Banno Digital Banking Platform

security & fraud protection

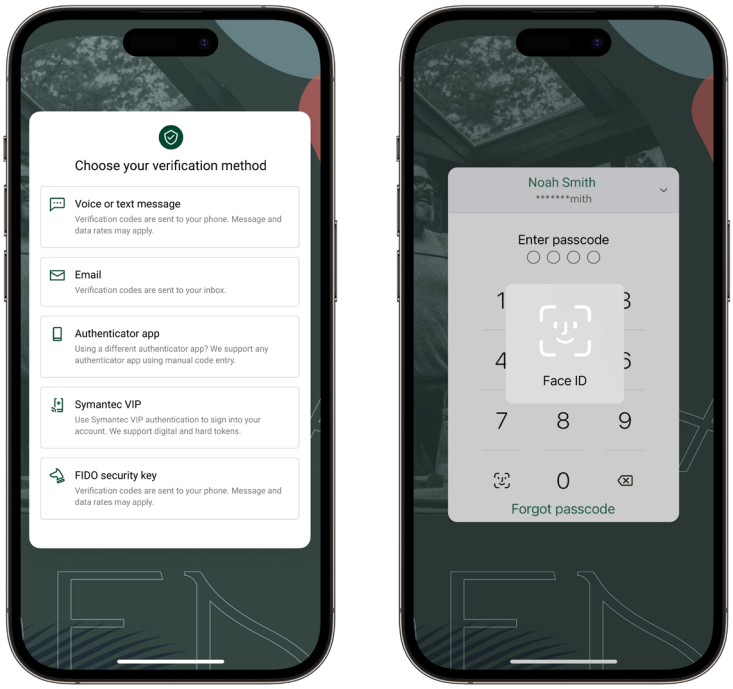
Fraud is top of mind for financial institutions everywhere, as it should be. Jack Henry knows the risk, and we spare no effort mitigating it.

safeguarding fast money movement

In keeping with modern security standards, Banno requires two-factor authentication for all users. Built-in Mastercard NuDetect analyzes user behavior, throwing red flags for account entry attempts that could be fraud. And we're doing away with screen scraping by establishing direct API connection with leading data aggregators – this preserves the ability for your accountholders to pass *only* the information necessary to get the most out of other fintech and encrypting it along the way.

meeting the gold standard

Two-factor authentication (2FA) has become the gold standard for account login. Banno requires it for all users to neutralize risks associated with compromised passwords, which can be easily purchased on the dark web. And the Banno 2FA options are so easy – for valid users – to pass that they hardly notice it's happening.



Double-Check Identity

Banno platform users must validate login attempts outside the app before they gain access to their account. 2FA is effective, because it asks users to produce something they *are* or something they *have* in addition to a username and password that – many times – can be purchased on the black market.

Two-factor authentication can be achieved on Banno via security keys (recommended), device biometrics capabilities (touch or face ID), SMS text message, voice calls, an authenticator app, one-time passwords, push notifications, and hard and soft tokens.

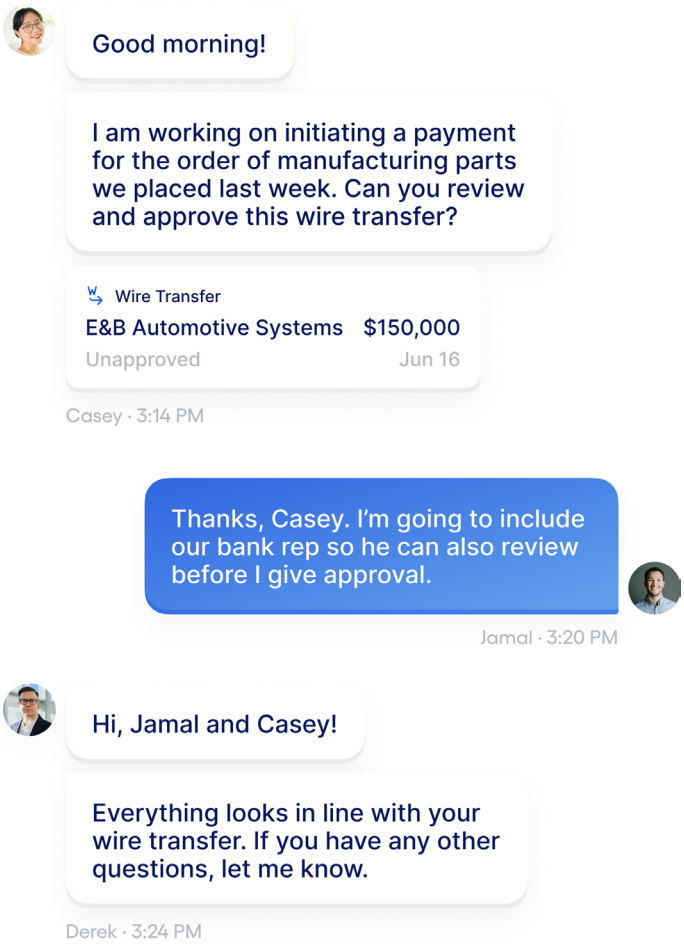
While security keys are the most secure 2FA options (and our number one recommendation for every business user), passkeys with biometric access are loved by users because it puts 2FA into a single step, and there is no threat of losing it – and Banno offers it. Their face or fingerprint is scanned by the device and verifies their identity. All they have to do is be themselves.

Remove Barriers to Service

Your financial institution's goals around being there for your accountholders whenever and wherever they need you are met by making "omni-channel" seamless. But most means of digital communication are not secure.

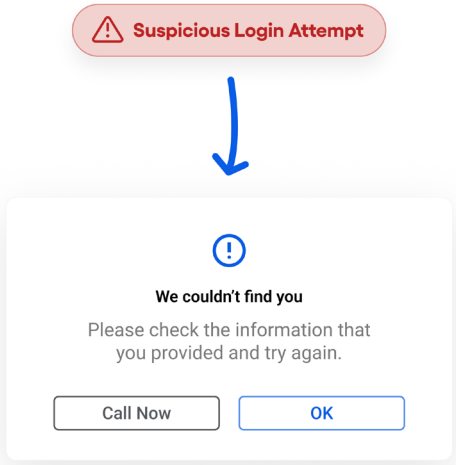
Two-factor authentication means your accountholders are fully authenticated when they're using Banno, which makes Conversations, our secure chat, a safe place for them to talk about account details, sign forms, and even initiate wires without having to drive to a branch. Your business users can even chat with their teammates in this secure channel and make approvals, leaving no room for email phishing fraud.

This seamless authentication promotes a continuous conversation between you and your accountholders, and it's woven seamlessly throughout the banking experience you provide.



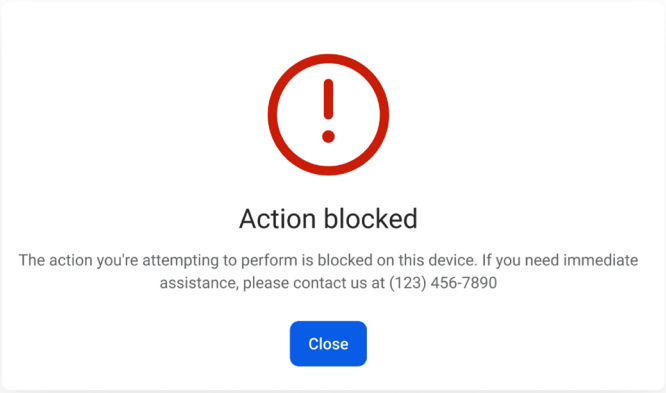
account takeover mitigation

Jack Henry is fully aware that digital banking account entry is a treasure storehouse for fraudsters. In fact, the Banno platform sees 1,800 invalid logins for every 15 valid logins – *per second*.



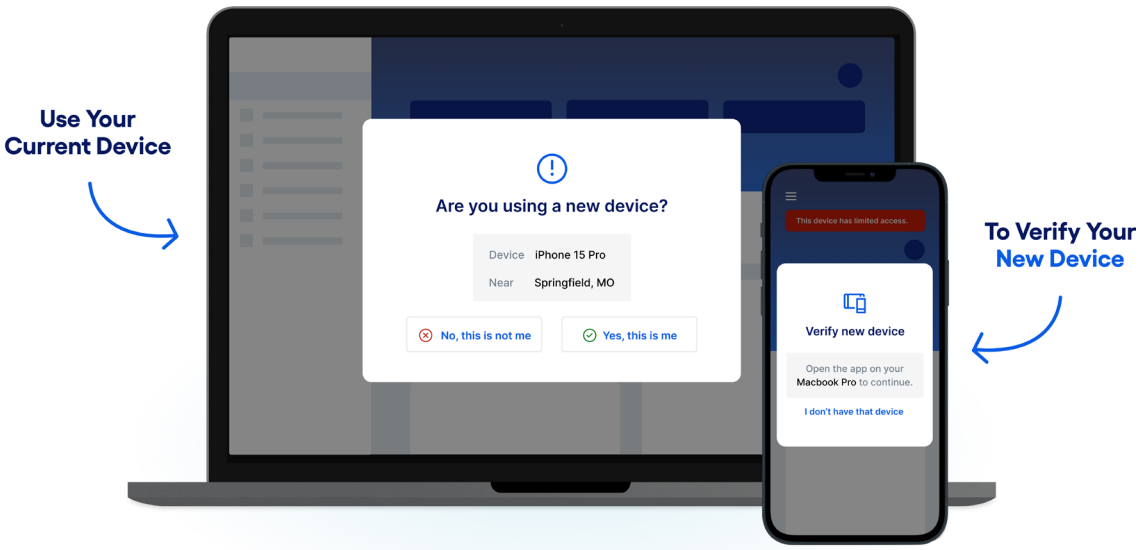
Prevent High-Risk Actions

Not all actions are created equal – some carry a higher risk. For sensitive actions that could impact your users' account security, like making an external transfer or updating their login credentials, Banno apps require an extra level of authentication. When a high-risk action is detected, your accountholder is prompted to re-enter their password correctly to continue, and a confirmation email is sent for added peace of mind. Because fraudsters target high-risk actions first, this safeguard ensures they're stopped before they even get a chance.



That's why, for new devices, we're providing flexible security modes that put you in control of how high-risk actions are managed:

- **Don't Block Mode:** Monitor device activity without restrictions, keeping the experience seamless for your users.
- **Waitlist Mode:** Hold high-risk actions on new devices for seven days – slowing down potential fraud with minimal impact on legitimate users.
- **Blocking Mode:** Provide the highest level of control by restricting all high-risk actions on new devices until authorized members of your team clear them, empowering you to take a proactive stand on account security.
- **Anchor Device Verification (Coming Soon):** Users with trusted "anchor" devices will be able to unblock new devices based on usage patterns, providing seamless access while reducing disruptions.



Proactively Protect Your Brand and Accountholders

Protecting your brand and your users from look-alike phishing sites is easier with our integrations with Allure Security and PhishLabs. These tools help defend your reputation by identifying and shutting down fraudulent sites that mimic your digital assets to trick users into sharing their personal information.

NOTE: For details on setting up these integrations, including the necessary contract and onboarding steps, check out the Knowledge Base article here.

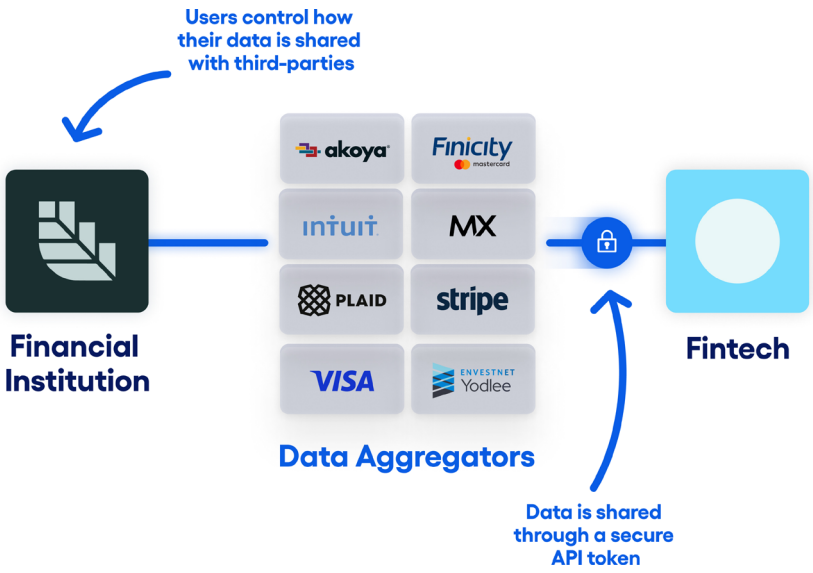
In addition, Jack Henry has joined forces with Nudetect by Mastercard to help you leverage user data analytics to define normal, legitimate behavior associated with account entry at your financial institution. Because when your system knows exactly what legitimate behavior looks like, it can identify and block anomalies in a second.

sharing *only* the right information

Behavior follows desire. And users want account connection between their financial apps. That's why screen scraping has become so common from services like Plaid. The practice of screen scraping by third-party fintechs solved a desire held by accountholders: a way to consolidate specific financial information from all of their accounts for easier money management. But the practice of screen scraping means handing over your login credentials to a third-party and allowing them to log in on a user's behalf, with no user control over which information is shared. Sound preposterous? It is. And Jack Henry solves this in a better way.

Forget Screen Scraping

The CFPB is proposing new regulation around screen scraping, and many in the industry are hoping for more time to be able to meet new requirements. Jack Henry has known screen scraping to be a security threat for a long time, so we didn't wait for regulation to do the right thing – we got started solving the problem.



Jack Henry has done the hard work to build partnerships on your behalf with all of the major data exchange platforms – Akoya, Finicity, Intuit, MX, Plaid, Stripe, and Yodlee – and we're completely replacing in-bound screen-scraping with direct API connection to easily and securely share *only relevant* data from user accounts to share with third-party fintechs of the user's choice – none of which is stored on a third-party server.

rest secure

Learn more about digital security in an engaging and interactive session hosted by our Head of Engineering, Chad Killingsworth, as he discusses all things security-related for our Digital Banking Platform. Save your spot!

Let's talk about this together. digitalexperience@jackhenry.com

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