SEPTEMBER 25, 2023 FINANCIAL SERVICES INSIGHTS

NAVIGATING REGULATORY AND COMPLIANCE REQUIREMENTS IN FINANCIAL DIGITAL PRODUCT DEVELOPMENT

By Rob Murray
Industry Leader for Banking, Financial Services, & Insurance

In financial digital product design, innovation is often fused with the call to meet regulatory and compliance requirements- and with good reason. As technology continues to evolve, so do the legal and ethical considerations surrounding the creation and use of digital products in financial services. Adhering to these legal and regulatory rules can be a complex endeavor, but it is essential that they be included in the design to both build customer trust and protect financial institutions and their users.

Understand the Complex Regulatory Landscape

The first step in meeting regulatory and compliance requirements is gaining a thorough understanding of the applicable federal and state laws, regulations, and standards that pertain to digital product development. There will be many complicated regulatory and compliance requirements to consider, including data privacy and security, cybersecurity protections, and consumer confidentiality.

The stakes are high. Privacy considerations have become increasingly important in the digital age, especially with users in banks and credit unions more concerned with how their data is collected, stored, and used. As a result, developers of digital products must now understand and incorporate privacy and security measures into the product's design and development process.

Promise data protection and strengthen cyber security

With the growing sophistication of cyber threats, and data breaches seemingly making daily headlines, assuring the privacy and security of user information is not only a legal and ethical obligation, but also a crucial component of building user trust.

In the last few years, numerous companies have fallen victim to data breaches and cyberattacks. Many of these have resulted in stiff financial penalties and loss of trust by customers. According to Statista, as of 2023, the average cost of a data breach in the worldwide financial services industry was $5.9 million. More concerning, in 2022, the US Securities and Exchange Commission (SEC) fined more than two dozen banks a combined $1.8 billion for failing to have proper communication security checks and balances in place.

All of this points to one very important conclusion: securing user data is non-negotiable. Depending on the nature and sophistication of the digital product, financial services development teams will need to include cloud-based data loss prevention (DLP) measures into their designs, along with encryption and two-factor authentication. Financial services companies also will need to conduct on-going security audits and vulnerability assessment strategies to safeguard user data. Development teams should keep in mind that the less information a financial organization collects, the less attractive the digital product becomes to potential cyber attackers.

Additionally, in the case of a data breach or security incident, all banks, credit unions, and other fintech companies should have a comprehensive incident response plan that outlines the necessary steps to take in the case of a security breach. This plan should include how to contain the breach, how to notify affected users, and how to communicate with internal and external stakeholders.

Most financial digital product developers now include encryption within their designs, which plays a pivotal role in safeguarding sensitive data. Using encryption during storage and transmission of data adds an extra layer of protection, making it significantly more difficult for unauthorized parties to gain access to valuable consumer information. Incorporating strong encryption protocols into digital product design also affirms that even if a breach occurs, the stolen data remains indecipherable to attackers.

Finally, development teams should implement robust two-factor authentication mechanisms to prevent unauthorized access to digital platforms. Multi-factor authentication adds extra security by requiring users to provide multiple forms of verification before getting access to their accounts. Digital product development teams also should consider adding role-based access control, which ensures that users have access only to the resources and functionality that are necessary for their roles, thereby reducing the risk of internal breaches.

Conduct regular audits and compliance monitoring

Financial regulatory and compliance requirements are not static. They evolve over time as new laws are enacted and revised. Therefore, financial institutions must engage in regular audits and compliance monitoring of their digital products to ensure ongoing adherence to relevant regulations. This commitment to continuous improvement will help mitigate legal risks and maintain a reputation for reliability for the product and the organization.

Because of the dynamic environment in financial services, financial institutions will want to collaborate with their legal departments now more than ever. Legal departments can provide invaluable guidance in helping to interpret complex financial regulations, which will support development teams in building digital project features that legally align with compliance and regulatory standards.

Aim for user transparency

When developing digital products, transparency is particularly important in data collection and processing. Informing users about the types of data being collected, how it will be used, and who will have access to it is a cornerstone of legal compliance—and important in gaining and keeping end-user trust. Being transparent with customers will empower them to make informed decisions about their personal information, while strengthening confidence in their financial institution.

Additionally, development teams should also strive for transparency in communicating terms of use and privacy policies to consumers who are using these products. These documents should be written in clear, understandable language that is readily accessible digitally or in print.

Insure product and platform accessibility for all

Accessibility is a critical consideration for financial digital product development teams to prioritize, particularly to ensure that digital products are available for individuals with disabilities. Making certain that digital and web platforms are accessible to people

with disabilities is a priority for the Department of Justice, and required by the Americans with Disabilities Act (ADA). These guidelines provide a framework for making websites, mobile apps, and other digital products accessible to everyone. Adhering to these guidelines not only promotes inclusivity, but also can prevent legal action against companies for discrimination and accessibility violations.

While covering every aspect of the ADA is beyond the scope of this article, banks, credit unions, and other fintech companies will need to remember to include accessibility features that meet ADA guidelines. These may include screen readers, captioning, voice recognition, and keyboard navigation. The features will need to demonstrate a commitment to reaching a diverse user base.

Conclusion

Navigating the financial regulatory and compliance landscape is a multi-dimensional challenge that requires careful consideration at every stage of digital product development. By adopting an ongoing commitment of adhering to regulatory and compliance rules, digital product developers can create digital financial products that prioritize user safety, protect consumer information, instill confidence, and delight customers.

In other words, by understanding and skillfully navigating the regulatory landscape, digital product developers can create innovative financial products that meet and exceed regulatory and compliance requirements, while delivering an undeniably positive user experience. To get started, contact us.