

Consumer Data Aggregation Checklist

Data aggregation is the process of gathering financial information and presenting it in a single comprehensive view. When it comes to your Personal Financial Website, that means connecting with and extracting information from the companies that manage your financial accounts and liabilities so that we can provide you with a consolidated view into your accounts in real-time.

The power of data aggregation lies in the fact that you gain a comprehensive view of your financial situation. Because it's important to protect your financial information, you should understand how a third party will access, store, and use your data before authorizing them to aggregate your data.

At eMoney, we employ the industry's best practices in data security and privacy. Read on to learn how our data aggregation system works and how we stack up against recommendations from the Financial Industry Regulatory Authority's (FINRA) consumer guidelines.

FINRA: Weigh the benefits of aggregation against the risks of sharing your security credentials. Be particularly diligent when you authorize a third party to facilitate payments on your behalf. Check to ensure your payments go to the recipient.

We couldn't agree more with FINRA's guidance: It's important to understand the potential risk of sharing financial information with a third party. Your Personal Financial Website mitigates the risk by securely aggregating data so that we can develop informed financial plans.

Additionally, we do not facilitate payments of any kind on your behalf. In fact, you can use the Spending tab of the Client Portal to closely monitor and spot unauthorized transactions you might otherwise miss. When this feature is combined with notifications of specific transactions, you gain a single application through which you can monitor all of your accounts.

FINRA: Read the terms and conditions of any user agreement or contract you sign. Know what rights you are granting with respect to accessing your financial accounts and using your data. For instance, how often are your accounts scraped and what data is collected?

The Terms of Service (ToS) of your Personal Financial Website clearly and concisely outline our data aggregation procedures. These state that you are only granting access to your advisor so they can retrieve and view your account information.

FINRA: Understand the aggregator's privacy and data security measures. A good place to begin is by reading the aggregator's terms of use, privacy and security information. Here are some things to look for does (or may) the aggregator share your security credentials and data with, or provide access to your accounts to, another data aggregator or service provider? Does the aggregator sell your data to a third-party entity? If so, are you comfortable with that?

We only use client data for the benefit of the client and we do not and never will sell your data to a third-party entity.

FINRA: Does the aggregator use encryption when retrieving your data? How long is the data retained? What is the process of purging or disposing the data once you terminate your contract?

We fully encrypt production data while in transit. Highly sensitive data is encrypted at all times using AES 256-bit standard encryption - the same level of security as that used by most banks. Data is stored for your advisor's use until you end your relationship with the advisor or at your request.

FINRA: What happens if there is a data breach or any unauthorized access to your account? Is there a process in place to notify consumers and financial institutions should a breach occur?

Our provider has never had a security breach. However, we have implemented a robust security incident response plan should we suspect an issue. The plan includes identification, assessment, remediation, resolution, and notification. All company employees are trained to identify and properly report any suspected breach of confidential information.

FINRA: What type of liability, if any, does the aggregator bear in the event of a consumer loss due to a data breach or unauthorized access? Does the aggregator have the financial capacity or insurance coverage to compensate consumers for loss? Is there a dispute mechanism in place to resolve any issues related to data breaches or unauthorized access?

We follow standard aggregation industry best practices. Ultimately, the consumer is responsible for any damages due to unreported or unauthorized use of the consumer's login credentials.

FINRA: How accurate are the scraping algorithms used to collect data from your financial accounts? To find out, you can ask whether the aggregator conducts periodic checks to ensure that it is collecting data and using it accurately to provide the required service. You should also check the data yourself against your primary source accounts.

Our provider has a dedicated data support team staffed with experts and certified professionals whose goal is to ensure the functionality and accuracy of your data. At any time, we can open a ticket and have your connected accounts reviewed for accuracy.

FINRA: Check with financial data providers to find out what, if any, data is delivered to aggregators through an Application Programming Interface (API), which is generally considered a safer alternative than scraping.

While our current aggregation standards follow industry best practices, we are transitioning from screen scraping to an [API-based approach](#) to provide even greater peace of mind.

FINRA: Finally, make sure you cancel your account and terminate the access and rights you have granted to the aggregator once you discontinue using the service. Failing to do so may expose your financial information to ongoing security risks. Understand and follow the steps that need to be taken to stop the ability of the aggregator to access your account. This may involve more than just deleting the software application from your computer or mobile device.

We believe your data should always be secure and under your control. To that end, you can terminate your use of our service at any time. At your request, we will delete your account and purge your data from our system.