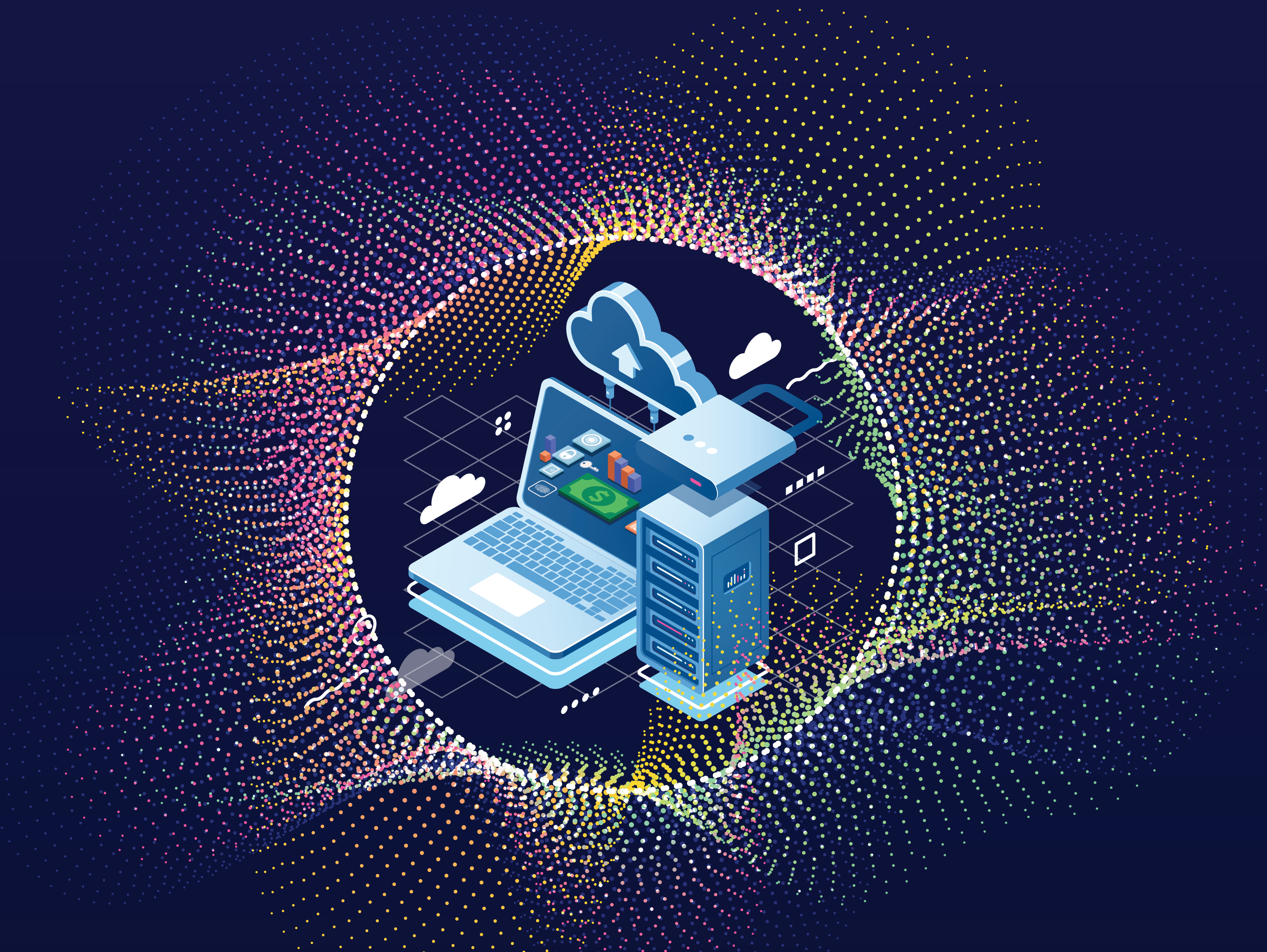
WHITE PAPER

Selecting a Financial Data Integration Platform

Key Vendor Evaluation Criteria for Fintech Adopters



Authored by LendIt Fintech

Sponsored by fiserv.

CONTENTS

1. The Role of Data Aggregation in Fintechs' Strategies

"Data is the new oil," argues Linda Jeng, a senior fellow at Georgetown Law and former Federal Reserve official. "If you have access to data, then you have the ingredients to build better services."[1]

For fintechs, building those apps and services relies on access to a wide set of customer financial data. As an example, envision an app that has secure, permissioned access to all of a consumer's bank, investment, credit and loan, tax, and insurance accounts. It presents all account information in one dashboard, monitors balances, advises on budgeting, supports loan underwriting, recommends savings techniques and investment portfolio allocation, and proposes new financial products. Other data-driven solutions may be more niche, but all depend on real-time information coordination.

Establishing access across tens of thousands of financial institutions, account types, and data sources is a monumental task. Varying regulatory regimes and APIs for connection to data providers require dedicated solutions for connectivity. Fintechs generally lack the focus, resources and expertise to build and maintain these. **Enter: data aggregators.**

Through partnerships with banks and other financial institutions (FIs), data aggregation platforms add a critical access layer. They are "facilitators," each with purpose-built technology to rapidly and reliably supply data as consumer demand for apps beyond traditional banking grows.

Platforms each offer unique strengths. Platform providers differentiate themselves in everything from their relationships with FIs to the mechanics of data structure. They vary in privacy controls and data use too. These differences and others underscore the importance of intelligent evaluation when selecting a platform partner.

Categories of Evaluation Criteria for Selecting an Integration Platform:

- Data Reliability and Cleanliness
- Coverage of Institutional Sources and Data Type Handling
- Platform Adaptability & Support for Innovation
- Security Practices
- Privacy, Transparency & Compliance

This paper details important platform selection criteria. Evaluation insights are based on interviews with leading data aggregation platform providers, as well as experienced US fintechs. Note that banks and other FIs not only deliver customer data but also consume data in their own customer applications. The findings herein also apply to these organizations.

1. https://www.politico.com/news/2020/02/07/banks-fintech-startups-clash-over-the-new-oil-your-data-112188

2. Key Platform Evaluation Considerations

i. Data Reliability and Cleanliness

Reliability refers to a platform's ability to maintain continuous, live connections to data sources and to correctly extract data. Cleanliness addresses data integrity, as well as efficient, easy-to-handle data structures.

Data reliability shortcomings are the death knell for financial apps. If the complete picture of customers' information requires multiple interactions or is interrupted by incomplete data pulls, then higher abandonment and churn will follow.

When considering reliability, fintechs will benefit from evaluating it in context. The performance of data integrators is impacted by regular infrastructure changes at FIs and application updates at thousands of institutions. This is one sector where "uptime" (i.e., the data access success rate) is measured in the low-to-mid 90 percent range. Note: the actual uptime of aggregators' internal systems is more akin to Six Sigma rates and measured separately in SLAs.

Because the integration platform providers are beholden to FIs as data sources, they differentiate on consistency and responsiveness to broken data connections. According to Kevin Hughes, Senior Product Manager, Data Aggregation Services at Fiserv, "**The real question is 'If something's broken, how fast can you get it fixed?'**"[2] Lowell Putnam, Head of Partnerships at Plaid, believes data aggregation is in essence a "maintenance business."[3] He asserts that what matters is, "**What percentage of your code base is built to monitor your own code?**"

Hughes also cites the depth and proactiveness of FI relationships as a reliability indicator. "Banks may call, advise that changes are coming and provide a test account to assess disruption. We can respond with script or API call changes, and 80 to 90% of the time make fixes in less than 24 hours. For clients with millions of users, even small percentage improvements in a platform's data access is meaningful to the end user experience."

The reported dispute between PNC Bank and P2P payments app, Venmo, highlights the criticality of stable data connections.[4] Citing "security enhancements," PNC Bank prevented aggregator access to its customers' accounts, disabling information flow for Venmo's end users via its integration platform. While the nature of access disputes varies, aggregator and bank frictions exist, and, until the industry defines clear parameters for the terms of access, good relationships help facilitate resolution.

Fintechs expect their data fast. But Bob Sullivan, President of FinancialApps, suggests that they underestimate a related factor – cleanliness. "Whether data is aggregated through scraping, direct connection, or open APIs like those supported by the Financial Data Exchange, it needs structuring to make it consumable. Companies' data sets may include legacy fields. **Either the integrator needs to reorganize their data structures or the burden falls to fintechs to strip out this excess.**"[5] This adds a technical and costly data preparation step.

The ease of using the delivered data is affected by the design of the calling APIs. Platforms should encourage prospective clients to experiment with their API set before committing to a platform.

2 LendIt & Fiserv - Interview January 2020
3 LendIt & Plaid - Interview February 2020
4 https://www.finextra.com/newsarticle/34970/pnc-bank-customers-locked-out-of-venmo-by-data-access-dispute
5 LendIt & FinancialApps - Interview February 2020

Key Takeaways: Data Reliability and Cleanliness

- Connectivity to thousands of data sources isn't perfect; mid-90% source access success is typical
- Platforms are differentiated on timeliness of re-connections, based on the quality of their FI relationships
- Clean and well-structured data reduces preparation costs and technical complexity

ii. Source Coverage, Data Types, and Access Methods

Coverage refers to the number of institutions from which a platform accesses data. This access is derived in a variety of ways, from direct FI connection to unstructured screen parsing. One also must consider the domains (e.g., consumer banking, small-to-midsize business activities, investments, taxes, utilities, insurance) from which a platform can accommodate information. Finally, there's the type of data elements captured, whether basic transactions and balances, meta-data about rates, fees and terms of an account service, or supplemental data such as loyalty points associated with a credit card.

Although platforms may advertise coverage of 15,000 to 20,000 connections across banks, credit unions, utilities, and beyond, these counts aren't necessarily core differentiators.

"Counts [from marketing] mean nothing to me," says FinancialApp's Sullivan. Everyone has thousands of them. What it really comes down to is how they count. Is Wells Fargo and its six subsidiary banks one connection, or is it seven?" He finds that **the long tail of connections is where platforms differentiate**. "If the count expands the footprint of smaller credit unions and banks, then it matters."

For Kevin Hughes of Fiserv, this long tail coverage is important for fintech companies' customer satisfaction. "As fintechs build their applications to appeal to the broadest possible customer base, they need to ensure accessibility to a full range of financial institutions. This sustains a great overall user experience. While they may not add small banks or credit unions every day, they should have these institutions available if a new user tries to connect tomorrow."

Similarly, Ryan Christiansen, Senior Vice President for Data Access at Finicity isn't convinced coverage volume is a top concern as "most platform's core data models are similar." Instead, he believes a platform's ability to access needed data is what fintechs should verify. "All solution providers have some degree of specialty," so source and data type coverage is a major consideration.[6] He advises that **fintechs should understand which information elements are mission critical to their application** (like tax, credit or bill payment data) and do a gap-analysis with a provider to understand how the data is accessed.

Much of the data for small-to-medium sized business financial activity is similar to consumer banking data, and thus also is covered in the integration discussion. This is a growing area of information use.

Coverage increasingly is facilitated through financial industry standards for open APIs. This is akin to the mid-1990s as the market for computers, phones and headphones grew. At that time, technology companies sought a standard for short range wireless communications. Today, over 30,000 brands have standardized on Bluetooth. PwC notes the parallels to data sharing today:

> **"The secure exchange of data through an industry-backed standard could replace the tangle of incompatible APIs and custom data-sharing arrangements. Through the launch of the Financial Data Exchange (FDX), a broad cross-section of banks, Fintechs, and financial services groups have aligned around a single data-sharing standard that could accelerate the adoption of open-banking API frameworks."**[7]

While FDX is just one of several US-centric standards that reflect progress with open-banking API frameworks, the US still lags the EU's Payment Services Directive (PSD2) in terms of participation and technical specifications. This means that one-off data sharing arrangements and unstructured, or "screen scraping", approaches are extant in the US. But direct FI connections in specialized

6 Lendit & Finicity - Interview January 2020

7 https://www.pwc.com/us/en/industries/financial-services/library/fdx-data-sharing.html

standards like FDX, Akoya and Durable Data offer cleaner, better formatted and more robust data.

"Instead of direct connection, some platforms parse information presented on the screen. This increases data cleansing requirements, grows the likelihood of errors and can impact the downstream product experience," says Finicity's Christiansen.

While screen scraping in a legacy sense is problematic in terms of accuracy, reliability and security, the market is migrating away from it. Plaid's Putnam notes that old-fashioned HTML website parsing is increasingly uncommon. Moreover, many banks including JPMorgan Chase are ending screen-scraping styled access and pushing API-based dashboard connections.[8]

But one provider cautions against worrying about platforms' source access methods altogether. Instead, they suggest focusing on what matters: data quality. "We use whatever means necessary to get the job done right – specifically, to provide quick, comprehensive and filtered data."[9]

Key Takeaways: Source Coverage, Data Types, and Access Methods

- Direct connection is preferred to an unstructured approach (i.e., screen-scraping)
- # of data access points matter, but data quality matters more
- Assess whether the data elements needed coincide with the data elements available

iii. Platform Adaptability and Support for Innovation

As fintechs build a wider range of personalized offerings, platforms' data access must be adapted to support evolving business models. Kevin Hughes from Fiserv notes that **"an expedited path to new offerings is critical. Additional data needs to be available in days or weeks, not months."** Adaptability means that a platform provider, working with its sources, can rapidly adjust the structured data provided to its customers' needs.

Bryan Garcia, CTO at FinLocker, shares how this flexibility enabled a business model adjustment early on. "We needed historical data beyond the standard 90 days and worked [with a platform provider] to pull 12 to 24 months for our new use case."

At one point, Garcia's team re-evaluated their aggregation provider and asked a competitor about flexibility. "They basically said, 'This is the data we pull; no more, no less'."[10]

Fintechs may need flexibility to move beyond traditional deposit accounts into bill pay or insurance, for example. Here, companies need to understand the vendor's architecture and flexibility. Hughes of Fiserv explains, "Our APIs are configurable so I can turn something on for one customer that I don't need to for everyone. Other platform providers see this as custom development work and are going to pass on those costs."

Productizing common data uses via applications from a platform is another innovation area. One example: AllData® PFM from Fiserv. This personal financial management tool aggregates data from most any online financial source, and applies balance and transaction alert, expense categorization, budgeting, and customized spending insights in a ready-made PFM solution. Users can embed these widgets into their app or service, or integrate into an existing banking site, as a value-add for end users.

Depth of partnership also signifies a platform provider's commitment to adaptability and innovation. FinLocker's Garcia recalls the initiative Fiserv took when FinLocker pursued Day 1 Certainty® approval for its asset verification solution with Fannie Mae. With this program, lenders can access asset verification reports to accelerate pre-approvals for their borrowers in minutes.[11] But Fiserv also

8 https://bankinnovation.net/allposts/operations/comp-reg/inside-the-chase-ban-on-screen-scraping/
9 https://www.morningstar.com/lp/quality-client-data
10 LendIt & FinLocker - Interview February 2020
11 https://singlefamily.fanniemae.com/media/9011/display

needed its controls and processes audited by Fannie Mae.

"They didn't come back and charge us," said Garcia. "They knew it would make all of us better and went through an 18-month certification. In talking to Fannie Mae, it was clear that not all third-party aggregators were willing to go to such lengths."

All the platform executives interviewed for this paper urged prospects to clearly understand their customer needs and use cases – data sets and structures, response times, insight strategies – before deep platform evaluation. The platform provider then can counsel on design and facilitate fast deployment. This **customer-centric planning often distinguishes those fintech market leaders with a killer app, from the rest of the pack**, according to FinancialApp's Sullivan.

Key Takeaways: Platform Adaptability and Support for Innovation

- Business models change; ensure that a platform can quickly expand the range and type of available data
- New apps and data insights reflect a platform provider's commitment to innovation
- Are fintechs viewed as partners, or is every service an upcharge?

iv. Security Practices

The protection of data by the integration platform on behalf of its data users and sources is a fundamental concern. In periods of disruption, such as the COVID-19 pandemic, concern heightens as consumers increasingly rely on digital applications to complete financial transactions.

Ken Blanco, the director of the Financial Crimes Enforcement Network, a bureau of the U.S. Department of the Treasury, describes the tense reality of data aggregation security: "FinCEN has also seen a high amount of fraud ... enabled through the use of synthetic identities and through account takeovers via fintech platforms," Blanco said. "In some cases, cybercriminals appear to be using fintech data aggregators and integrators to facilitate account takeovers and fraudulent wires."[12]

This creates a delicate dance between aggregators and financial institutions. Banks prioritize customer data protection and, naturally, worry about the liability of a data breach in conjunction with an aggregator. This prompts vigilant monitoring of aggregator traffic and screen scraping activities. If banks sense anything abnormal, they will cut off data access, disrupting app experiences.

Moreover, insecure practices can invite regulatory intervention. In 2018, FINRA issued warnings about data sharing with aggregators, and in 2019, the FDIC inspector general also raised public concern.[13]

For fintechs, an aggregator's security approach matters for two key reasons. First, any data loss poses significant reputational threat. Second, data connectivity relies on the FI's comfort with an aggregator's security.

During the evaluation process, fintechs should determine:

- Does the platform provider follow industry best practices in network security design and implementation? For example, separate production, staging, development, corporate and specialty networks should exist, and access controls should be in place between each zone.
- Are other key controls in place: multi-factor authentication, token-based access credentials (like OAuth), resilient and redundant infrastructure, and data encryption?
- What other FI-critical systems has the platform providers maintained? These security experiences may inspire confidence in data users.
- Is the aggregator's annual System and Organization Controls (SOC) report available for review?
- What data retention policies exist? Including, understanding what happens to customer data after account termination or deletion.

12 https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-federal-identity-fedid

13 https://www.forbes.com/sites/nizangpackin/2020/01/27/show-me-the-data-about-the-money-what-you-didnt-know-about-data-aggregation-can-hurt-you/

Data transmissions should employ end-to-end encryption, including encrypted data in motion. Tim Klemmer, Public Relations Chairman within the Corporate Communications working group at Financial Data Exchange (FDX), concurs. "If a platform is going to be viable, the data running through it must be encrypted at all times. And if an FI provides tokens representing customers, that platform should never hold those where data is stored."[14]

Key Takeaways: Security Practices

- Data connectivity relies on the bank's comfort with a platform's security
- End consumers and regulators are increasingly focused on data sharing practices
- Evaluate security best practices to increase consumer confidence and reduce potential data access disruption

v. Privacy, Transparency, and Compliance

While 54% of U.S. banking consumers use apps to help them manage money, 80% are not aware that apps may store their bank account credentials. Only 21% are aware that access is open until a user revokes their credentials.[15]

Although one might first look to the FIs and application providers as the primary repositories and custodians of customer data, integration platforms also cache data. Because few privacy-related restrictions govern data held by aggregators, some providers have anonymized it and sold it to third parties without clearly notifying consumers.

Lawmakers are pressing the Federal Trade Commission to investigate aggregators' data sales, though, given reports that even "anonymized" data can be unmasked using metadata and restructuring techniques.[16] Look for clear delineation of data use and notification practices in the platform provider's terms of service. Certain platforms declare outright that they will never sell data to a third-party.

Consumer unease highlights the need to understand aggregators' data practices. FINRA recommends fintechs ascertain:[17]

- **What rights are being granted with respect to access.** For example: how often are accounts scraped and data retrieved?
- That access is only for the service the customer elects to use.
- What type of liability, if any, does the aggregator bear in the event of 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?
- How do customers terminate data access and rights?

Some aggregators offer portals for consumers to monitor and control data use across the apps using a platform. Others provide customizable code letting their customers present all accessed data sources to their end users.

While fintechs' liability with respect to consumer data is real, other compliance responsibilities are pronounced as well. Platforms can help. "There are a lot of regulations in payments or credit decisioning. Platforms should have experience in a market and know the nexus points between data and regulations, like Fair Credit Reporting Act," Finicity's Christiansen shares. "They should be making their fintech partners aware of any compliance steps too."

Key Takeaways: Privacy, Transparency, and Compliance

- Data sharing is lightly governed for aggregators. Understand what a platform provider does and doesn't do with consumer data.
- Consumer control is paramount; evaluate what tools a platform has to guide information sharing

14 LendIt & Klemmer Interview January 2020
15 www.forbes.com/sites/nizangpackin/2020/01/27/show-me-the-data-about-the-money-what-you-didnt-know-about-data-aggregation-can-hurt-you/
16 https://www.vice.com/en_us/article/jged4x/envestnet-yodlee-credit-card-bank-data-not-anonymous
17 https://www.finra.org/investors/alerts/be-mindful-data-aggregation-risks

3. Forging a Future with a Data Platform

Fast, clean and wide-reaching data access drive innovations. For fintechs pulling consumer or SMB financial data, understanding the extent of these in a platform is critical. So too is understanding security and compliance as the stakes around consumer data handling grow.

Beyond these evaluation points, Kevin Hughes of Fiserv reflects on the necessity to think big picture: "Your fintech won't be the same company a year from now that you are today. From a relational standpoint, is this a platform provider you can grow your business with?"

About Fiserv

Fiserv, Inc. (NASDAQ: FISV) aspires to move money and information in a way that moves the world. As a global leader in payments and financial technology, the company helps clients achieve best-in-class results through a commitment to innovation and excellence in areas including account processing and digital banking solutions; card issuer processing and network services; payments; e-commerce; merchant acquiring and processing; and the Clover® cloud-based point-of-sale solution. Fiserv is a member of the S&P 500® Index and the FORTUNE® 500, and is among FORTUNE World's Most Admired Companies®.

Account Aggregation Services from Fiserv consolidate, normalize and enrich account data from more than 18,000 sources to provide end users with a comprehensive portfolio view of assets and liabilities held within their financial accounts. Financial institutions, wealth management firms, financial advisors, investors and mass market consumers rely on our AllData® Aggregation Services for financial planning, reporting and budget management.

Learn more about **AllData® Aggregation Services from Fiserv**

Join the conversation

USA | EUROPE | LATIN AMERICA

About LendIt Fintech

LendIt Fintech is the world's largest fintech event series dedicated to lending and digital banking. As finance undergoes a radical transformation, LendIt Fintech helps financial services leaders make sense of this rapidly changing world. With cutting-edge content and a focus on networking we are helping to shape the future of fintech. LendIt Fintech hosts three major conferences annually: LendIt Fintech USA, LendIt Fintech Europe, and LendIt Fintech LatAm, along with many smaller meetups and more intimate events.

For further information, please visit our website: **lendit.com**

Join the conversation