NuData Security
mastercard

CASE STUDY

How a bank delivered a better user experience to 91% of its users with behavioral biometrics

2.5x

more recognized users at login

0.01%

false positive rate

13m

total events analyzed

The short version

The problem

A bank's authentication solution was adding too much friction at login.

The solution

The bank implemented NuData's behavioral biometrics technology to validate good users without additional friction.

The results

- Nearly 2.5x more recognized users at login compared to traditional device and network-layer tools.
- 91% of users recognized after 15-day training period.
- 0.01% false positive rate.
- 13 million total events analyzed.

The full story

The client

Large U.S. bank.

The problem

A well-established bank's authentication solution was adding too much friction to its customers' login experience. With assets close to $200 billion, the institution came to NuData looking for a way to provide customers with a seamless, secure login.

The NuData delivery

The bank implemented NuData's behavioral biometrics solution to validate users at login. We looked at data from a sub-population of the bank's traffic that was processed through our behavioral biometrics solution to evaluate the results. This case study dives into the results with the bank's customers for more than six weeks, including the model's 15-day training period (the time it takes for a behavioral model to learn each new user's inherent habits).

The scope of this case study

- Total sub-population analyzed: 13 million
- Training period: 15 days
- Full performance period, including training: 45 days

Our technology builds user profiles based on hundreds of inherent behaviors like a user's typing cadence or how they hold their phone.

Why behavioral biometrics?

Extra authentication measures are sometimes necessary to keep users' accounts safe. But let's face it: When security protections become too irritating, users find ways around them. And considering how much of our lives we live online, user expectations for digital experiences are higher now. Companies need to provide a secure and user-friendly way to log in that also keeps users' personal information safe.

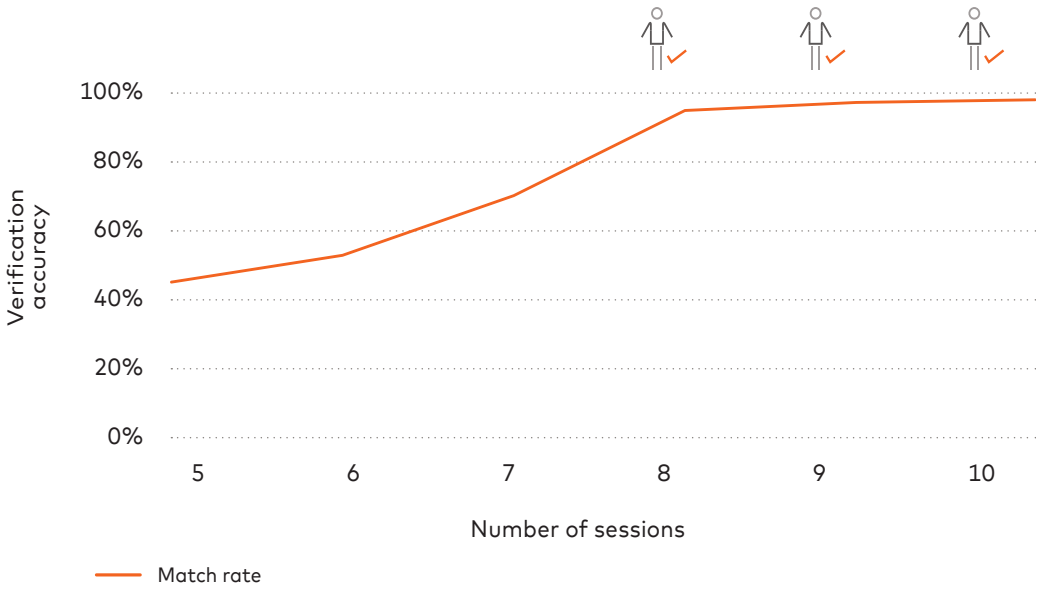
This is what inspired NuData's behavioral biometrics technology — a way to remove friction by reducing the need for further authentication. Our technology builds user profiles based on hundreds of inherent behaviors like a user's typing cadence or how they hold their phone. Those profiles are then used to identify and validate users without the need for additional authentication measures. The entire process is passive, so it doesn't add friction to the user experience.

01 | How the bank implemented NuData's behavioral biometrics

The NuData algorithm can build an online profile for a user in approximately 30 days or sometimes even faster.

The learning phase

The NuData algorithm can build an online profile for a user in approximately 30 days or sometimes even faster, depending on how often a customer accesses the online platform. It's like getting to know someone — you have to meet a few times before you learn personal details like their favorite meal or biggest pet peeve. The NuData model increases its accuracy once it has "met" a user seven to ten times. Our learning phase is significantly faster than other behavioral and passive biometrics models, which typically require at least 90 days to get to know the user and provide value.

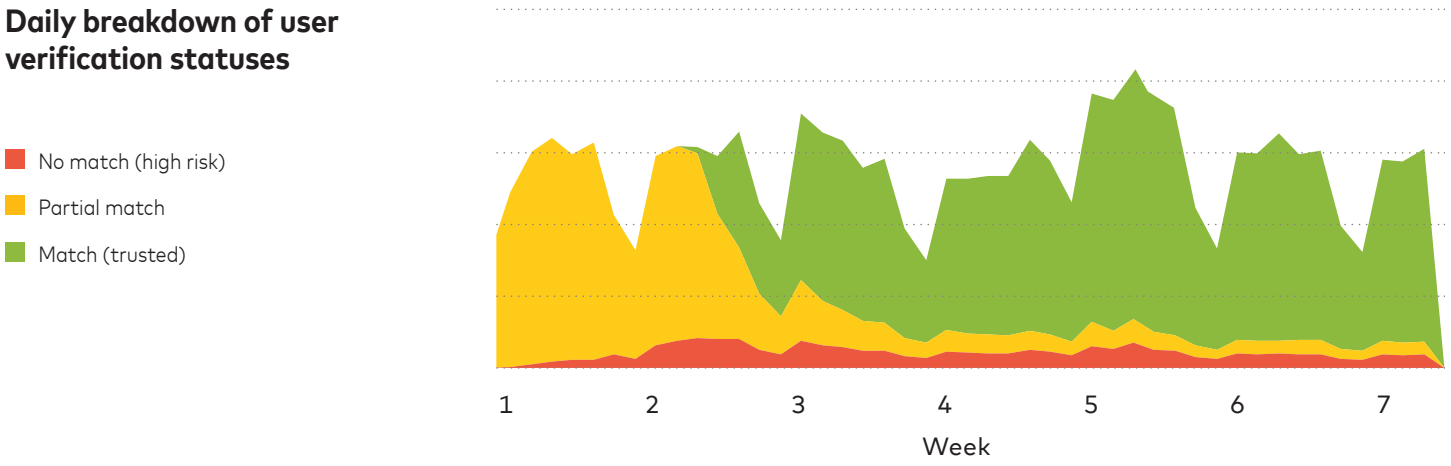


Turning it on

The first time you meet someone, you don't know anything about them. Similarly, 100% of the users NuData's solution "meets" are strangers at first. But this doesn't mean every user gets falsely declined on their first login attempt. NuData relies on other security layers like device intelligence and tested profiles of good and bad users from its Trust Consortium to decide whether an individual poses a threat. For example, a user whose login takes 0.01 seconds is probably not a legitimate user.

The chart below shows recognition results over the course of the first few days of our engagement with the bank. As expected, the technology was still acquainting itself with users. But by the 14th-day mark, the model better understood users' behavior. This created a match between the expected parameters and the parameters or signals the user actually showed. Let's keep in mind that users with a partial match were also evaluated with NuData's additional layers of technology to avoid impacting good users.

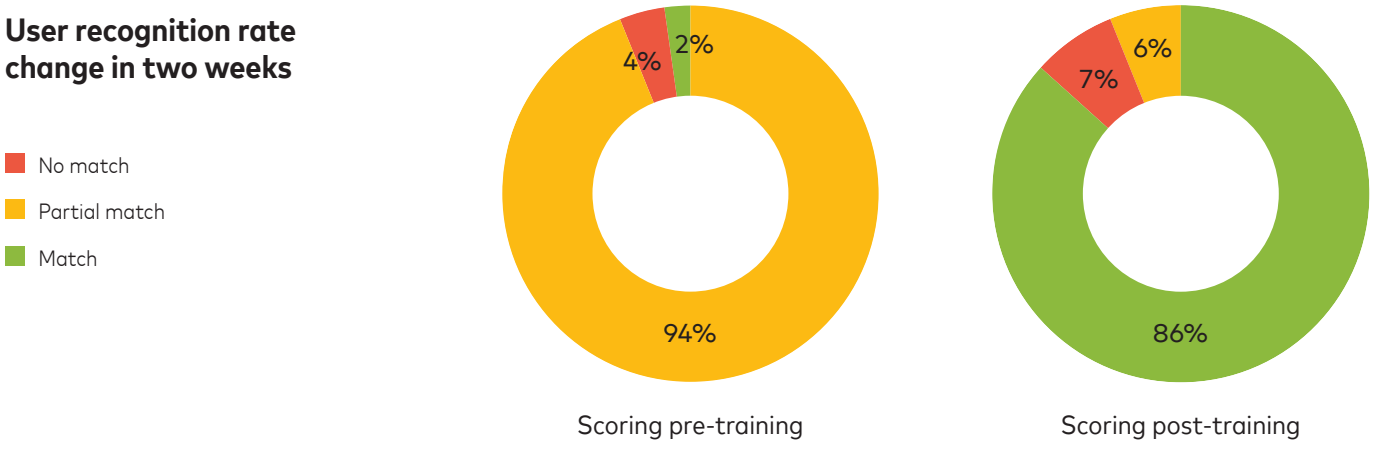
Daily breakdown of user verification statuses



The results

After the two-week training period, the solution recognized the vast majority of users with high accuracy. At this point, the bank could already streamline login for most of its trusted users without added friction. The chart below shows the stark change in user recognition from the solution's deployment to the time the model has learned its users' behaviors two weeks later.

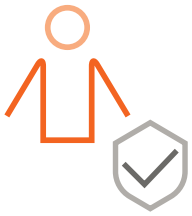
User recognition rate change in two weeks



02 | How does the model actually recognize users? Behind-the-scenes

96%

of profile match users have familiar input behavior



95%

of partial match users logged in using familiar devices

Our intelligence platform evaluates hundreds of rules and signals in real time to match the user behavior to existing profiles and determine the users' risk levels. By looking at a user's inherent behavior, the behavioral biometrics-specific signals passively build a risk score, without impacting the user experience.

In this case, we grouped users into three populations based on their risk level: profile match, partial match, and no match. This is an exclusive look under the hood of our model to identify the main signals or patterns that the majority of users within each group had in common.

Group 1: Profile match (trusted)

Users in this group shared matches on the highest number of the trustworthy parameters. Conversely, they showed the fewest matches — if any — to risky parameters.

Common trustworthy parameters in this population include:

- **Familiar input behavior: Seen in 96% of Profile match users**
  What is this? This parameter looks at how a user inputs their data at login. For example, do they use autofill or type out their password? If they type out their password, do they use a physical or digital keyboard? Familiar input behavior means a user inputs data in an expected way based on their user profile and other factors, like the device they're using.
- **Familiar typing pattern: Seen in 91% of Profile match users**
  What is this? By looking at a user's typing speed, pauses, and changes in rhythm, it's possible to identify typing patterns unique to each individual. A familiar typing pattern means the cadence of a user's typing, whether mobile or desktop, matches their past behavior and other elements of an expected profile.
- **Frequent device: Seen in 80% of Profile match users.**
  What is this? This parameter looks at whether the device used in the session is the same one used in the previous session, even if the device attributes (like device fingerprint) and ID have changed.

Group 2: Partial match

In this group, users matched both trustworthy and risky parameters. Depending on the criteria matched, account sharing is a potential reason behind a partial match. From here, it's up to the organization to decide whether they'll trigger an additional verification step, block, or let the user proceed. Each company can base their decision on their risk tolerance and business goals. But once they decide, NuData can automate this decision as a part of the real-time process. These are the trustworthy and risky parameters that most of the users in the partial match group displayed.

Risky traffic is 4x more likely to provide wrong credentials than a recognized user.

Trustworthy parameters:

- **Familiar state or province: Seen on 95% of Partial match users**
  What is this? This parameter looks at whether the user logged in from a location where they've logged in before.
- **Familiar device: Seen in 95% percent of Partial match users**
  What is this? The user logged in on a device they've logged in with before.

Risky parameters:

- **Unfamiliar input: Seen in 94% of Partial match users**
  What is this? This refers to a user providing information in an unfamiliar way. For example, when a website expects a user to type in their credentials, but the user instead copies and pastes, that can be a sign that they're a bad actor inputting stolen credentials from a list – or another member of the household sharing an account.
- **Unfamiliar touches: Seen in 91% of Partial match users**
  What is this? This means a user's typing cadence doesn't match expectations based on their past behavior, device or other aspects of their profile.

98%

of no match users logged in from an unfamiliar state or region

Group 3: No match (risk)

Users in this group are considered high risk — and they should not be allowed into the environment. From this population we also found that risky traffic is 4x more likely to provide wrong credentials than a recognized user. The behavioral biometrics parameters that assign them to this group include the following.

Risky parameters:

- **Unfamiliar state or region: Seen in 98% of No match users**
  What is this? The user is logging in from a new, unexpected location.
- **Unfamiliar device: Seen in 89% of No match users**
  What is this? The user is logging in from an unrecognized device that hasn't been used for login before.
- **Anomalous input pattern: Seen in 87% of No match users**
  What is this? This refers to a user providing credentials in a way that is not compatible with a regular human. This means it's a script providing the information, but the script is programmed to make systems think it's a human to bypass them. For example, a script could be programmed to use the keyboard to fake pauses between keystrokes.
- **No user interaction: Seen in 42% of No match users**
  What is this? Bad actors often deploy automated scripts at login to efficiently scale their attacks. Forty-two percent of no match users show telltale signs of bot behavior, revealing there's no human involved in the interaction — and they are using basic scripting tools. However, users that do look human can be suspicious, too. The other 58% of no match users had human or human-like interaction. This shows that attackers are, more often than not, evolving their tactics to bypass bot-protection tools.

91%

of users were seamlessly recognized by the bank

0.01%

of good users were incorrectly scored as Partial match or No match

- **Normal (human) user input: Seen in 13% of No match users**
  What is this? This happens when an attack leverages humans directly (like human farms or CAPTCHA solving apps) to bypass non-behavioral security tools. Interestingly enough, this human input is also expected for an average trusted user. However, given the other parameters that users also matched in the No match group, it's clear that it's a fraudster manually attempting to log in, impersonating the legitimate user.

The outcome

After monitoring 13 million events after the 15-day training period, the bank seamlessly recognized 91% of users. And false positives were rare — only 0.01% of good users were incorrectly scored as Partial match or No match and faced with an additional step up to access their account. The solution seamlessly recognized nearly 2.5x more users at login compared to traditional device and network-layer tools.

03 | Conclusion: How to offer exceptional UX for your trusted customers

The number of global online banking users is forecasted to reach 2.5 billion by 2024.[1] But as banks are digitally transforming, bad actors are waiting just around the corner. And with the amount of personal data stored in financial institution databases, there's no room for inaccurate authentication measures.

With NuData's behavioral biometrics, businesses reduce uncertainty, false declines, and false negatives. Companies can even prevent attacks created to bypass security rules, which is an increasingly common tactic for bad actors. As a result, we have seen in this case study how companies confidently reduce login friction for their trusted users without compromising security.

Additionally, based on our results, behavioral biometrics coupled with NuData's other security layers helps mitigate risk with 99% accuracy.

[1] *https://www.statista.com/statistics/1228757/online-banking-users-worldwide*

Email us to book a consultation with one of our fraud prevention and security experts at hellonudata@mastercard.com

NuData Security
mastercard

About NuData Security

Behavioral biometrics and device intelligence solutions are trusted by some of the world's largest brands across eCommerce, digital banking, and beyond. NuData helps companies stop account takeover, prevent new account fraud, and reduce unnecessary friction in real time.

With more than 20 billion risk assessments and 4.5 billion devices processed yearly, businesses across the globe benefit from the power of NuData's Trust Consortium to validate good users without disruption and stop bad actors before they can cause damage.

Click here to read about the successes of other companies with NuData.