Banno Business™

security overview

security is our number one priority

When we developed Banno for retail banking, we pulled out all the stops to ensure your users' data is safe and secure. Now we're doing the same for Banno Business because we know that the stakes are even higher when it comes to commercial banking.

protecting the front door is key

Above all else, protecting the initial login is critical. If a fraudster is able to make their way into an account, all you can do is try to mitigate damage. That's why we've placed the majority of our focus on safeguarding account entry.

Every login attempt requires two-factor authentication (2FA): the user's initial credentials and a second factor.

Two-Factor Authentication (2FA)

2FA has become a standard part of many login processes, protecting users from the danger of brute-force password-guessing attacks. 2FA, by definition, requires two of the following from the user: something they know, something they have, or something they are (facial recognition or fingerprint, for example).

Initial Credentials

Like any traditional login process, we require a username and password. The password is still your user's primary authentication secret, designed to keep both a remote attacker and an insider with access to a registered device from gaining access.

A Second Factor

2FA can be achieved with several second factor options. Here is what Banno Business is accepting today:

1. **One-time passcodes**

   One-time passcodes can be delivered by:

   - SMS messages
   - Voice calls
   - Authenticator apps
   - Broadcom/Symantec tokens

2. **Security keys (FIDO)** ★ Recommended

   A FIDO security key is a small physical key that is plugged into a device to serve as a second factor of authentication. FIDO security keys are the recommended second factor method because they are the most secure – it's the only method that cannot be compromised. In order for a user to move forward with login, they must have the security key in-hand, making it impossible to accidentally share credentials remotely.

Passkeys: The Simplest 2FA Option

As an alternative to initial credentials plus a second factor, users can take advantage of passkeys – an all-in-one solution that achieves 2FA in a single step because the device being used serves as something the user *has*, and the biometric identification serves as something they *are*.

Registered Devices

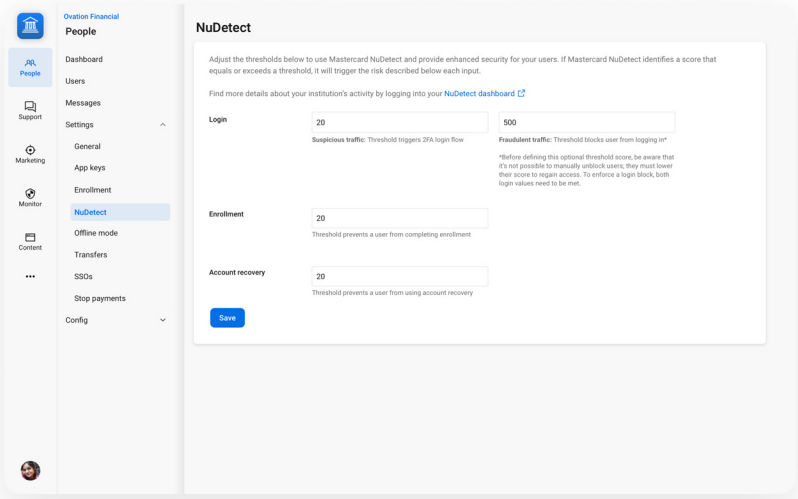
We know that it can be a pain for your accountholders to go through this whole process every time they need to check their bank account. In an effort to make it more convenient – without sacrificing security – we've provided the option for users to register their trusted devices. Once authenticated, users can opt to add the device to their trusted list and log in with only their password in the future – skipping 2FA.

This may seem risky, but it's completely safe. The Banno API ensures that every call is from an active and registered device, and users are able to deauthorize any lost or stolen devices to log out.

NuDetect by Mastercard

On top of all these login protections, we've also partnered with Mastercard to provide yet another layer of insurance: NuDetect.

Once enabled, NuDetect scores every login based on multiple factors, including user history, device characteristics, geographical location, and automated user behavior. Whenever a login event is noted as anomalous, extra precautions will be taken – whether that's ignoring trusted device status and requiring multi-factor authentication, or blocking the login completely.



protecting high-risk actions

In the event that an intruder manages to take over an account, we have further layers of security in place to prevent catastrophic events.

All sensitive operations require the user to re-authenticate using their password to proceed. These high-risk actions include:

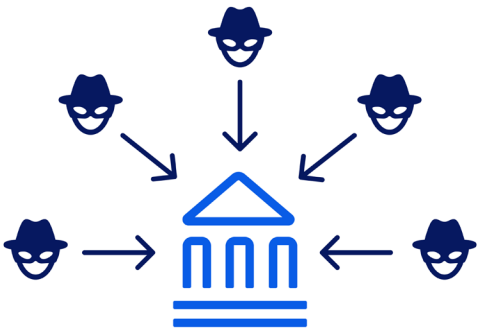
- Changing security settings
- Moving money outside of your financial institution (initiating ACH batches or wires)
- Inviting new users to your account (Coming soon)

attacks from every angle

You might be wondering, *"what are we working so hard to defend against?"*. Great question! We're working to prevent brute force, man-in-the-middle, and phishing attacks.

Brute Force

Credential stuffing, DDOS, and randomized credential attacks work by mass guessing usernames and passwords with hundreds of thousands of IP addresses. Luckily, the combination of inbound gateway protections offered by Jack Henry's cloud providers and Banno's built-in credential stuffing protections mitigate most of these attacks.



Man-in-the-Middle (MitM)

In a MitM attack a malicious third-party intercepts traffic between the victim and Banno, allowing them to see everything – including passwords and 2FA codes. While the scenario of an unsecure WiFi network exposing a user's sensitive information is often talked about, it is no longer a viable attack pattern thanks to encrypted certificate restrictions in browsers and apps.

Phishing

Phishing attacks use social engineering to trick users into trusting the attacker, convincing them to share credentials over a phone call, SMS, email, or fake website. These are the most common attacks today, resulting in the greatest losses.

differences from legacy systems

We've made some intentional changes to our security practices in Banno Business which differ slightly from our legacy platforms, like NetTeller®. Let's take a look at what's changed:

Configurable Risk Points

The Banno platform takes a secure-by-default approach, providing preset applicable risk points where users are always challenged to authenticate.

Wire PIN (Banks only)

These were originally designed for use by those calling into the wire room, and were moved into NetTeller before modern authentication methods existed. These have been replaced in Banno Business by high-risk action authentication.

RSA (Applicable to customers moving from NetTeller to Banno)

This outdated security system can now be replaced with either password or token challenges, protecting the NetTeller functions that are still utilized while allowing RSA to be removed.

frequently asked questions

FIDO Security Keys

What costs are associated with using FIDO keys?

Unlike our partnership with Symantec, which has a per-user cost, there are no additional fees from Jack Henry to enable the use of security keys. We believe that the best security options should be as accessible as possible. Since these are physical devices though, you will need to either purchase and distribute keys to your accountholders, or instruct them to purchase keys on their own. There are many different vendors who offer security keys, at varying prices and with different features. There is a possibility that Jack Henry will offer a vendor partnership at some point in the future, but that is not available at this time.

Which users need FIDO keys?

Our recommendation is that FIDO keys are the ideal security solution for all users, and in particular should be the only 2FA option available for business users.

Can you require certain users to authenticate with FIDO keys depending on their permissions and status in Banno Business?

At some point we plan to offer default categorization of users who need higher levels of security (those with access to ACH and Wire entitlements, etc.) but that is not available at this time. The only way to set this up would be to manually configure each user.

Do Banno Business users need a separate FIDO key for each organization they manage?

No, a single security key can be set up for use with multiple login credentials, and even for other websites and applications outside of your financial institution.

Can FIDO keys be used to re-authenticate users who have lost access to their account?

Yes, FIDO keys can be used to re-authenticate users in Banno Online™.

What happens if a user loses their FIDO key?

Just like if your user lost a phone or Symantec token, they would need to get in contact with you to remove the physical device registration from their account, and then register their new device the next time they log in.

Does the FIDO key have to remain plugged in for the entirety of the user's session?

No, the key only needs to be used during the initial login process of a new device. Once the user has been authenticated they can register the device to be trusted in the future.

When will FIDO security keys be an option for retail banking users?

This feature is now available in both Banno Online and Banno Mobile™.

General

Can a token be used to authenticate for high risk actions instead of a password?

Not at this time, but passkeys are available in Banno Online.

Will it be possible to disable Authy as an authentication option?

Yes, this feature is available.

Can the option allowing a user to bypass a 2FA challenge for trusted devices be disabled?

Not at this time. 2FA is designed to protect against remote attackers, which would not have access to the trusted device.

Will there be any disruption to third-party fintechs using the dashboard card framework?

If the third-party is using our API connection, or a proper OAuth 2.0 connection like Plaid, there will be no disruption. Any providers utilizing screen scraping will be disrupted, as this form of communication is completely blocked by FIDO keys.

Do passkeys work across devices?

Yes. Within either the Android ecosystem or Apple ecosystem passkeys can be transferred between devices, allowing users to authenticate one device with another (For example, a user could authenticate via their phone to login to their desktop banking).

In NetTeller every time a new cash management user is created, or an existing user gets new permissions, the user is placed in a hold status until the bank removes the hold. Does this same functionality exist in Banno Business?

Yes, this same hold feature is supported in Banno Business.

Are password managers an effective solution for reverse proxy + phishing attacks?

No. While password managers do provide a small amount of protection in this scenario – when your user lands on the incorrect URL, their credentials will not autofill like they do on your website – there is still the possibility of your user manually copying and pasting their information into the website, compromising it.

Is keylogging an issue to be concerned about?

Keylogging, the process of a criminal using a tool to record what a person types on their device, can potentially be an issue for password-based authentication. But when a second authentication factor is used, particularly a FIDO key or passkey, those attacks are made ineffective.

security made simple

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

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