YODLEE® INTERACTIVE

Key Security Questions to Ask a Financial Data Aggregation Provider

Is the data aggregation partner you're considering following the best practices for security and privacy? Here's how to find out.

TABLE OF CONTENTS

INTRODUCTION

As a financial services developer, you're in high demand. However, to create powerful, innovative apps, you need access to robust and accurate financial data, which means you need to identify and partner with the best financial data aggregation provider possible.

Financial applications by their very nature access sensitive personal and financial consumer data. Since your business is responsible for developing and providing the financial application, the security of your customers' personally identifiable information is your responsibility to manage. In this eBook, we'll focus on the crucial security aspect of data aggregation and outline key questions to help you identify an established partner with solid security, privacy, risk management, and compliance technologies and procedures behind their application programming interfaces (APIs).

> "As a startup, or a small business owner, **ultimately you're responsible for the compliance of your customer data.** But standing on the shoulders of trusted providers gets you a long way."
>
> *Fritz Robbins, CTO of Personal Capital*

DOES YOUR PROVIDER:

Follow Privacy and Security Best Practices?

Without cutting edge security and risk management protocols in place from the start, managing the physical, electronic, and procedural safeguards that protect consumers' financial data from unauthorized access or misuse is next to impossible. That's why you'll want to ask the right questions to ensure that your data aggregation provider follows industry best practice guidelines in the design and implementation of their network security environment.

QUESTIONS TO ASK

- **Does the provider offer separate production, staging, development, corporate, and specialty networks, with access control devices between each zone?**

- **Do they further segment networks within each zone to apply granular security and audit controls appropriate to each function?**

DOES YOUR PROVIDER:

Raise the Bar on Developer Standards?

It's important for your data aggregation partner to maintain high developer standards, including a certification program for those leveraging their data and resources. You'll also want to choose a data aggregation provider that fully supports open authentication protocol for authorization and authentication of consumers who want to interface with social media and other apps.

QUESTION TO ASK

- **Does the provider fully support open authentication protocol for authorization and authentication of consumers who want to interface with Facebook® Apps, Yahoo!® Widgets, Google® Gadgets™, and Apple® Apps?**

DOES YOUR PROVIDER:

Offer an Ultra Secure Platform?

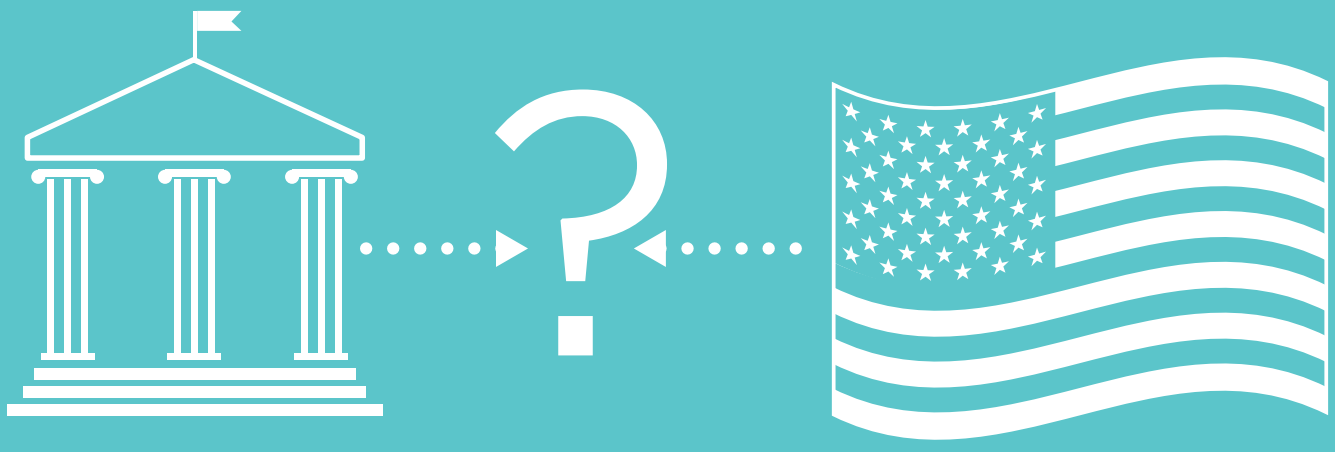
As the engine that will power your app, any data aggregation platform you're considering should be comprised of a set of infrastructure components that intelligently and securely aggregate, cleanse, augment, and store consumer data. Ask questions to ensure the platform has the security features that you need and the privacy and data protection your consumers require.

QUESTIONS TO ASK

- **Are the communication channels encrypted for all browsers, mobile, and tablets, and is the aggregation provider collecting their data over encrypted channels?**
- **Does the provider have APIs that minimize the amount of sensitive data available on a consumer's mobile device and make the provider responsible for handling data encryption?**
- **Does the provider offer a Defense-in-Depth layered approach to network and data security consisting of redundant firewalls, efficiently managed certificates and DNS, and a hardened architecture across the entire environment that they manage and control?**

DOES YOUR PROVIDER:

Comply with U.S. Regulations?



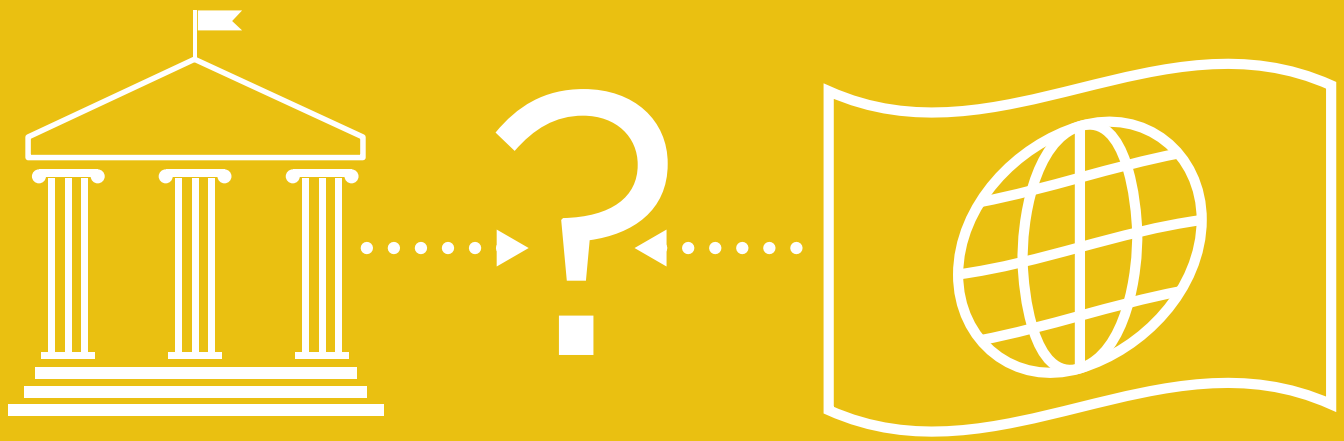
In the U.S., financial institutions, such as banks and brokerages, are heavily regulated to ensure the safety and soundness of their operations. Financial data aggregation providers that touch bank data are also supervised and regularly examined by the government to ensure they comply with the Gramm-Leach-Bliley Act (GLBA) and other similar regulations. Make sure your data aggregation provider can support you in your compliance obligations and in their own obligations as well.

QUESTIONS TO ASK

- **Is the platform compliant with security and privacy requirements in the U.S.? Is the provider willing to enter into contractual obligations with you and your regulatory bodies?**
- **Is the provider a technology service provider under U.S. banking laws? If not, how do you know if they are allowed to access banking data?**
- **Is the provider PCI-DSS compliant? If not, how do you know if they are allowed to access credit card data?**

DOES YOUR PROVIDER:

Comply with International Standards?



As your solution grows, you may attract customers in other countries, which means there are additional laws and regulations to contend with. If offering your solution in another country is even a remote possibility, or if you're accessing data from other regions, you'll want to ask your financial data aggregation provider if they're equipped to handle security and privacy requirements outside the U.S. If the data is handled offshore, international security laws may apply regardless.

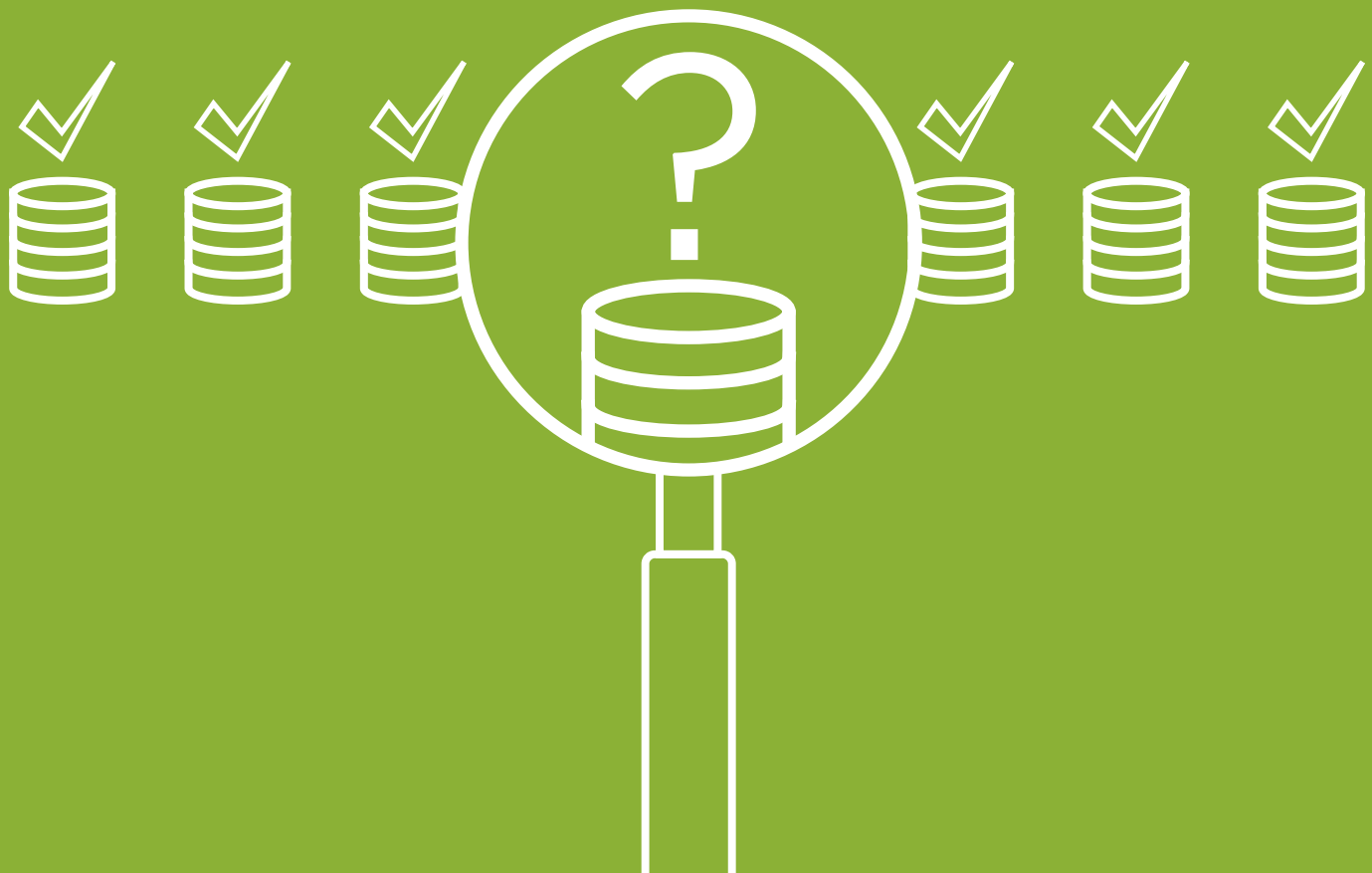
QUESTIONS TO ASK

- **Does the provider comply with international requirements such as the European Union Safe Harbor, EU Member States, or Asia Pacific Economic Cooperation Cross Border Rules for data transfer privacy?**

- **Does your provider engage with sub-contractors and cloud service providers to handle development, support, or disaster recovery outside of the country?**

DOES YOUR PROVIDER:

Monitor and Manage the Risk to Data?



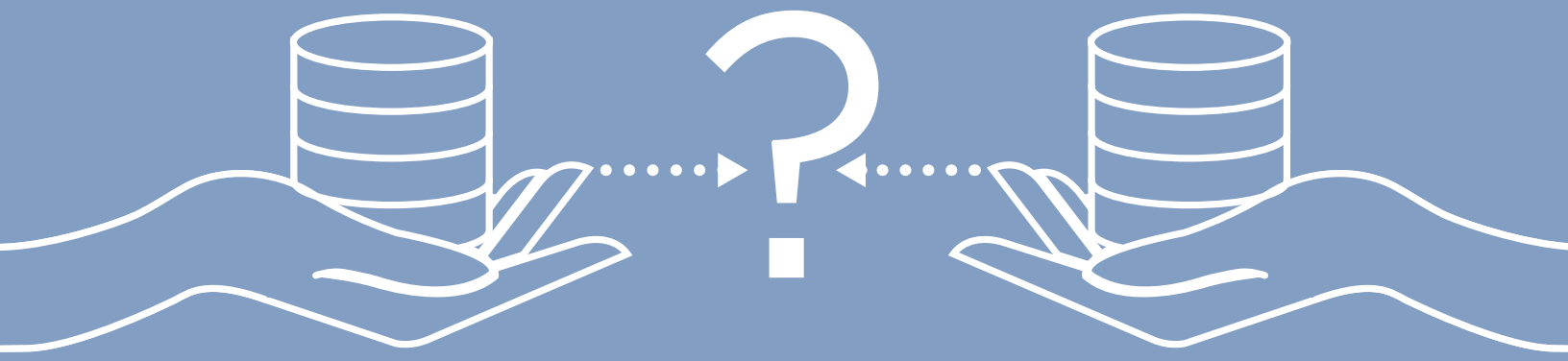
To ensure your app has consistent, secure access to quality data for your customers, all data sources, data quality, and data operations must be monitored constantly. If a data source becomes unavailable, specialized operations personnel should be on hand to solve the problem. A sophisticated, proactive monitoring and debugging infrastructure that addresses data source, data quality issues, and data availability quickly and without compromising the security and privacy of consumer data is essential.

QUESTIONS TO ASK

- **Who's responsible for vulnerability management?**
- **Who's responsible for patching and resiliency?**
- **Who's watching the traffic to manage operational and security concerns?**
- **How has the provider handled data breaches in the past?**

DOES YOUR PROVIDER:

Own the Data? Or Do You?



Before you sign the contract, make sure you understand who owns the data and who can use the data, since ultimately, as the data controller, you're obligated to your customers to make sure the data is used appropriately. If it's not clearly spelled out in the contract or defined in the service level agreements with liability and repercussions for non-compliance, then it's in your best interest to look elsewhere.

QUESTIONS TO ASK

- **Does your contract clearly define who owns the customer data?**
- **What rights do you have to the data in order to maintain it?**
- **What access do you have to the data?**
- **Do you have direct access via the provider's APIs to carry out your consumers' wishes?**
- **What rights does the aggregation provider have to use that data for their own purposes?**

DOES YOUR PROVIDER:

Have an Experienced Team?

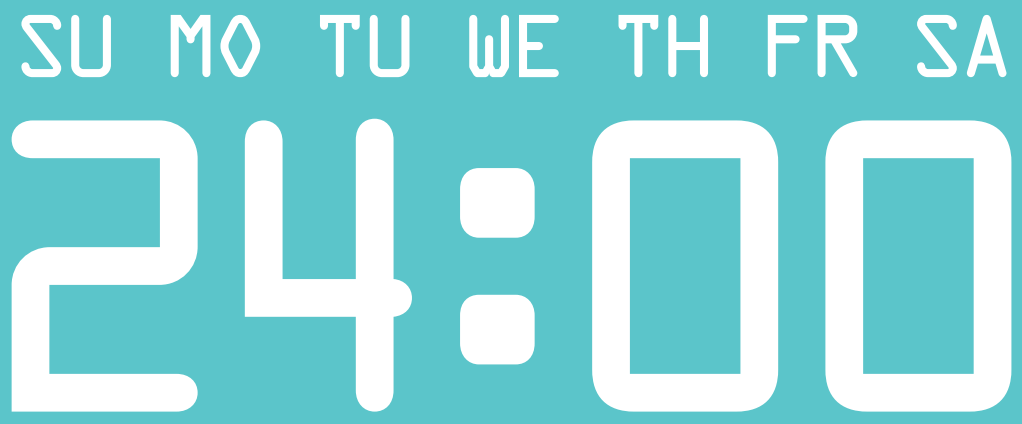
Your data aggregation partner should have your full and complete trust. Don't be afraid to ask them about their experience and their relationships with financial institutions. Also, check into their general reputation in the industry through peers, forums, and industry news. The right data aggregation partner has nothing to hide.

QUESTIONS TO ASK

- **How many years has the provider been in the business?**
- **Which certifications have they earned? Going through the process of earning certifications such as the ISO/IEC 27000 family of standards and PCI DDS demonstrates a strong focus on security that other providers may lack.**
- **Does the provider have a relationship with financial institutions?**
- **Can they answer your questions in terms of storing data, security credentials, etc.?**
- **Will the provider offer guidance if you need it?**

DOES YOUR PROVIDER:

Offer 24/7 Support?



Validating a provider's security standards doesn't end when you sign the papers. Making sure your standards align is an ongoing process that requires consistent check-ins, validation, 24/7 support and scalable customer support programs that grow as you do.

QUESTIONS TO ASK

- **Will your provider constantly be there to monitor connections with banks and provide support 24/7?**
- **Will your provider schedule regular site audits to insure your system integrations run smoothly?**
- **Will they continue to be there over the long term?**

Meet Yodlee Interactive: A Proven Certified Data Aggregation Provider

When you partner with Yodlee® Interactive to build next-generation digital financial apps, you'll benefit from streamlined access to data, payments, and extensive digital security. The Yodlee Interactive financial cloud offers one of the most robust financial data platforms in the world. It delivers bank-level security, encryption, risk management, and APIs enabling flexible, innovative, and multi-channel distribution solutions. With more than 16 years' experience integrating into the largest banks in the world, security is in Yodlee Interactive's DNA.

Yodlee is the leading provider of digital financial services in the industry and leverages financial data from over 14,000 global sources. As a pioneer in bringing SaaS applications to the financial services industry, and an FFIEC supervised Technology Service Provider, Yodlee Interactive has extensive experience in meeting the highest standards in data security, privacy, and regulatory compliance.

CONCLUSION

Aggregation-based technology is powering exciting digital financial solutions that are changing the way people interact with their personal finances. These solutions can help you create more personalized financial experiences and empower customers against fraud with transaction analyzing and alerting tools. To develop the powerful financial applications that consumers want, you need a best-of-breed financial data aggregation provider — one with a secure, scalable data infrastructure that safely brings together disparate, personal financial information from all over the web. The best way to find this trusted partner is to ask the right questions.

HOW CAN I LEARN MORE?

- Download the white paper "How to Choose an Aggregation Platform"
- View the webinar "How to Choose a Financial Data Platform and Aggregation API"

ABOUT YODLEE INTERACTIVE

Built on the foundation of Yodlee's 16 years of aggregated consumer financial data, Yodlee Interactive empowers visionary entrepreneurs, partners, and developers to build the next generation of disruptive and innovative FinDat (financial data) solutions using the award-winning Yodlee platform.

Yodlee Interactive is focused on making the Yodlee platform available everywhere that value can be created by entrepreneurs, partners, and developers to build digital financial apps and services. As the architects of a new digital ecosystem, Yodlee Interactive optimizes the wisdom of the financial technology crowd to create, catalyze, and distribute innovations faster through an open and secure data API. Used by hundreds of companies, both small and large, Yodlee Interactive is the horsepower behind today's coolest and most personalized digital experiences.

For more information, visit: **yodleeinteractive.com**