A New Era of Data Ownership in Finance

Navigating 1033 Compliance for Fintech Firms and Financial Institutions

Dodd-Frank Act Section 1033, the Consumer Financial Protection Bureau (CFPB)

KEY SUBJECTS

Key compliance factors

- Timeline considerations
- Consent & data ownership
- Data interoperability & seamless integration
- Additional considerations
- Heightened cybersecurity & privacy requirements
- Increased accountability & compliance monitoring

How to navigate 1033 with confidence

- Adopt open banking standards & APIs
- Future-proof your tech stack
- Invest in cybersecurity infrastructure
- Assemble cross-functional teams

Turning compliance into a competitive advantage

- Partnering with experts in fintech innovation

10Pearls as your fintech partner

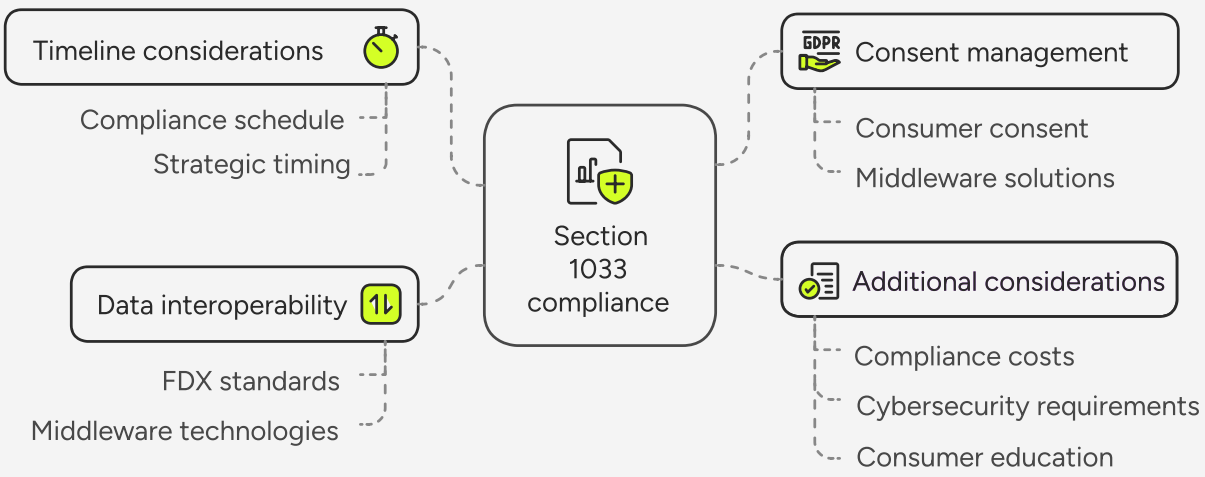
In its final rule implementing Section 1033 of the Dodd-Frank Act, the Consumer Financial Protection Bureau (CFPB) has set clear standards for consumer access to financial data. According to CFPB, data providers and authorized third parties must give consumers secure, efficient, and transparent access to their data.

- **Data providers** include financial institutions like banks, credit unions, and other entities that control or possess consumer financial data, such as digital wallet providers and payment apps.
- **Authorized third parties** are entities that consumers authorize to access their financial data.

1033 compliance in fintech presents new operational and technical challenges for companies, especially in the areas of data interoperability, cybersecurity, and customer engagement. This white paper examines these challenges and offers fintech companies solutions to align with the CFPB's requirements while capitalizing on growth opportunities.

Key compliance factors

The CFPB's final rule to implement section 1033 defines obligations for financial institutions and fintech firms, setting specific requirements for data accessibility, security protocols, and transparency in data-sharing practices. Compliance can benefit consumers by giving them more control over their financial data, but it poses significant hurdles for financial companies.



Timeline considerations

Many financial institutions may have felt some relief with the updated compliance schedule for section 1033. Most large financial institutions are already prepared to meet the requirements well before the April 1, 2026 deadline. However, there will be many who wait until the last minute to comply, hoping a basic core provider solution or CFPB reprieve will save them in the end, but waiting doesn't just present risks, it also causes financial organizations to miss out on new opportunities to provide innovative solutions to customers.

Data point:

Around 46% of US consumers are highly willing to use open banking for at least one product or service; that number jumps to 66% for millennials.

PYMNTS

Not only that, but it will also pose an inherent challenge with being able to maintain, grow, and expand service offerings as a primary financial provider. We predict that section 1033, along with various other factors, will accelerate mergers and acquisitions in the financial services space.

Here is the new tiered compliance schedule, outlining important implementation deadlines for financial institutions - but don't let this slow you down.

Implementation timeline for 1033 compliance

Tier	*Compliance Date*	*Depository Institutions*	*Non-depository Institutions* *(including fintech)*
1	April 1, 2026	At least $20 billion in assets	At least $10 billion in total receipts in either 2023 or 2024
2	April 1, 2027	At least $10 billion but less than $250 billion in assets	Less than $10 billion in total receipts in both 2023 and 2024
3	April 1, 2028	At least $3 billion but less than $10 billion in total assets	N/A
4	April 1, 2029	At least $1.5 billion but less than $3 billion in total assets	N/A
5	April 1, 2030	Less than $1.5 billion but more than $850 million in total assets	N/A

Consent & data ownership

In the past, access to consumer data has been made available to fintech firms through direct connections with financial institutions, standard protocols, and screen scraping. With section 1033, fintech firms will require consumer consent to access their data.

Financial institutions may assume this is a fintech requirement. However, financial institutions are well-positioned to manage consent and implement simple middleware solutions, and a new protocol will be insufficient to ensure the best possible consumer experience with the next generation of open banking solutions.

Consumers will need a way to manage their consent for third parties to access their data, allowing them to stay informed about specific data that will be shared, how it will be used, and the duration of their authorization. They must also be given the right to revoke this consent. While each fintech will need to track and maintain the consent it has been granted from each consumer, the financial institution should be the system of record for consent. It's most feasible for the consumer to go to their financial institution for a complete record of consent and to access revocation capabilities rather than going through hundreds of fintech firm applications to manage consent.

This will require investment in new consent management systems that act as an intermediary or governing system in between data access requests and data access fulfillment. These systems may have an opportunity to push consent changes out to fintech firms so they can take more immediate action to adjust their offerings.

Under the final section 1033 rule, fintechs can leverage open banking to access consumer-permitted data for secondary purposes like enhancing products and services or preventing fraud. However, they are prohibited from continuing to access consumer data beyond one year without reauthorization. As a result, the next generation fintech and financial institution systems must also accommodate reauthorizations. This applies for all fintechs even if they merely facilitate pass-through payments.

Data interoperability & seamless integration

In addition to managing consent, financial institutions will ultimately be required to adopt new standards for data interoperability and integration with fintechs in their role as "authorized third parties." No longer will they be allowed to restrict access to consumer data, so long as the consumer has provided consent.

The most likely winner in the standards race for data accessibility is the Financial Data Exchange (FDX). FDX is a non-profit industry standards body operating in the US and Canada that has spent most of the last decade working to unify the financial services ecosystem around a common, interoperable, and royalty-free technical standard for user-permissioned financial data sharing, aptly named the FDX API.

FDX has a global membership that includes financial institutions, financial data aggregators, fintechs, industry utilities, payment networks, consumer groups, financial industry groups, and other stakeholders in the financial sector.

Similarly, financial institutions and fintech firms will need to invest in new middleware technologies and technology partnerships to accelerate their support for FDX, while FDX facilitates the achievement of interoperability and third party access to data across their legacy systems, third-party platforms, and newer technologies.

Unfortunately, it may be difficult for smaller financial institutions to allocate sufficient resources to manage these demands, which could put them at a disadvantage in the marketplace. Again, it is advised that regardless of the timeline considerations outlined above, all financial institutions need to start moving now to comply and thrive in the future.

Additional considerations

There are three other areas that financial institutions and fintech firms should consider as they move forward with section 1033 compliance:

- **Compliance costs and resource constraints** – Any new set of rules has the risk of adding to the compliance burden already being faced by financial institutions. As previously stated, new costs will include the cost of managing consent, supporting new data-sharing protocols, and securing new technology partnerships. Apart from initial setup costs, section 1033 compliance will require continuous monitoring, auditing, and reporting over time.

- **Heightened cybersecurity and privacy requirements** – In the longer-term, section 1033 compliance is likely to reduce cybersecurity and privacy risks over current data access mechanisms, particularly related to screen scraping. However, in the short-term, financial organizations will need to ensure that support for data sharing and access are implemented in a way that leverages the best-of-breed cybersecurity frameworks to prevent breaches. Both financial institutions and fintech firms must ensure that all data-sharing processes are seamless and secure, which involves implementing authentication systems that verify user identity without creating unnecessary user friction. Managing this balance is difficult, and any misstep could result in non-compliance, consumer frustration, or even regulatory penalties, if consumer data is compromised.

  Increased data privacy requirements under section 1033 will also demand rigorous data access controls, particularly around consent management solutions and practices. Consent management frameworks must honor user preferences consistently and not allow edits by bad actors.

- **Consumer education on data access rights and security practices** – As with any new and significant change, both financial institutions and fintech firms will need to work together to provide consumers with detailed, accessible information about their data access rights. This will ensure that users are informed about how they can access, control, and share their data. By proactively educating users, financial organizations can help consumers make informed decisions about sharing their financial data, fostering the transparency, control, and autonomy that section 1033 aims to provide.

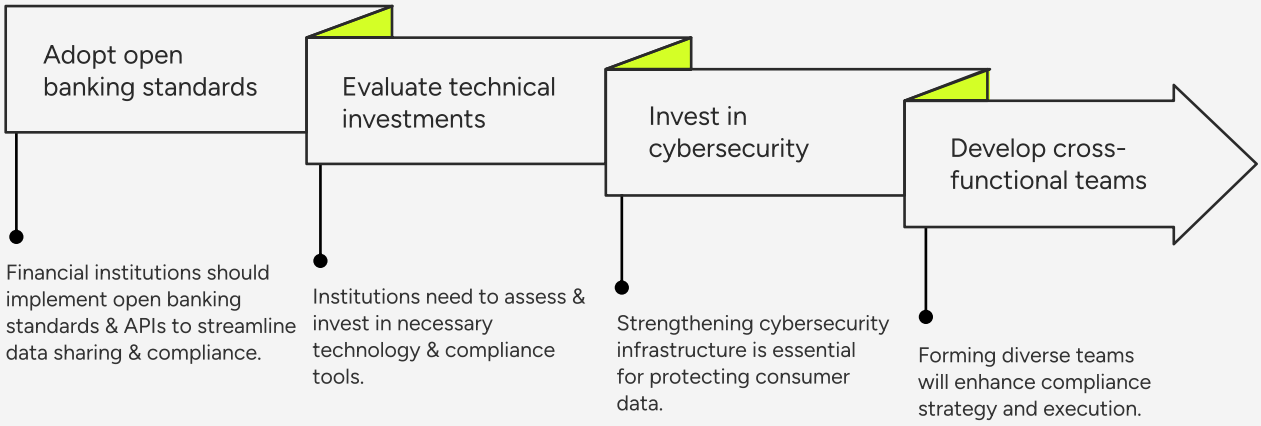
  A well-informed consumer base also helps financial organizations manage consent more effectively, a critical component of 1033 compliance. When consumers understand their data rights, they are more likely to engage thoughtfully with consent management processes, providing explicit permissions for data sharing.

How to navigate 1033 compliance with confidence

Achieving 1033 compliance can be a complex task for financial institutions. With evolving regulatory landscapes, ensuring adherence while maintaining operational efficiency is more critical than ever.

Here are some recommended next steps for financial institutions and fintech firms as they navigate the compliance and opportunities of section 1033:

Strategic steps for section 1033 compliance



Adopt open banking standards & APIs

As stated above, the FDX API ensures a secure, efficient means of providing consumers with real-time, structured access to their data, which will dramatically facilitate the rollout and adoption of section 1033 in a cost-effective manner. By following these open banking standards, financial organizations can reduce complexity when handling consumer data. With consistent standards in place, financial institutions and fintech firms can more quickly position themselves to fulfill consumer data requests, automate responses, and avoid the operational burdens of handling data inconsistently.

Advancing standardization will allow financial organizations to streamline secure data sharing and reduce the costs of supporting access to data as mandated by section 1033. The FDX further provides user experience, security, and compliance best practices that align closely with the regulatory demands of section 1033. This unified approach simplifies compliance management, reducing the likelihood of errors and easing the reporting process when demonstrating compliance with regulators.

Future-proof your tech stack

Financial institutions will need to consider how to best tackle section 1033 compliance in a way that makes the most sense for their institutions. This is likely to include a variety of buy vs build partner decisions and technology partnerships. Relevant investments include:

- Enhancements to identity and access management frameworks to validate incoming requests
- Middleware and messaging support for open banking standards
- Consent management platforms, including digital self-service solutions to make changes
- Compliance platforms with reporting tools that make regulatory tracking more straightforward

Invest in advanced cybersecurity infrastructure

Building trust through strong data security is essential for financial institutions and fintech firms across digital transformation initiatives. By investing in advanced cybersecurity measures, financial organizations can ensure that consumer data is well-protected from unauthorized access or breaches. This protection is essential for meeting regulatory expectations and providing consumers with a safe platform to access their data without fear of compromise. Strong cybersecurity best practices also enhance consumer trust, as customers are more likely to engage with a platform that takes their data security seriously.

By investing in cybersecurity best practices, fintech firms can align with section 1033's requirement for secure data access, providing consumers with the confidence that their financial information is safe. Moreover, cybersecurity investments help firms detect and respond to potential breaches more quickly, enabling rapid responses that can mitigate damage and protect consumer information.

An effective strategy and execution team that leverages these new opportunities will set apart the winners from the losers. Financial organizations should bring together professionals from various departments, including strategy, legal, IT, cybersecurity, customer service, and data management, to consider and address section 1033 requirements comprehensively.

Data point:

Financial services companies with close cooperation between compliance and strategy teams reported a 20-40% reduction in compliance issues.

McKinsey

With expertise spanning different functional areas, these teams are well-equipped to interpret the nuances of section 1033 and implement solutions that align with regulatory expectations. By fostering collaboration among departments, financial organizations can ensure compliance is integrated across operations rather than treated as a siloed function. Where outside expertise is required, financial organizations should consult with trusted technology partners and legal counsel to ensure the efficacy of their strategies and approaches.

Turning compliance into a competitive edge

The CFPB's final rules for section 1033 compliance create a new regulatory landscape for financial institutions and fintech firms, demanding enhanced data access, security, and consumer engagement solutions. While these requirements can strain resources, financial institutions and fintech firms can successfully navigate the challenges and achieve success so long as they proactively invest in open banking standards, make requisite technology and cybersecurity investments, and successfully collaborate across cross-functional compliance teams. These strategies will help not only ensure compliance but thrive in building trust and long-term consumer loyalty.

Partnering with experts in fintech innovation

10Pearls is an end-to-end product engineering company that ensures the success of your product development initiatives as you move from strategy to implementation. We help organizations achieve:

- Next generation user experiences
- Award-winning digital applications and features
- Secure and scalable solutions
- Excellence in integration and technical design

Our financial services bring you decades of experience with financial institution and fintech innovation along with dedicated practices devoted to leveraging the best advanced technologies to meet your goals. With over 1,300 resources worldwide, we bring financial institutions, fintech CEOs, technology and product leaders the knowledge, skills, and talent they need to realize their vision and succeed in financial services.

Choosing 10Pearls as your fintech partner

10Pearls is a custom mobile application development company that helps fintech firms innovate with advanced technology. With a variety of outsourcing models, development locations, and engagement options, we tailor our financial services to meet your unique needs and budget.

Our deep expertise in finance and open banking, global team of top tech talent, 24-hour development cycles, and collaborative culture make us one of the top fintech app development companies and the perfect partner for 1033 compliance in fintech.

Reach out today to discuss your project with one of our fintech app development experts. Let's connect.