each time a Consumer checks all her transactions at all her Banks she only exposes her Fin-Tech password, which has just read-only access. If she were to check each of her Bank websites – the average American family has 15 bank, broker, credit card, loan, mortgage, 401k, 529 and other financial accounts – she will expose 15 Bank passwords, each of which has full money-transfer capability.

This observation reinforces the most fundamental value of account aggregation. By making it easy for a Consumer to see all transactions in all accounts at all financial institutions, the Consumer can quickly see if any accounts have been compromised through any means – malware, phishing, hacking, data breach, social engineering or inside fraud. **This is the ultimate and universal solution to the problem of protecting your money from fraud of all types.**
17. What industry standards currently exist, in development or otherwise, to enable consumer-permissioned access to financial account data?

Here is a more detailed analysis of the four existing methods of financial data aggregation, the proposed OAuth method, and the simple act of logging in to a Bank website.

1. **Secure Channel.** This is the method used today with most large financial institutions, and so it represents the large majority of data requests. It involves the following steps:

**Set-Up**
- A Consumer passes her Bank password to a financial technology company (a Fin-Tech).
- The Fin-Tech passes the Bank password to the Data Hub.
- The Data Hub stores the Bank password, creates an associated UID and returns the UID to the Fin-Tech.
- The Fin-Tech immediately deletes the Bank password from its own records.
- That is the only time the Consumer ever enters her Bank password.

**Operation**
- The Consumer passes her Fin-Tech password (not her Bank password) to the Fin-Tech.
- The Fin-Tech retrieves her Data Hub UID, and passes that to the Data Hub.
- The Data Hub passes the Consumer’s password to the Bank using the Bank’s API and the Bank returns the Consumer’s data.

Among the many strengths of this system are: (1) Her Bank password is entered on her computer – the weakest link in the chain – once and only once. (2) The Fin-Tech does not store the Bank password so there is no possibility of a data breach at the Fin-Tech. (3) The Data Hub is a highly secure environment* and the passwords are encrypted at rest. (4) The transport channels between all parties are encrypted and secure. (5) Passwords are managed at the Fin-Tech and the Data Hub via secure software and humans do not have access to them. (6) The Bank is presented with the same password it uses every day to authenticate the user, so there is little development work to be done to deploy or support such a system.
* Yodlee is the largest Data Hub. It undergoes the same security audits that the banks undergo with banking regulators including the FDIC, FFIEC, OTS and Office of the Comptroller of the Currency. Yodlee also undergoes security audits from many of the banks themselves – over 200 audits per year.

And, in the event a Bank wanted to increase this already-high security even higher, it could establish the same UID exchange between the Bank and the Data Hub that already exists between the Data Hub and the Fin-Tech. In which case, the Data Hub would archive the encrypted passwords offline, and there would be effectively no possibility of a data breach at the Data Hub.

We assess the Secure Channel method to be very secure.

2. **OFX.** OFX was the earliest data transmission protocol for financial data collection. I led the coalition of financial technology companies (Intuit, Microsoft and Checkfree) that formed it 20 years ago on February 14, 1997. It is currently supported by 7,000 financial institutions.

   OFX 1.0 uses an SGML-based syntax, while OFX 2.0 and later uses XML. OFX incorporates two functions: data definition and user authentication, and the main thrust of the protocol has always been data definition: to standardize the data set used by financial applications. The protocol has always supported password authentication; optional support for so-called Multi-Factor Authentication was added in 2006; and optional support for OAuth 2.0 was added in 2016 as part of OAuth 2.2.

   There are other API-based protocols that function similarly to OFX – one example is the FS-ISAC’s recently-released Durable Data Application Programming Interface (DDA) which to my knowledge has yet to be implemented at any bank, and another example is the use of a bank’s existing API for mobile apps (sometimes referred to as Screenless Data Collection). These API-based data collection methods work similarly to OFX.

   We assess the OFX method (with password and/or MFA authentication) to be very secure.

3. **Server-Side Scraping.** Widely used since the early days of data aggregation, this is still the method used with the most financial institutions, although those institutions tend to be smaller. The Server-Side Scraping method is almost identical to the Secure Channel method. In the following workflow, only the italicized last step is different.
Set-Up
• A Consumer passes her Bank password to a financial technology company (a Fin-Tech).
• The Fin-Tech passes the Bank password to the Data Hub.
• The Data Hub stores the Bank password, creates an associated UID and returns the UID to the Fin-Tech.
• The Fin-Tech immediately deletes the Bank password from its own records.
• That is the only time the Consumer ever enters her Bank password.

Operation
• The Consumer passes her Fin-Tech password (not her Bank password) to the Fin-Tech.
• The Fin-Tech retrieves her Data Hub UID, and passes that to the Data Hub.
• The Data Hub’s software enters her Bank password into the Bank’s website and navigates through the website to find and return the Consumer’s data.

The Server-Side Scraping method has most of the benefits of the Secure Channel method, with one security and two operational exceptions: (1) It passes the Bank password over the Internet to the Bank website. (2) It can put more traffic on a Bank’s website. (3) Because websites are often redesigned, the programs that collect data from a bank’s web page can stop working when that page is changed, until the aggregator updates the programs.

We assess the Server-Side Scraping method to be highly secure.

4. Client-Side Scraping. Client-Side Scraping is identical to Server-Side Scraping except for the very last step. Rather than entering the Bank password directly into the Bank website, the Data Hub passes the Bank password to a small application on the Consumer’s local computer which then redirects the password to the Bank website.

Client-Side Scraping is used primarily when a bank attempts to prevent a Data Hub from accessing its website directly. Because the password is exposed on the Consumer’s computer each time data is being aggregated, this method is subject to attack from local malware. However, it is still safer than having a Consumer type her password, because any typed input can be captured by a simple keylogging malware.

We assess the Client-Side Scraping method to be moderately secure.
5. **OAuth.** OAuth is an authorization framework that allows a site (such as a Data Hub) to request information from another site (such as a Bank). It is a “tokenization” system that can be used in combination with methods such as OFX.

OAuth uses a complex set of interactions to achieve what a password could achieve by itself. From a security point of view, the advantage is that the Bank password is not given directly to the Data Hub. However, the disadvantages are that (1) implementation across many partners is complex and cumbersome, (2) depending upon the expiry of the tokens, it can require more frequent exposure of the Bank password on the Consumer’s local computer where the risk of malware is greatest, and (3) it is susceptible to phishing attacks and, more importantly, trains users to be less vigilant against phishing attacks.

At a very basic level, it’s easy to see why OAuth is less secure than existing methods: depending on the period of expiry of the tokens, it can require regular exposure of Bank passwords on the Consumer’s local computer, whereas existing methods do not.

OAuth is sufficiently complex that it merits its own diagram:
OAuth’s vulnerability to phishing stems from the fact that in steps H and I above, a browser screen pops up on the Consumer’s local computer asking for her Bank password. When the system functions as intended, that screen will be from the Bank itself. But it is not hard to substitute the true Bank screen with a false one.

More importantly, OAuth trains users to ignore safe Internet practice, because the pop-up password screen is automatically generated without the Consumer typing a known URL into her browser. Most of us in the industry work hard to educate users that they should never enter their password into a page unless they have navigated there using a known URL. The advantage of the other methods of data collection is that they all require the Consumer to type known URLs of the Bank and/or the Fin-Tech into her browser.

It’s interesting to note that a large part of the internet ignores this safe practice, the most glaring example being Facebook Connect. But this is one of the reasons no bank would consider using Facebook Connect as a method to log in to their bank website.

OAuth is a useful cybersecurity tokenization framework, but version 2.0 has been morphed into an enterprise solution rather than a consumer Internet solution. In the context of data collection from thousands of banks and brokers for tens of millions of consumers, it is not sufficiently secure or scalable.

OAuth is not sufficiently secure because when moving from version 1.0a to version 2.0, in an effort to make it easier for developers to implement, the requirement that the tokens be digitally signed was removed.* Although version 2.0 states that TLS or SSL should be used to encrypt every connection, it is up to each developer to properly implement this. Moreover, the tokens remain in the clear and unprotected on each computer through which they pass.

* For this and numerous other reasons, Eran Hammer, the lead author and editor of the OAuth protocol has rejected version 2.0 as a framework for secure high-scale multi-party Internet data exchanges. Here is an excerpt from his well-known article, “OAuth 2.0 and the Road to Hell.”

“When compared with OAuth 1.0, the 2.0 specification is more complex, less interoperable, less useful, more incomplete, and most importantly, less secure. To be clear, OAuth 2.0 at the hand of a developer with deep understanding of web security will likely result in a secure implementation. However, at the hands of most developers – as has been the experience from the past two years – 2.0 is likely to produce insecure implementations.... The web does not need yet another security
framework. It needs simple, well-defined, and narrowly suited protocols that will lead to improved security and increased interoperability. OAuth 2.0 fails to accomplish anything meaningful over the protocol it seeks to replace.”

OAuth is not sufficiently scalable because of its complexity and the number of times it must be invoked. Its complexity is demonstrated in the diagram above. The number of times it must be invoked can be calculated by multiplying the number of Consumers using data aggregation (tens of millions) times the number of financial accounts they aggregate (an average of 15 per household) times the reauthorization frequency determined by the bank-specified expiry of each token. Banks may set the expiry of each token at a year, a month, a week, or even an individual session.

If the tokens were set for weekly reauthorization, this would mean between 8 and 20 billion reauthorizations each year – each of which would expose a Bank password on a Consumer’s local computer.

An even more difficult challenge for OAuth scalability is the number of financial institutions that would have to implement and operate the required infrastructure. There are 14,000 financial institutions in this country, most of which are small and lack sophisticated cybersecurity architects and coders. Even large banks with well-funded cybersecurity teams have had difficulty properly implementing new protocols like this. And to make OAuth work for financial data aggregation, it would require each of these institutions, or the service providers to whom they may have outsourced their technology operations, to enter into bi-lateral contracts and establish secure back-channel connections with every data aggregator. This would not happen in my lifetime or yours.

Finally, OAuth is not secure or scalable for the Consumer, either. It’s not secure because it trains the Consumer to enter their passwords into pop-up browser windows that they haven’t navigated to using a known URL. This is precisely the bad Internet hygiene we all warn our customers against and which makes phishing attacks successful.

It’s not scalable (or, better said, it’s too inconvenient to be scalable) for the Consumer because of the constant requirement to be re-entering passwords to reauthorize access to various financial accounts. My experience is that very few Consumers would be willing to do something like this.

We assess the OAuth method to be less secure.
6. **Bank Log-in.** Surprisingly, the least secure way to see your data is to log in to your bank website. Every time a Consumer logs in to her Bank website, she exposes her Bank password on her local computer – where the malware resides.

One of the automatic security benefits of using an aggregation service is that each time a Consumer checks all her transactions at all her Banks (which we recommend should be at least twice per week) she only exposes her Fin-Tech password, which has read-only access. Not only is aggregation a more secure way to look at Bank data, but it is the only practical way to do transaction monitoring.

This observation reinforces the strategic value of account aggregation. By making it easy for a Consumer to see all transactions in all accounts at all financial institutions, the Consumer can quickly see if any accounts have been compromised through any means – malware, phishing, hacking, data breach, social engineering or inside fraud. This is the ultimate and universal solution to the problem of protecting your money from fraud of all types.

(In fact, account aggregation is the way many users realized they had been given fraudulent accounts by Wells Fargo – new and previously-unknown accounts showed up on their aggregation services.)

We assess Bank Log-ins to be least secure.

1. **What types of products and services are currently made available to consumers that rely, at least in part, on consumer-permissioned electronic access to consumer financial account data?** What benefits do consumers realize as a result? This question covers the use of such data to deliver products or services or to assess eligibility for a given product or service.

There are thousands of products and services made possible by consumer-permissioned electronic access to consumer financial account data. Everything from budgeting to credit decisioning to transaction monitoring to online payment to tax preparation to personal financial management.

Most of these products and services fall somewhere in the category of financial advice. Whether it’s finding a better credit card or building a long-term retirement plan, they provide explicit or implicit advice to improve your financial life.

A necessary condition for good financial advice is to build it on an understanding of the financial situation of the individual or family being advised. Data aggregation is the very foundation of responsible financial advice in all of its forms.
2. **How many consumers are using or seeking to use such products or services? What demographic or other aggregate information is available about these consumers?**

Tens of millions of American families use data aggregation to build better financial lives.

Personal Capital has over 1.3 million registered users of its personal financial management and financial planning software. Those users are tracking (via aggregated data) over $270 billion in assets and liabilities.

3. **To provide or assess eligibility for these products and services, what kinds of consumer financial account data are being accessed, by what means, under what terms, and how often? How long is accessed data stored by permissioned parties or account aggregators?**

In order to fulfill our promise to our users, Personal Capital collects data from all your financial accounts at all your financial institutions. We refresh the data at least once a day, usually overnight, and then again when the user logs in. We store the data until the user instructs us to delete her account. The data includes:

- Account Types
- Balances
- Transactions
- Holdings
- Interest Paid and Charged
- Interest Rates
- Overdraft Fees
- Commissions
- Advisory Fees
- Embedded Fund Fees
- Other Fees and Costs

In his annual shareholder letter, J.P. Morgan Chase CEO Jamie Dimon said about data aggregation: “Far more information is taken than [the customer and the software she uses] needs in order to do its job.” This makes no sense. How would J.P. Morgan know what information was necessary, and why would a customer let the bank decide?

Some financial institutions like Fidelity would like to limit aggregators to only balances. This would make the data all but useless for most purposes. Transaction monitoring
would not be possible without transactions. Investment analysis would not be possible without transactions and holdings. Rate comparisons would not be possible without rates. Financial analysis would not be possible without fees and costs. And responsible financial planning – the single most important activity that everyone should do and most people don’t – would not be possible without all of the data.

It’s just silly to argue that consumers should not be given “too much” of their data. (Unless you’re a financial institution with high or hidden fees or uncompetitive products, in which case you’d prefer not to make that data available.)

4. **To provide or assess eligibility for these products and services, what kinds of non-financial consumer account data are being accessed by parties that also access consumer financial account data? By what means, under what terms, and how often? How long is accessed data stored by permissioned parties or account aggregators?**

With permission of each user, Personal Capital collects and stores three primary types of data:

- Aggregated data from consumer financial accounts
- Customer profile data provided by the user
- Market data and securities attributes

As an example, we enhance a user’s aggregated holdings data by combining it with numerous attributes of each individual security (type, class, sector, geography, etcetera) and mutual fund or ETF (fees, performance, underlying holdings, etcetera). This allows us to provide the most detailed and complete investment analysis available.

How long the data should be stored varies by application. For personal financial management and financial planning, the data should be stored indefinitely, until the user instructs us to delete the account. Long historical data is a very valuable input into the financial planning process, and the ability to compare financial plans to actual behavior can be both insightful and motivating.

5. **What types of companies offer products and services that rely, at least in part, on consumer-permissioned electronic access to consumer financial account data, either to deliver the product or service or to assess eligibility for the product or service? To what extent are such products and services offered by entities that offer transaction accounts? To what extent are they offered by other market participants?**
Of the wide array of products and services based on aggregated data, almost all are or could be offered by traditional banks and brokers, in addition to the financial technology companies that usually pioneer them. An observed pattern is that young financial technology companies to create a new product or service and, if successful, the more progressive financial institutions copy the product or service a few years later.

For example, Personal Capital pioneered digital wealth management with the combination of online tools and human advisors in 2011. Vanguard copied that approach in 2015, and Schwab has announced they will do so in 2017.

6. **In what ways, if any, do consumer products and services that rely, at least in part, on consumer-permissioned electronic access to consumer financial account data differ according to whether the offering company provides or does not provide transaction accounts to consumers? Do any such differences impact consumers? If so, how?**

Some services, such as many payment services, are easier to provide if the institution controls the financial account.

Many services, such as Mint or Personal Capital rely on broad data to help consumers understand how they are performing against their financial goals. Limiting data and access limits prudent financial analysis and reduces a consumer’s ability to monitor and manage their financial lives.

Consider the FICO analogy: for decades, financial institutions have required access to consumer credit reports and scores to offer their own proprietary financial products. Some financial technology companies evaluate broad-based consumer behavior across a large set of consumer financial accounts, in order to price, underwrite, offer and service their own products. This use of held away transactional data is much like the banks’ use of credit reports and scores, which is aggregated data that examines consumer spending and creditworthiness across financial institutions, merchants and other businesses.

7. **To what extent do market participants compete to offer consumer products and services that rely, at least in part, on consumer-permissioned access to consumer financial account data? How does such competition impact consumers?**

There is a high level of competition to provide most of the products and services enabled by aggregated data.

More importantly, widespread availability of aggregated data is a vital enabler of increased competition for traditional financial services. For instance, access to credit
card account data powers many services that help consumers find and evaluate the best credit card offers.

8. What incentives or disincentives exist for consumer financial account providers to facilitate or discourage consumer-permissioned access to the account data that they hold by permissioned parties or account aggregators? In what ways do consumer financial account providers directly or indirectly facilitate or restrict consumer-permissioned access to account data? What are the associated impacts to consumers and other market participants?

Most financial institutions have embraced customer data access, but some are still resisting or are attempting to restrict it. Those that resist are often motivated by a desire to control the customer’s data and therefore control the customer. They prefer the customer come to their site rather than an aggregated site. They prefer the customer not see all the costs and fees. They prefer the customer not be able to easily compare offerings among different financial institutions.

Today’s resistance is the effort by J.P. Morgan Chase and Wells Fargo to impose the OAuth method on data aggregators. The argument that this will solve widespread security problems is specious, because OAuth will actually decrease overall security, as shown in answer to Question 17.

The argument that J.P. Morgan Chase is motivated by a concern over possible data breaches is equally specious. I am not aware of any data breaches at any data aggregators. But I do remember the headline: “JPMorgan fell victim to the largest theft of customer data from a financial institution in US history,” when the bank revealed in a 2015 SEC filing that more than 70 million households and seven million small businesses may have had their private data compromised in a cyberattack.

9. What impediments, obstacles or risks do consumer financial account providers currently face in providing data to or allowing access to data by permissioned parties or account aggregators? Describe specific operational costs, risks, and actual or potential losses, and identify their specific causes.

Some banks argue that it is a costly burden to respond to data requests from aggregators. This argument is specious, as well. With today’s technology, responding to a high volume of data requests should be an easy and inexpensive thing to do. For example, Google responds to 40,000 data requests per second.
To the extent that a bank doesn’t have the technology to fulfill the legitimate requests of its customers for access to their data, it’s in their interest, their customers’ interest and the public interest for the bank to upgrade its technology.

Regular monitoring of aggregated transaction data is the best available way to protect consumer bank accounts from fraud of all types. If a bank doesn’t have the computing capacity to participate in making this fraud-prevention regime possible on a wide scale, it’s not contributing to the common defense of all banks.

10. What impediments, obstacles or risks do permissioned parties or account aggregators currently face in obtaining such data? Describe specific operational costs, risks, and actual or potential losses, and identify their specific causes.

The best way for an aggregator to collect the data is via the Secure Channel or other API-based methods. Most large institutions have entered into bilateral agreements with large aggregators to facilitate this. Those that don’t make it more cumbersome for both the bank and the aggregator to do their jobs.

In some instances, banks have cut off (blackout) or restricted (brownout) the data provided to an aggregator. J.P. Morgan Chase and Wells Fargo did this to Intuit multiple times in 2016. They did it in order to coerce Intuit into accepting their version of OAuth.

Occasionally, banks have attempted to restrict Server-Side Scraping with techniques such as IP blocking. These techniques are not effective to prevent Client-Side Scraping.

11. What impediments, obstacles or risks do consumers currently face in obtaining—including permitting access to—such data?

The only impediments consumers face come from the occasional bank that attempts to restrict access.

The risk that a consumer assumes when aggregating her data is quite low. The bigger risk is that if she does not aggregate she’ll expose her bank password more frequently on her local computer, and fail to have an effective transaction monitoring capability.

12. What security and other risks do consumers incur if they permit access to their financial account data in order to obtain a particular product or service? What steps have consumer financial account providers, account aggregators, permissioned parties
and other users of consumer-permissioned account data taken to mitigate such risks? What information do these parties communicate to consumers about associated risks?

Personal Capital is very explicit with its users about our privacy and security policies and procedures. (See Question 13.) We have assembled one of the most experienced Internet security teams in Silicon Valley to build a service that protects our users. We do not store our users’ passwords on our systems. And we enable read-only access to the data, but no transactional capabilities.

And again, the best way to protect yourself against fraud is to regularly monitor all your transactions at all your financial institutions using an aggregation service like Personal Capital.

13. In what ways, do account aggregators or permissioned parties use consumer-permissioned account data for purposes other than offering or facilitating the delivery of a specific product or service to the permissioning consumer? Do such companies continue to access or store data after the consumer ceases to use the product for which the permissioned data use was intended by the consumer? Do such companies share the data with other parties and, if so, under what terms and conditions? What are the associated impacts to consumers?

The first four sentences of Personal Capital’s Privacy and Security Statement read:

   Personal Capital is committed to the protection of your privacy. We understand keeping your information secure and confidential is critical to earning and keeping your trust. We NEVER rent, sell or trade your personal information to anyone. Ever.

Personal Capital does not store our users’ bank passwords. When we are given a new bank password, we transmit the password to Yodlee, our data aggregator, and immediately delete the password from our systems. This initial transmission of the password is performed with automated software, so no human sees a bank password.

Personal Capital makes it easy for a user to delete their account and all the associated data:
14. When consumers permit access to their financial account data, what do they understand about: what data are accessed; how often they are accessed; for what purposes the data are used; whether the permissioned party or account aggregator continues to access, store or use such data after the consumer ceases to use the product or service for which the permissioned data use was intended by the consumer; and with which entities a permissioned party or account aggregator shares the data and on what terms and conditions? What drives or impacts their level of understanding? What impact does their level of understanding have on consumers and on other parties, including on consumers’ willingness to permit access?
Mr. Jamie Dimon, CEO of J.P. Morgan Chase, said this in his annual letter to shareholders.

“When we all readily click “I agree” online or on our mobile devices, allowing third-party access to our bank accounts and financial information, it is fairly clear that most of us have no idea what we are agreeing to or how that information might be used by a third party.”

In fact, when consumers click “I agree” on a website like Personal Capital’s, it’s very clear what they’re agreeing to. And much clearer than when clicking “I agree” on most bank websites.

In the first place, when someone agrees to use data aggregation tools such as ours, they know exactly how their information will be used – for data aggregation.

Second, we make it abundantly clear in our Terms of Use, the link to which is immediately follows the “I agree” button. Here are an initial six paragraphs of Personal Capital’s Terms of Use. (Emphasis added where the language describes how our customers’ information will be used and for what.)

https://www.personalcapital.com/content/terms-of-use/

Personal Capital Terms of Use
Last updated on January 20, 2017

Welcome to Personal Capital, a personalized money management solution for a better financial life. You are just minutes away from enjoying Personal Capital’s award-winning financial dashboard, allowing you to make sense of your whole financial picture wherever you are. With the Personal Capital’s financial dashboard, you can effortlessly track all of your personal finances -- account balances, cashflows, transactions and holdings – from the convenience of your computer, tablet or phone. Before you get started, we ask that you take a few minutes and read the important Terms of Use Agreement below. We look forward to your use of our dashboard.

Terms of Use Agreement

Description of our Services

Our goal is to provide you with a personalized money management solution for a better financial life. Our Services are comprised of the following features, delivered to you through our Dashboard, marketing partners, and through communications with our professionals, as follows:
Financial account aggregation. We offer financial account aggregation, where Personal Capital, acting as your authorized agent, will retrieve your financial account information, such as your account balances, transactions and holdings, from financial institutions you designate. Financial account aggregation is an optional Service you may utilize by providing financial account credentials, allowing us to securely connect with third party financial institutions, to present your financial information on our Dashboard. Our account aggregation Services are regularly refreshed, effortlessly providing you with up-to-date financial account information.

Financial visualizations. Your financial account information, collected through account aggregation or manual account information you provide, is used to display your consolidated financial picture. Financial visualizations include various charts, detailed transactional data and other financial account data that we present to you, summarizing your financial life at a glance.

Financial insights. Your financial account information, along with optional personal and financial information you may provide, are used to generate financial insights. We utilize your aggregated account data, along with stated assumptions or information you provide, to share important financial observations that can make you aware of your overall financial picture and opportunities to improve it.

Financial consultations. You may be eligible to receive a free financial consultation from a licensed financial advisor. The consultation is optional for eligible Dashboard users or through our marketing partners, offered via solicitation from one of our professionals. A financial consultation is a personalized analysis of your financial situation, based on information gathered from your use of our Dashboard or interactively with a licensed advisor, to make you aware of potential risks and opportunities within your current financial situation. Your participation in this Service may result in an offer for wealth management services, separate from the free financial consultation Service itself.

By contrast, on J.P. Morgan Chase’s consumer website, the link to the Terms of Use is buried at the bottom of the home page in small type along with other legal disclaimers. The Terms of Use has no mention of what the customer is agreeing to or how his or her information will be used. In fact, it also refers to two other terms of use, neither of which are linked: “The jpmorgan.com Website and the jpmorganchase.com Website contain separate terms and conditions, which are in addition to these terms and conditions.” Here are the first three paragraphs of Terms of Use on the chase.com website. [https://www.chase.com/digital/resources/terms-of-use](https://www.chase.com/digital/resources/terms-of-use)
Terms of use

PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY. BY ACCESSING THIS WEBSITE YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS BELOW. THESE TERMS AND CONDITIONS ARE SUBJECT TO CHANGE. ANY CHANGES WILL BE INCORPORATED INTO THE TERMS AND CONDITIONS POSTED TO THIS WEBSITE FROM TIME TO TIME. IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, PLEASE DO NOT ACCESS THIS WEBSITE.

Unauthorized use of JPMorgan Chase's Websites and systems, including but not limited to unauthorized entry into JPMorgan Chase's systems, misuse of passwords, or misuse of any information posted to a site, is strictly prohibited.

You acknowledge that JPMorgan Chase may disclose and transfer any information that you provide through this Website to (i) any company within the JPMorgan Chase group, its affiliates agents or information providers; (ii) to any other person or entity with your consent; or (iii) if we have a right or duty to disclose or are permitted or compelled to so disclose such information by law. You consent to the transmission, transfer or processing of such information to, or through, any country in the world, as we deem necessary or appropriate (including to countries outside the EEA), and by using and providing information through this Website you agree to such transfers. Use of this Website, including any patterns or characteristics concerning your interaction with it, may be monitored, tracked and recorded. Anyone using this Website expressly consents to such monitoring, tracking and recording.

On Wells Fargo’s consumer website, the link to the Terms of Use is not even on the home page. You have to find “Privacy, Cookies, Security and Legal” among literally 179 links on the home page. After clicking that link, a link to Wells Fargo’s Terms of Use appears as the sixteenth of seventeen links on that second page. Similar to J.P. Morgan Chase, Wells Fargo’s Terms of Use has no mention of what the customer is agreeing to or how his or her information will be used. The first four paragraphs of Wells Fargo’s Terms of Use (as is the rest of it) are designed to protect Wells Fargo, not to protect the customer: https://www.wellsfargo.com/privacy-security/terms

General Terms of Use

You are currently viewing a page of the wellsfargo.com website or a related website (the “Site”) belonging to Wells Fargo & Company or one of its subsidiaries ("Wells Fargo"). This Site and any of the services provided by Wells Fargo in connection with this Site (the “Services”) are being provided to you
expressly subject to these Terms of Use, which govern your use of the Site. Please read these Terms of Use carefully. By accessing this Site you agree to be bound by these Terms of Use. The Site is intended for individuals who are at least 13 years old. If you are under the age of 13 years old, you should not be visiting this Site.

“Services” under these Terms of Use include financial services for consumers and businesses, business services offered to you directly by Wells Fargo, and additional services available to you from independent third party service providers accessed through navigation from the Site.

**Copyrights and trademarks and restrictions on use**

All of the pages and screens on the Site are owned and controlled by Wells Fargo, except as otherwise expressly stated, and are protected by U.S. copyright laws and international treaties. The copyrighted materials on the Site include, but are not limited to, the text, design, software, images, graphics, source code, and the content on the Site. You are authorized to view the information available on the Site for your informational purposes only. You may download copyrighted materials for your personal or internal business purposes only. You acknowledge that you do not acquire any ownership rights by downloading copyrighted material. You may not copy, display, distribute, transfer, link to, reproduce, license, frame, alter, create derivative works of, or republish all or any portion of the Site for any commercial or public purpose without Wells Fargo’s prior written consent. The WELLS FARGO® stagecoach design and the WELLS FARGO “box” logo are federally registered trademarks owned by Wells Fargo. Other featured words used on the Site to identify the source of goods and services are trademarks and service marks owned by Wells Fargo or owned by third parties. You may not use, copy, display, distribute, modify, or reproduce any of the trademarks found on the Site except as authorized in this paragraph. You may not use any of the Wells Fargo trademarks as a link to the Site except pursuant to a written trademark license agreement.

The Site may contain links to websites controlled or offered by third parties (non-affiliates of Wells Fargo). Wells Fargo hereby disclaims liability for any other company’s website content, products, privacy policies, or security. In the event you choose to use the services available at a linked site, you agree to read and adhere to the policies and terms of use applicable to that site. In addition, any advice, opinions, or recommendations provided by the linked site providers are those of the providers and not of Wells Fargo. Your participation in any linked site, including payment for and the delivery of goods or services, is based solely on the agreement, if any, between you the linked site provider.

And Wells Fargo’s Terms of Use ends with an even more ominous tone:
Indemnification

You agree to defend, indemnify, and hold harmless Wells Fargo, its affiliates, and their respective directors, officers, employees, and agents from and against all claims and expenses, including attorneys' fees, arising out of your violation of these Terms of Use or misuse of the Service or this Site, including such violation or misuses conducted by your employee or agent, if applicable.

15. To what extent are consumers able to control how data is used by permissioned parties or account aggregators that obtain that data via consumer-permissioned access? Are consumers able to control what data are accessed, how often they are accessed, for what purposes and for how long the data are used, and with which entities, if any, a permissioned party or account aggregator may share the data and on what terms and conditions? Are they able to request that permissioned parties, account aggregators, or other users delete such data? Is such data otherwise deleted and, if so, when and by what means? To what extent are consumers consenting to permissioned party and account aggregator practices with respect to access, use and sharing of consumer financial account data?

Personal Capital users have complete control over how their data is used, in that we only operate the service for people who direct us to do so. If a user wants to stop using the service, there is an easy way to delete her account on our website (see Question 13). When we delete an account, all the data becomes unrecoverable.

16. Do consumer financial account providers vet account aggregators or permissioned parties before providing data to them? Do consumer financial account providers perform any ongoing vetting of account aggregators or permissioned parties? If so, for what purposes and using what procedures? What are the associated impacts to consumers and to other parties?

Yodlee undergoes the same security audits that the banks undergo with banking regulators including the FDIC, FFIEC, OTS and Office of the Comptroller of the Currency. Yodlee also undergoes security audits from many of the banks themselves – over 200 audits per year.

17. What industry standards currently exist, in development or otherwise, to enable consumer-permissioned access to financial account data?
Our response to Question 17 has been moved up in this document to a position ahead of Question 1.

18. What changes are or may be expected to happen to any market practice described in response to questions 1 through 17, why, and with what impacts to consumers, consumer financial account providers, permissioned parties, and account aggregators? Responses to this question may be integrated into responses to questions 1 through 17 if commenters prefer.

We see no likely changes in market practice, nor do we believe changes are necessary.

19. What changes should happen to any market practice described in response to questions 1 through 18, why, and with what impacts to consumers, consumer financial account providers, permissioned parties, and account aggregators? Responses to this question also may be integrated into responses to questions 1 through 17 if commenters prefer.

We see no likely changes in market practice, nor do we believe changes are necessary.

20. Are “industry standard” practices that provide consumers with data access comparable to that envisioned by section 1033 of the Dodd-Frank Act likely to be broadly adopted by consumer financial account providers, permissioned parties and account aggregators in the absence of regulatory action? If not, how will “industry standard” practices be insufficient? What marketplace considerations are likely to bear on such developments? Generally, how will the advent of standard practices for consumer-permissioned access to consumer financial account data affect competition and innovation in various consumer financial service markets?

The existing “industry standard” practices are to support access to a wide set of data using the Secure Channel, OFX, Server-Side Scraping and Client-Side Scraping methods. These practices have grown organically to huge scale with high security connecting 14,000 financial institutions with tens of millions of consumers.

Section 1033 of the Wall Street Reform and Consumer Protection Act clearly mandate that all financial institutions provide their customers with easy and effective electronic access to their own financial data.
“SECTION 1033. CONSUMER RIGHTS TO ACCESS INFORMATION
(a) In general, subject to rules prescribed by the Bureau, a covered person [a bank or broker] 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.”

Even so, widespread data aggregation happened a decade before the passage of Section 1033 of the Dodd-Frank Act. It happened because the bank’s best customers wanted it to happen. And it happened because most banks understand it’s a good thing for them, for their customers and for the banking industry. And so it will continue.

Respectfully submitted.

Sincerely,

Bill Harris
CEO of Personal Capital

One Circle Star Way, First Floor
San Carlos, CA 94070
bill@personalcapital.com

[Biography attached below.]
BILL HARRIS BIOGRAPHY

Harris is Founder and CEO of Personal Capital, and former CEO of Intuit and PayPal. He has worked in the Silicon Valley for over 25 years, and founded multiple financial technology and cybersecurity companies. He served on the boards of directors of numerous public companies, including SuccessFactors, Macromedia, Visual Sciences, EarthLink, Yodlee and RSA Security. He spent ten years in the media industry in New York, where he was Executive Vice President of U.S. News and the Atlantic Monthly, and ran consumer marketing for Time, Money, Fortune and People magazines. Harris graduated from Middlebury College and Harvard Business School.

Relevant Experience

• CEO of Personal Capital, provider of the best cloud-based personal financial management and financial planning software in the world, which uses aggregated data.

• Former CEO of Intuit, the makers of Quicken and QuickBooks, the best desktop personal financial management and financial planning software in the world, both of which use aggregated data.
  
  o Harris formed the coalition of financial technology companies – Intuit, Microsoft and Checkfree – to create Open Financial Exchange (OFX), the first standard for aggregation of financial data, launched 20 years ago on February 14, 1997.
• Former CEO of PayPal, the leading online payment system, which uses aggregated data to verify the identity of its users and the authenticity of payment instructions.

• Former President of ChipSoft, the makers of TurboTax, the leading tax preparation software which is now used to prepare over one half of the tax returns in the nation.
  o In 1993, Harris built one of the first two electronic filing systems in the country, and worked with the IRS to develop industry standards for electronic submission of tax returns to federal and state governments and for electronic payment of tax refunds. Over 90% of all individual and business tax returns in the U.S. are now filed electronically.
  o In 1996, Harris led the creation of Tax Exchange Format (TXF), the industry standard for electronic transmission of tax-related data from banks and brokers to their customers.

• Founder and former CEO of PassMark Security, which built the online authentication system now used by the majority of bank and broker websites in the U.S.

• Co-Founder and Chairman of XTeC, which is the leading provider of identity management and access control systems for the federal government, including the Secret Service, the Department of Homeland Security, the State Department and much of the military.
  o XTeC’s secure cloud-based systems use both PKI and SKI encryption and incorporate shared secrets, digital signatures, encrypted tokens, smartcards and various forms of biometrics including fingerprints and facial geometry recognition.

• Co-Founder and former Chairman of IronKey, which built the world’s most secure flash drive, used for private and public data storage and for remote authentication.

• Founding member of the Board of Directors of the Anti-Phishing Working Group (APWG).
  o The APWG is the industry, law enforcement and government coalition focused on unifying the global response to cybercrime through development of data resources, data standards and model response systems and protocols for private and public sectors.

• Former member of the Board of Directors of RSA Security, the largest cybersecurity company in the world.

• Former member of the Board of Directors of Yodlee, the largest aggregator of financial data in the world.
  o Harris served on Yodlee’s Audit and Risk Committee, which was responsible for the security and protection of its customers’ data. The committee oversaw over 200 cybersecurity audits conducted each year by federal agencies (including the FDIC, the FFIEC, and the Comptroller of the Currency) and by the large banks and brokers themselves.