Digital Banking Platform

High-Risk Action Blocking

In today's fast-paced digital landscape, providing seamless banking experiences while ensuring absolute security is the top priority for every financial institution. As accountholders and businesses rely on digital platforms to manage sensitive transactions, the threat of sophisticated cybercrime continues to grow. You want to offer the convenience your users expect, but not at the expense of their financial safety and your reputation.

navigating the problem landscape

Across financial institutions, account takeover (ATO) fraud poses a significant threat to financial stability, brand reputation, and customer trust. Its true cost extends far beyond technology – driving compromised customer accounts, direct financial losses, and a steep erosion in consumer confidence.

Internally, ATO places heavy strain on IT, security, and call center teams, increasing operational costs and slowing response times. The scale of the problem is substantial: in 2024 alone, ATO fraud cost U.S. adults an estimated **$15.6 billion**, underscoring the urgent need for stronger, real-time prevention.[1]

unpacking the solution

To address this gap, Jack Henry introduced High-Risk Action Blocking, which prevents new devices from performing risky actions. We call these actions "high-risk actions." Because fraudsters target high-risk actions first, this safeguard ensures they're stopped before they even get a chance. Banno™ has created a built-in list of actions that could compromise the security of your users' accounts, and for those actions we require an extra level of authentication.

Banno's Strategic Approach

This initiative was driven by Banno's broader security strategy to help financial institutions proactively reduce fraud at the point of risk. In early 2024, our team identified high-risk actions – such as sensitive transactions initiated from newly added devices – as a critical vulnerability and set out to close that gap with device-based trust controls.

> **"Our commitment to security is focused on helping community financial institutions shift from reactive defense to proactive prevention. High-risk action blocking was born from a need to bridge the gap between user convenience and absolute security."**
>
> **Julie Morlan**
> Assistant Vice President of Core and Digital Product Management, Jack Henry

To validate the impact of high-risk action blocking, Jack Henry collaborated with four financial institutions representing a mix of community banks and credit unions with varying customer bases and risk profiles. These financial institutions piloted high-risk action blocking by focusing on actions most frequently targeted by fraud – while maintaining day-to-day usability for legitimate users.

Their participation provided early signals on real-world fraud reduction, operational impact, and customer experience – helping shape this feature and its enhancements ahead of broader availability. The institutions who participated include:

- Armstrong Bank – approximately $2.5B in assets across 29 locations
- Incredible Bank – approximately $2B in assets across 16 locations
- Think Bank – approximately $2.1B in assets across 8 locations

Launched in fall of 2024 through a phased rollout, the solution first established reliable enforcement of high-risk action blocking and then evolved to optimize the accountholder experience. Later enhancements, including streamlined verification, gave financial institutions flexible configuration options to apply strong protections while minimizing friction for trusted users.

Reflecting on the impact of these measures, Phil Suckow of Incredible Bank shared,

> **"What we found is that, with what the Banno team continues to expose from a security aspect, we've actually driven fraud in-branch. Now we're seeing fraudsters being more brazen [in their attempts], because we've figured out how to identify them and block them [in the digital channel] with Banno's help."**
>
> **Phil Suckow**
> Vice President of Innovation, Incredible Bank

Where Community Financial Institutions Stand Today

As of early 2026, approximately 400 unique financial institutions, representing more than a third of those on the Banno Digital Platform™, have adopted high-risk action blocking by selecting the configuration that best aligns with their risk posture to safeguard accountholders.

- **Full Blocking Mode:** Over 100 institutions have opted for the highest level of control, restricting all high-risk actions on new devices until the new device has been verified by the institution.
- **Waitlist Mode:** Nearly 200 institutions have opted for a more balanced approach, temporarily blocking high-risk actions on new devices for up to 30 days to mitigate fraud while minimizing user impact.
- **Anchor Device Mode:** A growing list of just over 100 institutions are leveraging established anchor devices, allowing accountholders to seamlessly unblock themselves.

the impact on minimizing the problem

The true measure of a security solution is its impact on fraud reduction. For our customers, high-risk action blocking has translated directly into significant, quantifiable reductions in ATO and related losses.

Jonathan Sexton of Armstrong Bank reported immediate success, noting,

> **"I think we were one of the first few to turn it on toward the end of last year [2024], and we've had $0.00 – knock on wood – in Zelle® losses since then."**
>
> **Jonathan Sexton**
> Executive Vice President Director of Innovation, Armstrong Bank

The results prove that proactive, controlled friction is a highly effective deterrent.

Don't Just Take Our Word for It

This level of protection is consistent across various risk profiles. Brett Demers of Think Bank highlighted that by adopting these device-based controls, they have been able to significantly mitigate losses.

> **"By implementing Banno's new high-risk action blocking, Think Bank has seen impressive outcomes that keep risk management smart and customer experience front and center. Through this enablement we've been able to reduce specific product loss by nearly 87%, while reinforcing our ability to serve customers with greater confience and care.**
>
> **Brett Demers**
> Digital Solutions Manager, Think Bank

While some bad actors attempted to "hang low" during the initial waitlist period, Think Bank found that moving to a full blocking mode effectively closed the window of opportunity.

healthy friction

We understand the concern about friction. And yes, enabling high-risk action blocking does add an extra step for accountholders wanting to perform what we consider a "risky" action. However, the reality is that *frictionless doesn't mean effortless – it means expected.*

Redefining "Frictionless"

A truly "frictionless" digital experience isn't one with zero steps – it's one that aligns with a user's mental model and expectations. In high-risk moments, such as initiating a large transfer or adding an external account, users actually expect and assume the platform will apply stronger safeguards.

This strategic friction doesn't feel like an obstacle; it feels like protection, building the confidence and peace of mind necessary for a modern digital banking experience.

Empowering End Users to Self-Serve

Strategic friction is balanced by intuitive self-service avenues that allow accountholders to unblock themselves without friction-heavy manual intervention.

Adam Letson of Bank Independent shared,

> **"Bank Independent launched high-risk action blocking with anchor device verification in late 2025. We were impressed to find that implementation was as simple and easy as the Banno team had told us it would be, and we've already seen fraud prevented with minimal impact to our customer-facing teams."**
>
> **Adam Letson**
> Product and Payments Officer, Bank Independent

By giving accountholders the power to unblock themselves, financial institutions transform necessary security friction into a relationship-building moment of empowerment and control.

Call-In Verification via High-Risk Action

Support staff can initiate a secure, self-service verification flow directly from an accountholder's profile in Banno People. This sends a high-risk challenge to the accountholder's devices, allowing them to instantly verify themselves and clear any blocks. The process works in tandem with high-risk action blocking, giving your team real-time visibility and reinforcing the critical security rule: accountholders should **never** share a one-time passcode over the phone.

Anchor Device Verification

Anchor device verification adds a powerful layer of protection by designating a user's primary, trusted device as the gatekeeper for sensitive actions. When high-risk activity is initiated – such as updating credentials – the anchor device confirms the legitimacy of the accountholder, removing the block so the new device can complete the request.

This creates a seamless yet highly secure flow that stops fraud at the source while giving users confidence that they're in control of their own digital identity.

This transition to self-service has a direct impact on the back office. Phil Suckow notes that after implementing anchor device unblocking,

> **"Accountholders stopped calling us to unblock their devices. They just natively started doing it."**
>
> **Phil Suckow**
> Vice President of Innovation, Incredible Bank

The result is a highly efficient, self-service model that increases accountholder confidence and decreases friction, allowing your support teams to focus on higher-value interaction.

turn on high-risk action blocking today

Navigate to the *Security* settings in Banno People to get started.

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

sources

1. Pitt, Jennifer. *2025 Identity Fraud Study: Breaking Barriers to Innovation*, Javelin Strategy & Research, March 25, 2025.