securely navigating the future of banking

Staying Up to Speed on Digital Security Best Practices

Securing your accountholders' sensitive data is as much a strategic imperative as it is a regulatory requirement.

The Federal Trade Commission says consumers lost $8.8 billion to fraudsters in 2022, up 44% from 2021.[1] While a majority of consumers trust their financial institution's security measures, they're still apprehensive.[2] When you keep your data and your accountholders safe, you're ultimately safeguarding your organization's integrity by building (and keeping) trust.

staying in step with regulations

In an era when data breaches and fraud are on the rise, regulatory bodies are tightening their grip.

The Federal Trade Commission (FTC) is now empowered to issue privacy regulations to protect consumers. The recent proposal of the Personal Financial Data Rights rule to Section 1033 by the Consumer Financial Protection Bureau (CFPB) is a game-changer. This rule targets organizations like community and regional banks and credit unions, prohibits screen scraping, and mandates data sharing in machine-readable, standardized formats.

Gartner predicts that by 2023, 65% of the world's population will be covered under modern privacy regulations – which means keeping on top of these developments is crucial.[3]

digital security best practices

To successfully navigate the challenges of 2024, we need to address key security topics that impact not only your organization's stability and regulatory compliance, but also the trust your accountholders place in you.

Embrace Open Banking

In the pursuit of accountholder trust, providing ownership and privacy over financial data is non-negotiable.

Open banking, facilitated by secure API connections, serves as a crucial means for seamless financial data exchange. By adopting open banking standards and leveraging secure API connections, you'll create a standardized, secure, and controlled environment for data sharing. And by building this open and extendable ecosystem – through a combination of flexible and scalable next-generation technology and seamless integration of best-of-breed capabilities – you can ensure consumer-permissioned access for your accountholders.

Consumer-permissioned access empowers individuals and strengthens their relationships with you, their financial institution. It lets accountholders specify, use, and completely control their data and how it's shared with third-party providers, including the ability to give or revoke data rights inside the digital banking experience.

With transparent, machine-readable data exchanges, both you and your accountholders gain visibility into shared data, reducing errors and enhancing security.

Remove Screen Scraping

Screen scraping has been a thorn in the side of the financial industry, posing risks to data privacy and security.

In an era when **data breaches are on the rise**, regulatory bodies are tightening their grip.

The CFPB estimates that at least 100 million consumers have authorized third parties, including 9,000 banks and credit unions, to access their account data. That's why replacing screen scraping with API-enabled data sharing marks a new era of secure financial data exchange. Accountholders gain control over their data permissions, minimizing risks associated with indiscriminate data extraction.

Since 2022, Jack Henry™ has been working with the major data aggregators – Finicity, Plaid, Akoya, Envestnet | Yodlee, MX, and Intuit – to implement open API-enabled data exchange.

This effort has removed screen scraping from the Banno Digital Platform™ ahead of the implementation of the CFPB's new rule.

Automate Fraud Detection

Fraudsters are becoming increasingly sophisticated, with account takeover fraud increasing 354% year-over-year in 2023 and 422.1 million people affected by data breaches in 2022.[4]

In collaboration with Jack Henry, NuDetect (behavioral security technology by Mastercard® company NuData Security) offers a unique solution to this problem. By leveraging user data analytics, NuDetect defines normal behavior associated with account entry. It reinforces vulnerabilities, tracks user behaviors, and takes appropriate action, ensuring that suspicious login events trigger two-factor authentication and fraudulent events are promptly blocked.

The point of NuDetect is to differentiate good users from bad – before they do any damage.

Rather than solely focusing on fraud detection and prevention, NuDetect focuses its efforts on making sure good users have reduced levels of friction throughout their journey – whereas bad users don't get access to accounts and funds.

The point of NuDetect is to differentiate good users from bad.

securing your future

By addressing screen scraping, embracing data privacy through open banking, and adopting cutting-edge fraud detection tools, you're not just keeping up – you're staying ahead in safeguarding your accountholders' trust and your organization's integrity.

safeguard your sensitive data

Learn more about securely navigating the future of banking with a trusted partner at your side.

For more information about Jack Henry, visit jackhenry.com.

sources

1. Sarah O'Brien. *Fraud Cost Consumers $8.8 Billion Last Year, Federal Trade Commission Says*. CNBC. Accessed January 24, 2024.
2. *Half of Consumers Want More Security Measure From Banks*. PYMNTS. Accessed January 19, 2024.
3. *Gartner Says By 2023, 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations*. Gartner. Accessed January 23, 2024.
4. Becca Thies. *2024 Cybersecurity Industry Statistics: ATO, Ransomware, Breaches & Fraud*. Accessed January 23, 2024.

jack henry™