neuroID

3 Must Do's for Onboarding: A Roadmap For Secure Growth

Digital Behavior improves digital identity knowledge and onboarding.

Digital-savvy prospects have sky-high expectations when it comes to online customer experiences. Seamless account opening is a critical competitive differentiator and key to conversion of genuine customers; however, as online enterprises smooth onboarding experience, fraudsters—either alone or as part of a fraud ring[1]—also find it easier to infiltrate.

How can organizations with online account setup provide genuine applicants with a killer experience while keeping criminals and bots at bay?[2] Coming into 2023, the stakes are higher. Identity fraud spikes when the economy declines:

- Personal identity fraud rose 12% in 2009 to hit peak levels on the heels of the 2008 global economic crisis,[3]
- As unemployment and interest rates rise, buying power dwindles—and both casual fraudsters and large-scale fraud rings are itching to supplement their incomes.

The inability to balance onboarding and fraud has already caused chaos across the digital world.

- It's why many major hotels, car rental companies, and other large merchants have stopped accepting digital credit cards.[4]
- It's how 4.5 million fraudulent customer accounts[5] were created at PayPal—causing a 25% stock slump.
- It's why the investing app Robinhood created a list of digital banks from which it *bans* transfers: literally turns away money.

This was all *before* worries about a looming recession, which will inevitably bring higher fraud risks with it.

Another downturn is on the horizon. Now is the time for digital enterprises to ensure they can secure growth through seamless account opening experiences **that don't simultaneously increase risk for fraud**.

1. https://www.neuro-id.com/whitepapers/the-anatomy-of-a-fraud-ring-report-white-paper
2. https://grcoutlook.com/the-digital-identity-crisis-why-we-need-to-solve-it/
3. https://www.prnewswire.com/news-releases/javelin-study-finds-identity-fraud-reached-new-high-in-2009-but-consumers-are-fighting-back-83987287.html
4. https://www.forbes.com/sites/elizahaverstock/2021/12/03/fintechs-fraud-problem-why-some-merchants-are-shunning-digital-bank-cards/?sh=4418923275bd
5. https://www.forbes.com/sites/jeffkauflin/2022/02/02/paypal-admits-45-million-accounts-were-illegitimate-as-fintechs-fraud-problem-grows/?sh=6629fe3336b9

3 Milestones on the Road to Securing Growth Today

At the height of the pandemic, headline after headline[6] told stories of online fraud perpetrated by fraudster opportunists taking advantage of the unprecedented push to digitization. While we can't predict the future, we can prepare for it. Here are three major milestones to focus on for fortifying your account opening strategy against the predicted influx of new and more sophisticated fraudsters.

Milestone 1: Assess the applicant. Not just their data.

Behavior is unique. No two voices are alike, and digital behavior is also uniquely distinct. Fraud prevention needs to balance protection while also letting through legitimate transactions. Consider the following:

- False positives, or when genuine customers are locked out of onboarding, can often cost more than fraud itself.
- Avoiding false positives is even more important when you realize that some of your most potentially lucrative long-term customers are those hit hardest by false positives.
- Younger generations who don't have a long credit history—but have a long lifetime of potential customer loyalty ahead of them—often are pinged as risks by traditional fraud stacks due to that thin-file credit.

The best identity fraud defense requires a holistic approach that layers tand optimizes friction[7] as a tool to both predict fraudulent intent and optimize downstream expenses in a way that simultaneously flags fraud, reduces false positives, and invisibly assesses identity, making for a seamless applicant experience.

> "Now is the time for digital enterprises to ensure they can secure growth through seamless account opening experiences that don't simultaneously increase risk for fraud."

6. https://www.washingtonpost.com/us-policy/2022/05/15/unemployment-pandemic-fraud-identity-theft/
7. https://www.neuro-id.com/resources/blog/take-the-path-of-smart-resistance

Milestone 2: Look for security gaps in your digital onboarding journey.

Fraudsters and fraud rings are patient and persistent. We've seen them even take the time to learn about their targets' step-up policies and identity verification procedures before an attack, so they can discover how targets react and build an entire strategy for each level of fraud stack prevention.

You need to have the same vigilance in evaluating and fortifying your fraud stack as they have when testing the parameters.

- Synthetic identity fraud—which accounts for about 80% of today's fraud attempts—thrives on stolen PII and as such is one of the hardest types of fraud to detect and prevent.
- **These attacks are part of why PII is not the gold standard it used to be, for any industry,[8] even though for many it remains the singular foundation of fraud prevention.**
- Fraud attacks go way beyond what they used to be—fraud prevention needs to go beyond PII as well, while constantly taking the user experience into account.
- Detecting a fraud influx requires analyzing the onboarding experience and then orchestrating that account opening journey.

A close evaluation and assessment of how your funnel (device intelligence, identity resolution, and behavioral analytics, etc.) is layered will arm you with the right insights to secure both your online conversions and your digital onboarding. By allowing invisible, pre-submit identity assessment tools, like behavior, to sit at the very front of the journey, digital leaders minimize the amount of unnecessary identity verification steps undertaken by genuine customers. Such steps are both annoying and costly.

> "The best identity fraud defense requires a holistic approach that layers and optimizes friction[7] as a tool to both predict fraudulent intent and optimize downstream expenses in a way that simultaneously flags fraud, reduces false positives, and invisibly assesses identity, making for a seamless applicant experience."

8. https://www.neuro-id.com/resources/blog/poisoned-pii-what-to-do

Milestone 3: Create a Friction-Right Framework.

It costs the average bank up to $130 to verify a new identity.[9] Behavioral analytics secure growth by providing insight early and invisibility, so that decisions of who to fast-track and who to escalate within an existing crowd stack are natural, frictionless and accurate. Behavioral analytics measure how familiar each applicant is with their inputting PII at onboarding, and then analyze users' behaviors as they interact with a digital form or application, looking for scientifically proven tell-tale signs of unfamiliarity with what should be known PII. By interpreting these behavioral signals instantly at onboarding, users are tagged with a friction-right account opening approach:

- **Low Friction:** If they're familiar with the data they've input, the likelihood is that they are who they claim to be. Friction can be optimized to move them through the process faster, for fewer false positives and less UX-based conversion loss.
- **High Friction:** If an applicant shows patterns of unfamiliarity with the data they've input, they're flagged for potential fraud. Onboarding journeys can be optimized to include additional security checks for these threats, so they weed themselves out instead of being allowed to spread seeds of fraud throughout a business ecosystem.

How to Use Digital Behavior as a Conversion Tool

Behavior is likely already available for analysis on your existing application process, but it requires time, resources, and internal expertise to implement as a fraud detection tool.

Off-the-shelf behavioral analytics use AI-driven analysis to aggregate, sort and review a broad range of cross-channel, historical and current customer behaviors to develop clear, real-time portraits of potential risks.

- Stolen PII doesn't impact the results, because behavioral analytics look at abnormal aspects of the bad actors' form-filling behavior.
- Credit scores and other false positive drivers are irrelevant, because behavioral analytics rely on pre-submit data—which is built on the digital body language of taps, keystrokes, swipes, backspaces, pastes, tabs, clicks, etc. as users complete online forms—to reveal authenticity (or inauthenticity), malicious intent, fraudulent behavior (whether from a singular actor, a bot, or a fraud ring), and more with startling accuracy.

This gives behavioral analytics astonishing predictive power that doesn't discriminate, while securing both your bottom line and your fraud prevention.

9. https://www.profgalloway.com/id/

NeuroID is the digital behavior company driving the human identity movement. Its pre-submit behavior signals inform risk, conversion, and account opening journeys for some of the largest and most respected financial institutions and organizations in the world, including TransUnion, Intuit, Square, Affirm and many others. These signals can be viewed both at an aggregate level for a bird's eye view of applicant behavior or at an individual level, delivering a pre-submit, top-of-funnel behavioral flag maximize existing identity tools and invisibly improves applicant onboarding experiences.

neuroID