Digital Banking

NuDetect by Mastercard

Banno sees exorbitant numbers of login attempts. For every 15 valid logins, we block 1,800 invalid account entry attempts.

Fraudsters are getting more sophisticated, so upping intelligent security at account entry points is in the best interest of your accountholders *and* your financial institution.

Reinforced Vulnerable Spots

NuDetect adds protection to the major account entry opportunities in the digital space – login, enrollment, account recovery, and high risk prompts.

Definable Risk

NuDetect tracks and scores user behaviors for events associated with account entry. Scores are added up, and the total is held against a threshold score which defines an event as risky.

Appropriate Stops

Login events that are scored as *suspicious* require two-factor authentication to retrigger. Login, enrollment, account recovery, and high risk prompts that score as *fraudulent* are flat-out blocked.

NuDetect by Mastercard

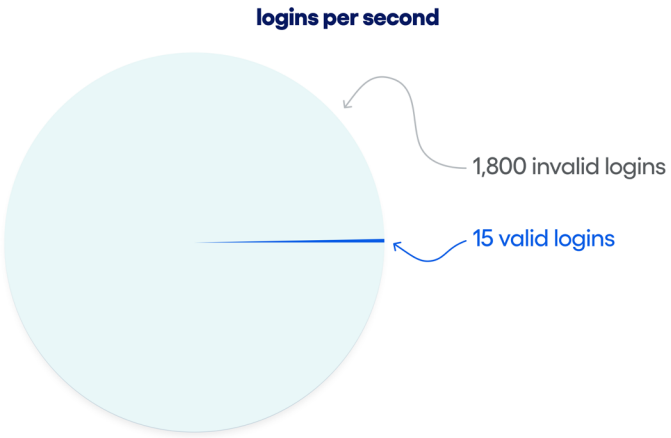
outsmarting bots and fraudsters

Account compromise is an inherent digital banking risk that Jack Henry has been mitigating for years because faster access to money means faster fraud.

Leveraging data in the right way helps you avoid fraud, sparing your financial institution a PR nightmare and maintaining your accountholders full faith that their deposits are safe with you.

It's Happening Right Under Your Nose

This threat isn't just "out there," happening to "other people." The Banno platform sees 15 logins per second. That's a lot. But the number is miniscule compared to the 1,800 invalid logins we see per second.



Fraudsters Are Getting Sophisticated

As fraud protection protocols, services, and solutions become more robust, scammers' tactics get more sophisticated.

Bad actors are using data from past breaches to perform brute force attacks, establishing phishing schemes like they're marketing strategies, and even exploiting human error or lapses in judgment to trick their victims (or those close to them) into sharing account information.

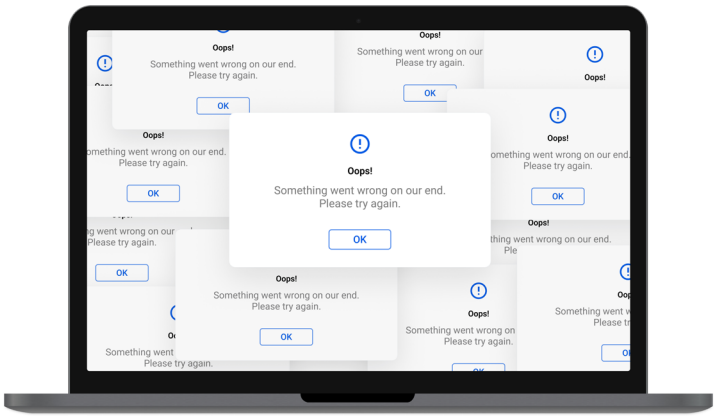
how to prevent invalid logins

It's been said that the best way to know a counterfeit bill is to know and recognize all the attributes of legitimate currency. What if we could use the same logic to identify fraudulent account activity? We can.

The major digital banking events that are attractive to fraudsters for account entry points are: account logins, account enrollment, account recovery, and high risk prompts.

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 you know exactly what legitimate behavior looks like, you can identify and block anomalies in a second.

For example, you may define it as reasonable for an accountholder to login to one, even two accounts several times a day. But if it's detected that an "individual" tries to access 1,000 accounts in just three seconds, that would cause NuDetect to halt account entry. Here's the logic: if a single device from a single IP is accessing this number of accounts in such a short amount of time, it's a bot.



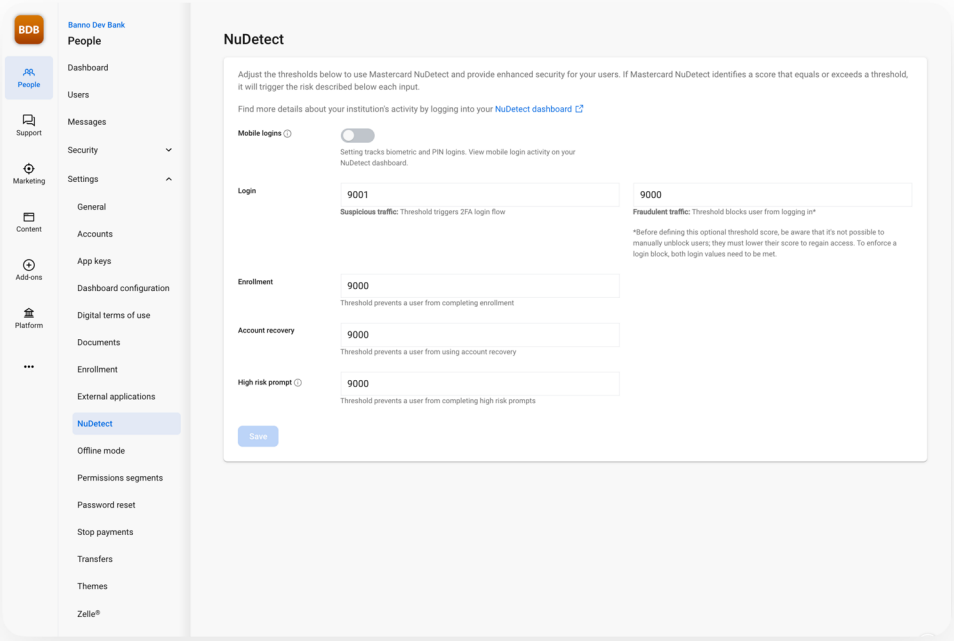
How It Works

NuDetect uses a pass/fail system to evaluate account entry events. It tracks multiple user behaviors and assigns a numeric score to each one. Those scores are totaled and compared against a threshold set by your financial institution.

The scoring is based on the user's (or bot's) behavior and device usage over time – and it's 99.99% accurate. In addition to Banno-specific behavior, NuDetect leverages consortium data from across the network to help identify known fraudsters. If an event is linked to a device or behavioral pattern with a history of fraudulent activity, it can be flagged and blocked even quicker – giving you broader protection beyond just your own user base.

Tactically, here's what's involved:

- Your financial institution sets threshold scores for events like account logins, account enrollment and account recovery in the back office settings of Banno People™. Rest easy – we have resources to help you decide what your threshold should be to match up with the needs of your financial institution.
- When an event fails, or exceeds the threshold score, NuDetect will block account access for that user.



what happens in Banno when an event gets a failing score?

In simplest terms, appropriate stops are set in motion.

Login

NuDetect asks you to set thresholds for two categories of risky login attempts: a lower threshold score for suspicious traffic, and a higher threshold score for fraudulent traffic.

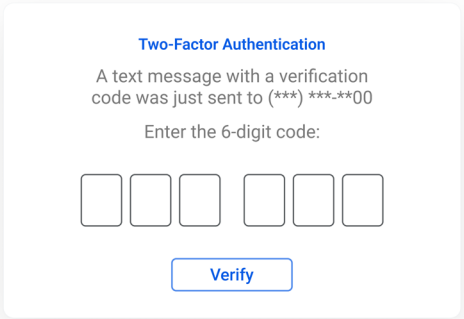
These thresholds apply to both desktop and mobile logins. Most login traffic comes from iOS and Android devices – including those using biometric or PIN-based authentication – which now appears in your dashboard, giving you greater visibility into mobile user behavior and helping you spot suspicious patterns more effectively.

Biometric and PIN-based logins are not blocked based on risk scores; instead, these events are passively evaluated to assess user behavior, ensuring a seamless experience for legitimate users while still detecting anomalous activity.

Here's what happens in each case:

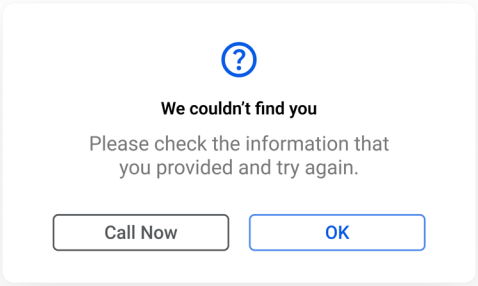
Suspicious traffic

In the event of a suspicious login, the accountholder is prompted to complete two-factor authentication.



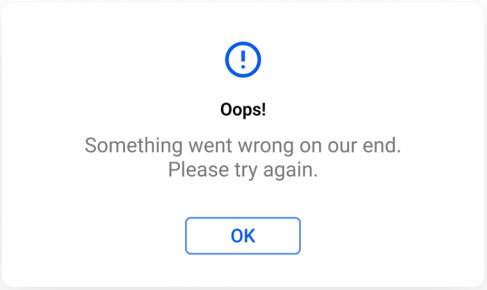
Fraudulent traffic

In the event of a fraudulent login attempt, the accountholder is denied access to digital banking. The only way for the user to gain access again is to work directly with the financial institution to restore their digital banking privileges.



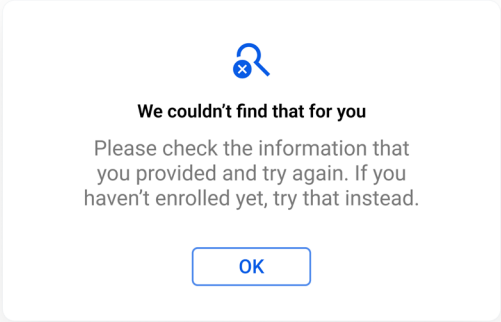
Enrollment

Enrollment events that return a score equal to or above the threshold score prevents the accountholder from processing to enroll.



Account Recovery

Account recovery events that return a score equal to or above the threshold score prevents the accountholder from recovering an account.



High Risk Prompts

High risk prompt events that return a score equal to or above the threshold score prevents the user from completing the high risk action. This is the only post-login area where NuDetect is integrated – so even if someone logs in with PIN or biometric authentication, a high risk score here can still trigger blocking, adding another layer of protection where it counts.

one more layer of defense in your aresenal

Jack Henry is committed to staying on top of security and fraud prevention for community and regional financial institutions. Banno is already equipped with the latest standards in web security, such as two-factor authentication and eliminating screen scraping. With NuDetect, you have even more control over security for your accountholders.

bad guys blocked

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

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