eMoney | WHITEPAPER

Scaling Your Practice with **Secure, Reliable Data Connections**

OVERVIEW

In a world increasingly driven by seamless digital experiences, consumers want easy access to their sensitive financial and personal information. They expect comprehensive views of what they own and what they owe, regardless of where their assets are held or managed.

To satisfy these expectations while protecting their reputations, firms must offer secure, reliable account aggregation. But not all aggregators are the same. Advisors must choose aggregation partners dedicated to keeping client data private and protected.

Aggregation benefits advisors as well as clients. With secure views of client account balances, advisors can deliver plans that reflect the current state of clients' finances. For example, with access to client spending and saving transactions, advisors can create budgets that update in real time to help clients stay on track to achieve their goals.

In addition to helping clients understand their financial situations, account aggregation also helps advisors identify opportunities to expand assets under management (AUM).

Enhancing the Business with Client Data

By using a third-party aggregator to automatically collect client account data from a variety of financial institutions, firms can:

- **Eliminate error-prone, manual entry** of client data into financial plans, performance reporting, CRM, and client portals so advisors can focus on activities that add value.
- **Build comprehensive views of client finances** quickly and easily.
- **Create sticky experiences that retain clients** by providing them with a single portal for all of their financial information.
- **Offer digital planning experiences,** based on accurate client financial data, that eliminate the need for paper reports.
- **Grow share of wallet** by identifying assets not currently under management so advisors can offer comparable products, or charge for assets held away.
- **Enhance the client experience** with automatic, accurate, and timely updates of financial data that relieve clients of the need to present paper statements.
- **Win over prospects** by using account aggregation as an impactful "try before you buy" preview of the client experience.
- **Respect client privacy** by ensuring the aggregator doesn't resell client data and only accesses the data it needs to provide its service.

Growing Adoption of Account Aggregation Services

Because of the benefit it provides to both advisors and clients, firms are increasing their use of account aggregation as indicated in recent studies.

In their 2019 Adviser Technology Study, InvestmentNews reports that a growing number of firms have added account aggregation software, with the adoption rate jumping from 53 percent in 2013 to 68 percent in 2019.[1,2]

Forty-five percent of firms that participated in the 2017 InvestmentNews Adviser Technology Study believe that account aggregation is among the most important features of a client portal, second only to portfolio performance reporting.[2]

Collaborating to Produce Real-time Financial Plans

Aggregation benefits clients by compiling the figures from their various financial accounts. That benefit increases when their account information is available in real time through an interactive client portal that is part of a comprehensive financial planning platform.

With access to live account information, advisors and clients can work together to establish goals, manage cash flows, and create scenarios that visually model the potential outcomes of financial and life decisions: What happens if the client buys a boat? Or delays retirement by two years? Or downsizes now and retires in six months?

This collaborative approach to financial planning differs radically from the traditional, annual meeting, much of which is spent capturing and updating client account values from paper statements to produce a 50-page report that clients then digest at home.

By contrast, the collaborative approach creates an engaging client experience. It uses aggregated data to deliver real-time financial planning through an interactive client portal. And if the client portal provides screen sharing, then advisors can meet with clients when the need arises from wherever the client happens to be, rather than meeting yearly in the office.

Recognizing the Importance of Security and Privacy

While collaborative planning experiences build trust and deepen relationships between advisors and clients, concerns regarding cybersecurity and data privacy are justified.

In their 2019 Thales Data Threat Report, IDC reports that 60 percent of organizations stated that they have been breached.[3] And according to the Ponemon Institute and Accenture, the average cost of cybercrime to the financial services industry is $18.3 million per company, the highest for any industry segment.[4]

Akamai Research reports that 66 percent of U.S. consumers would like rules that force brands to provide them with greater privacy, security, and control of their personal data.[5]

Respecting Data Ownership and Privacy

In addition to their concerns about data security, clients have issues regarding the privacy of their financial data.

In a 2018 The Clearing House study, 89 percent of fintech users report concern about information privacy when they use online or mobile fintech applications. Of those respondents, 33 percent were "very concerned," and 34 percent felt "extremely concerned."[6]

Financial services clients want to control:

1. Who accesses their data,
2. What data they access,
3. How the data is used,
4. If and for how long the aggregator will access the data after the service agreement ends.

After learning that many terms and conditions grant fintechs the authority to use consumer data for purposes other than providing the agreed service, 47 percent of users report being less likely to use those services.[7]

Fifty-one percent of respondents would like to provide explicit consent to every third party that seeks to access their data. And 56 percent report the desire to control which of their financial accounts and data types—which may include Social Security number, date of birth, phone number, email address, and home address—can be accessed by any third party.[7]

Unfortunately, many aggregators gather more client data than they need to provide their service. And they resell it.

Unlike companies regulated under the Fair Credit Reporting Act (FCRA), including traditional credit bureaus that must provide your personal data on request and correct inaccuracies, data aggregators are largely unregulated and aren't required by U.S. law to make any such guarantees.[8]

Before selecting an aggregation partner, be sure to know which client data they will gather, how long they will retain it, and whether they resell data.

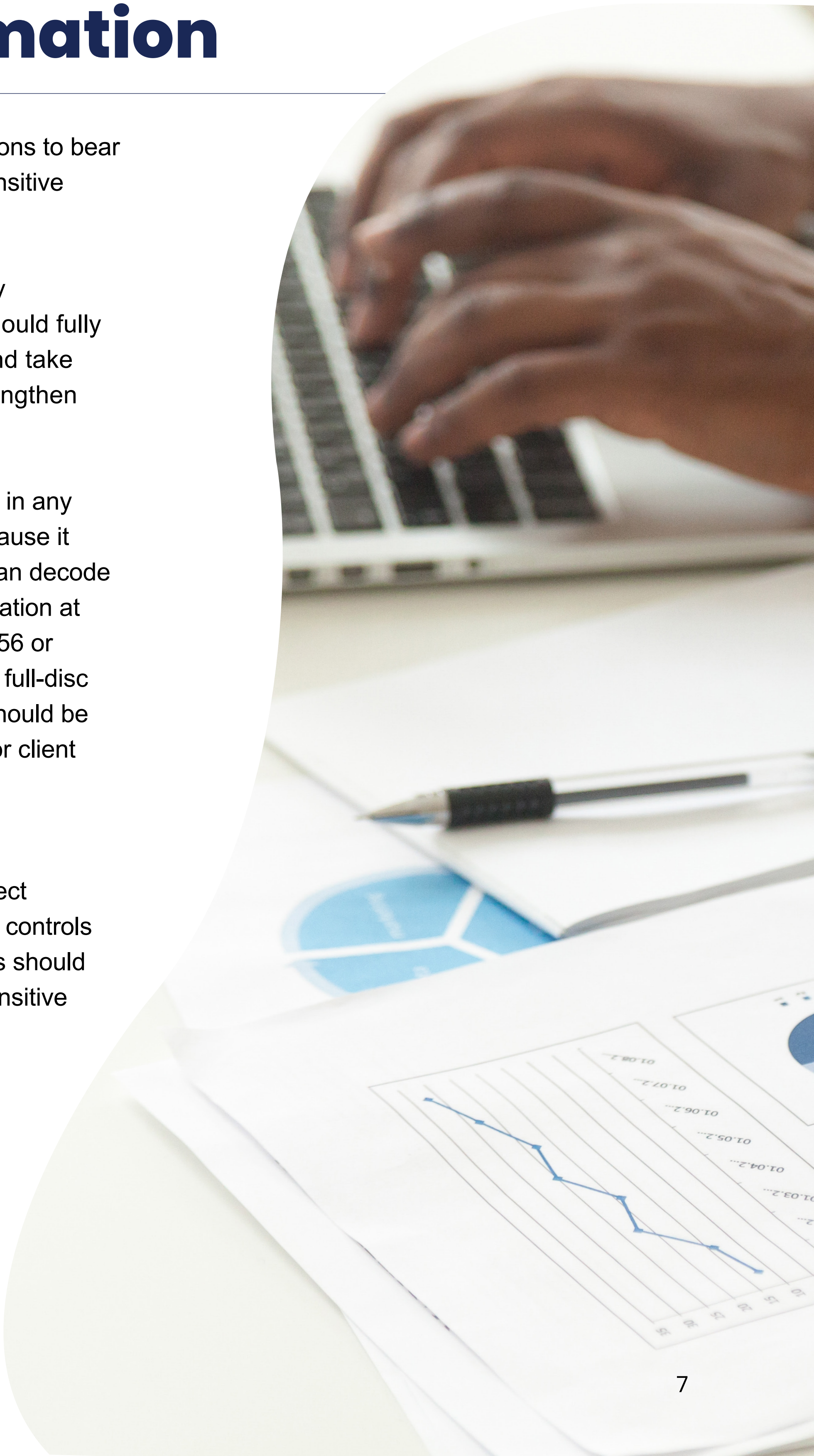
Protecting Sensitive Client Information

There are several security considerations to bear in mind regarding aggregation and sensitive client data.

Because online threats are constantly evolving, your aggregation partner should fully understand the security landscape and take steps to continually evaluate and strengthen their IT infrastructure.

Encryption is an important component in any online exchange of sensitive data because it ensures that only authorized parties can decode and read it. Sensitive customer information at rest should be encrypted using AES 256 or greater and at the hardware level with full-disc encryption. Customer data in transit should be encrypted using TLS 1.2 and higher for client connections and IPSEC for internal communications.

Aggregation vendors should also protect customer data with strict client access controls and multi-step authentication. Vendors should also have formal policies to protect sensitive data and client privacy.



Collecting Client Financial Data – APIs and Data Scraping

Account aggregation works through two methods: direct data connections and “data scraping."

Gathering Data with Direct Connections

APIs are an increasingly prevalent approach to aggregation for large financial institutions, which have the resources to develop them. APIs create a direct connection between two computer systems—the aggregation service requesting the information and the financial institution that will provide it. This form of aggregation is generally more reliable and accurate than data scraping. There are two predominant API technologies:

RESTful APIs

APIs built using the REpresentational State Transfer architecture (REST) enforce security by requiring that authentication credentials be validated on the financial institution’s server for each and every request. This approach is superior to that used by other API standards.

OFX APIs

Open Financial Exchange (OFX) is an older data exchange standard created in the mid-1990s. Used by over 3,000 North American banks, OFX is used to exchange financial data and to perform financial transactions between institutions and financial applications.

Scraping Client Information

The more traditional aggregation method is data scraping. This technique requires the aggregation service to log in to the financial institution’s website using the client’s user name and password. Once the service accesses the website, it searches for and extracts the needed financial data.

Challenges to Data Scraping

Depending on the aggregator, data scraping can securely gather client data. However, because this approach relies on scanning web pages, it requires regular maintenance due to the following challenges:

- **Website redesign:** Firms may redesign their websites or change the names of fields that contain financial data. Any changes to the names or locations of these data fields will interfere with the data scraper.
- **Client security credentials:** When clients change their user names or passwords, the data scraping technology can no longer access their data.
- **Institution security technology:** As institutions work to stay ahead of hackers, they may adopt new security technologies like multi-factor authentication. Most changes in security will impact the data scraping technology.

While data scraping requires regular maintenance, it will be around for the foreseeable future because many firms lack the financial and human resources to develop and maintain APIs.

Assessing Aggregation Partners: A 10-point Checklist

When selecting or reviewing a data aggregation partner, consider the following:

1. **Security defenses:** Determine if your tech vendor conducts annual audits and penetration tests. Ask how often they monitor their production network for intrusion.
2. **API-based aggregation:** Confirm that your vendor prioritizes RESTful-based APIs over those based on the OFX standard.
3. **Encryption:** Customer data at rest should be encrypted using AES 256 or greater and at the hardware level with full-disc encryption. Customer data in transit should be encrypted using TLS 1.2 or higher for client connections and IPSEC for internal communications.
4. **Privacy:** Many aggregators sell client data, often without the client's permission. Confirm that your aggregator respects client privacy by refusing to resell data.
5. **Data disposal:** Ask the aggregator how long it will retain client data. Confirm their process for disposing of client data after you or your client terminate the contract.
6. **Servers and storage infrastructure:** Understand how your vendor stores your client data. The vendor might manage their own servers and storage infrastructure, in which case they're directly responsible for protecting the data. If the vendor outsources storage to a cloud-based service, vet those third parties.
7. **Service intrusions:** Ask your vendor how they monitor their infrastructure for intrusions 24/7.
8. **Breaches:** Learn how your aggregator will respond to a data breach or any unauthorized access to your client data. Confirm that there is a process to notify clients should a breach occur.
9. **SOC 2 compliance:** SOC 2® is a compliance standard for protecting online data that requires a thorough audit of security, availability, process integrity, privacy, and confidentiality by a certified third party. Be sure that all aspects of the aggregator's service are SOC 2 compliant.
10. **Access and rights to data:** Verify that the aggregator will only access the data it needs to provide its service. If you discontinue service, ensure that the aggregator will terminate their access and release their rights to the data.

Aligning Data Practices With Data Privacy Concerns

By offering secure, reliable account aggregation, firms can create engaging experiences that deliver long-term value to advisors and clients. But to best serve their clients, advisors need to address their concerns about data security and privacy. And ensure that aggregators' data practices address those concerns.

When a firm works with an independent aggregation partner focused on privacy, security, an interactive user experience, and stable aggregation, everybody wins.

SOURCES

1. InvestmentNews. "2019 InvestmentNews Adviser Technology Report."

2. InvestmentNews. "2017 InvestmentNews Adviser Technology Report."

3. IDC. "2019 Thales Data Threat Report." go.thalesesecurity.com/rs/480-LWA-970/images/2019-DTR-Global-A4-Web-ar.pdf. Accessed April 2019.

4. Ponemon Institute and Accenture. "Cost of Cyber Crime Study." www.accenture.com/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf. Accessed April 2019.

5. Akamai Research. "Consumer Attitudes Toward Data Privacy Survey, 2018." www.akamai.com/us/en/multimedia/documents/report/akamai-research-consumer-attitudes-toward-data-privacy.pdf. Accessed April 2019.

6. The Clearing House. "Fintech Apps and Data Privacy: New Insights from Consumer Research." www.theclearinghouse.org/-/media/New/TCH/Documents/Data-Privacy/TCH-Consumer-Research-Report-08-20-2018.pdf. Accessed June 2019.

7. Security on Demand. "Your Bank's Digital Side-Door." www.securityondemand.com/news-posts/hacker-summer-camp-series-your-banks-digital-side-door/. Accessed May 2019.

8. Fast Company. "Here are the data brokers quietly buying and selling your personal information." https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information. Accessed June 2019.