The 2025 Buyer's Guide to Behavioral Analytics for Fraud Prevention

How to Find the Right Solution to Fit Your Unique Needs

neuroID

A part of experian.

How to Use this Guide

While behavioral analytics has been around for decades, its best use cases within a fraud stack are not always well understood. We created this buyer's guide to provide insights on the different approaches to behavioral analytics for fraud prevention so you can find the best solution for your specific needs.

This guide will provide you with a decision-making framework for evaluating if you need behavioral analytics at all, and if so:

- How to identify the specific problem within your fraud stack that behavioral analytics will help solve
- The key differentiators between behavioral analytics and other fraud tools
- Best practice considerations for finding the right behavioral approach for your needs
- What to expect from a trial and implementation process in impact, benefits and scope
- Questions to ask when choosing a behavioral analytics provider or deciding whether to build in-house
- How to evaluate the long-term impact of a behavioral analytics solution

NeuroID, a part of Experian, was built on behavioral analytics. Our experts have seen the evolution of fraud from basement-dwelling fraudsters to Generative AI (GenAI). We know what works for most, what works for some and what behavior isn't designed to solve — and we want to make sure you feel confident during every stage of your behavioral analytics evaluation. Beyond an analysis of behavioral tools, this guide will also walk through how your peers address the balance between fraud, friction and conversion, and how to ensure all the components of your fraud stack are working more efficiently.

This buyer's guide will empower you to make the most informed decisions to protect against today's evolving threats and tomorrow's unexpected challenges. Let's get started.

Table of Contents

Sophisticated Fraud is Rising

Automated Attacks
Up 1760%

New account opening fraud
Up 125%[1]

Identity Theft Rose to the **#1 Most Encountered Fraud Attack** in 2024[3]

Part 1: The Big Questions to Ask

You don't read a buyer's guide for fun. You're considering behavioral analytics for a distinct reason. In this section, we'll make some assumptions about the questions you're thinking about — based on our experience with engineering behavioral analytics for over a decade — and try to answer them.

Question 1. Why Behavioral Analytics? Why Now?

Fraudsters' rapid adoption of GenAI has been a catalyst for the explosion of automated fraud attacks, which have increased **1760% since 2022.**[1] Similarly, the **42% growth in real-time payment transaction volumes** has opened numerous new vectors of fraud and created an entirely new playing field for fraudster teams.[2] And "teams" is really the right way to think of today's cybercriminals — they are organized attackers and fraud rings with playbooks and their own KPIs to hit.

These teams have goals and gumption, and every digital business is a target. Since you're reading this guide, you've likely felt the impact of this surge in sophisticated attacks. It's an earthquake of fraud activity, pushing up from the deepest depths of the Dark Web and causing cracks across the solid foundation of every fraud and identity stack.

> **You're reading this guide, so you're looking for a solution to some of those cracks (or chasms) in your own fraud approach. How can you tell if behavioral analytics will be the right choice?**

Whether or not behavioral analytics is right for your stack depends on your fraud management strategy. The right behavioral structure can help reduce fraud losses, as well as drive expansion and enhance brand trust. The wrong one can add unnecessary noise, friction and frustrations.

Understanding when and where your stack could benefit from behavioral analytics is the first step. The following sections will help you determine the appropriate level of new behavioral investment for your business.

Question 2. What Kind of Behavior Do You Need?

At its core, behavioral analytics is the process of analyzing digital user interactions to understand and predict the likelihood of risk. But as vendors, regulators, and lawmakers have twisted behavioral solutions into new forms, it has become a cloudy term. We most commonly see it confused with biometrics, which is a wholly different approach that focuses on identity verification (while behavioral analytics focuses on risk detection).

Here is how to differentiate between behavioral-based fraud tools and biometrics-based fraud tools:

Physical Biometrics Tools:

signature recognition

fingerprint recognition

facial scan

Ties unchangeable traits (e.g., fingerprints, facial recognition, gait patterns) directly to an individual's identity. For regulators and legislation, biometrics is being carefully considered for consumer protection and privacy concerns. This technology confirms "who" someone is.

Behavioral Analytics:

typing speed

clicks

hover patterns

Uses interactional data (e.g., typing speed, mouse movements) to predict risk without tying the data back to a specific individual, thus avoiding many of the privacy issues associated with biometrics. As opposed to identifying "who" the person is, this measures "how" someone behaves.

In this guide, we're focused on behavioral analytics. Behavioral analytics measure a user's behavior and interactions, such as keystroke dynamics, mouse movements, typing speeds, touches, swipes, trackpad movements, window transitions, copy/paste of data, field and page transitions, and more, to detect if a user is risky or genuine. Behavioral analytics never collects personal identifying data (PII). It provides a behind-the-scenes, frictionless way to measure users' intention. Behavioral-based solutions don't see **what** data users enter but rather **how** they enter it.

Although sometimes used interchangeably, physical biometrics is a separate category when it doesn't include the use of behavioral data. Behavioral biometrics is a combination of both physical biometrics and behavioral analytics.

Of course, these details only matter when you're considering the problem you want to solve within your fraud stack and the priority. For example, do you prioritize low friction over low fraud? Do you have biometric regulations to consider? Do you want to identify users or only identify their risk and intent?

This table can help you decide what you need within the behavioral or behavior-with-biometrics universe.

Table 1. The Differences Between Physical Biometrics and Behavioral Analytics

Use Case	Physical Biometrics	Behavioral Analytics (the focus of this buyer's guide)
Risk Detection	Detects if the user's behavior is indicative of a potential fraudster	
Identity Verification	Verifies identity based on biological or physical traits, occasionally using liveness tests	Is not identity verification, only identifies user risk
User Authentication	Authenticates the user is who they say they are	Identifies whether the user attempting to create or access the account is risky or likely trustworthy, and—for existing accounts — whether the login criteria's risk level has changed from prior attempts
Integration Ease	Lengthy and complex	Fast and simple, typically a JSON integration
Privacy Implications	High. Biometric data is sensitive and personally identifiable. Its collection and storage are highly regulated	Low. Data is anonymized and never connected to an individual. Its collection is considered privacy friendly by regulators
Regulations	New laws have been enacted to control the collection, storage, and disclosure of biometric data	Limited applications and often exceptions are highlighted for fraud mitigation
End-User Impact	High. Biometrics is a friction-filled process where a user has to provide a face, retina, fingerprint, voice, etc.	Low. Collects no personal data and is invisible to the end-user, adding no new friction

Question 3. Would Behavior Help Your Fraud & Identity Strategy?

Balancing fraud numbers, friction and financial pressure is a complex problem for fraud teams — and in many cases, it has created a very complex fraud stack. Ideally, you've layered a variety of solutions for a comprehensive defense. Maybe you start with a device and network vendor, progress to an ID check — possibly a credit check — continue with a document upload and default to CAPTCHA followed by manual reviews for most users. Meanwhile, returning users experience more device and network checks, an OTP and maybe a KBA if something looks off.

In theory, it should all be a dynamic workflow. But in reality, as fraud evolves many organizations have taken a throw-the-kitchen-sink-at-it approach instead, hoping solutions are filling the right gaps rather than ensuring each tool is adding non-duplicative value. This has created fraud stacks full of redundancies, inefficiencies, slow responses and an overwhelming amount of data to parse..

Behavior can add a lot of value. But do you really want to add one more layer of complexity?

This is a critical question to answer. Behavioral analytics has a wide litany of uses, so it can be tempting to throw it on the pile and call it good. But we've found that the best way to ensure a strong return on your behavioral investment is to focus on solving a specific problem or improving on older technology. You want to ensure behavior is adding modernity and nuance and not redundant data noise. Don't just add behavior because it's new and topical, but instead focus on one or two challenges you're looking for it to solve.

Example of Existing Stack without Behavior

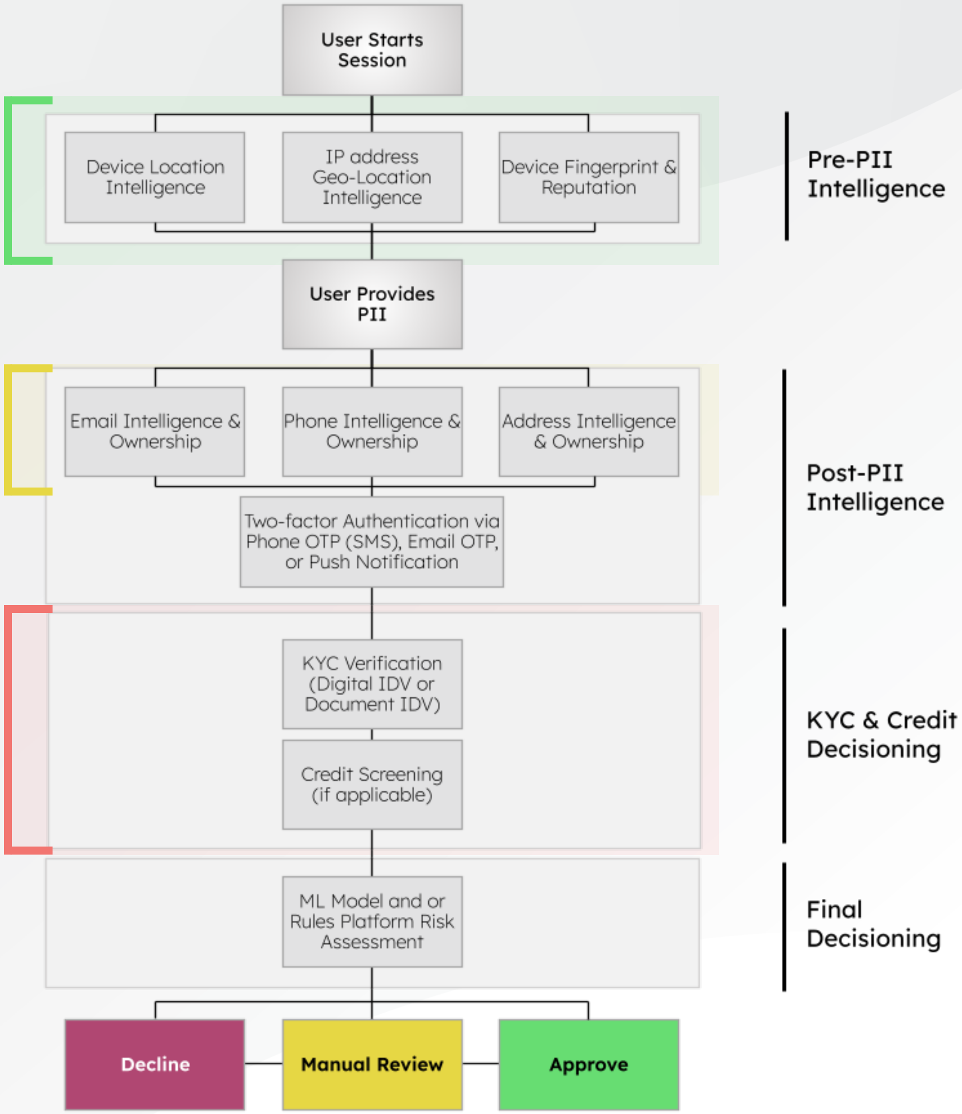

User Starts Session
Device Location Intelligence
IP address Geo-Location Intelligence
Device Fingerprint & Reputation
Pre-PII Intelligence
User Provides PII
Email Intelligence & Ownership
Phone Intelligence & Ownership
Address Intelligence & Ownership
Two-factor Authentication via Phone OTP (SMS), Email OTP, or Push Notification
Post-PII Intelligence
KYC Verification (Digital IDV or Document IDV)
Credit Screening (if applicable)
KYC & Credit Decisioning
ML Model and or Rules Platform Risk Assessment
Final Decisioning
Decline
Manual Review
Approve

Table 2. Common Challenges & Whether Behavior Can Help

Common Challenge	Typical Approach	Will Behavioral Analytics Help?	Voice of Your Peers[4]
Too much data noise that causes significant amounts of step-up verification to validate a user	Device or IP blocklists, document uploads, liveliness tests via biometrics, CAPTCHA, OTPs, KBAs	✓ Yes. Behavioral analytics detects specific behaviors clearly correlated with fraud. Many organizations are comfortable rejecting users based on a high fidelity behavioral risk flag alone. Behavior can give you a clear go or no-go answer before you make the next fraud or identity call. Unrelated to any other data in your stack, it provides an independent, actionable risk analysis. Adding behavior can solve this challenge by reducing your reliance on step-up methods, giving you a clearer view of risk and who to step-up or move along, deciding when to add friction at the right point in time.	"Before behavioral analytics, we were not automatically denying applications. They were getting an IDV check and going into a manual review. But with behavioral analytics at the top of our funnel, we implemented automatic denial . . . saving us additional API calls and reviews. And we're capturing roughly four times more fraud." - Fraud Strategy Manager, Elevate Digital Credit Solutions
Manual, low-automation level fraud and identity stack	Hard-to-meet reject and auto-decline rules; users all experience the same flow — no auto-declining and a lack of confidence in risk signals too hard to decision off of	✓ Yes. Behavior outputs can be heuristic signals and often leveraged for automated decisioning. The clear-cut, "yes this is high risk and looks like known fraudster's behavior" should be a data signal you trust enough to outright decline. The more you can trust your data signals, the less you'll need to pass to manual review teams.	
Attacks leveraging sophisticated fraudster techniques, such as GenAI fueled bots, and fraud results that miss synthetic IDs, ATOs, and PII-based attacks	Standalone device and network solutions, physical biometrics and/or synthetic identity fraud (SIF) risk models	✓ Yes. Behavior gives you the ability to see beyond the veil of even the most sophisticated fraud attacks. It is exceptionally strong in detecting third-party fraud, including attacks that use advanced bots, synthetic IDs, stolen IDs, promotion abuse, fraud rings, account takeover (ATO) and more. Behavioral analytics doesn't use PII, so can't be fooled by PII. Fraudsters prioritize easy wins and there is enough to hold their attention without trying to hack behavior, which is incredibly difficult to beat (even with GenAI).	"They're going to pass name, address, social, all of that stuff. And if they're more sophisticated, they're also gonna pass IP and device checks because they're going to spoof all of that. But spoofing behavior is on another level. I think that's where behavior really shines. Behavioral analytics is one of those key bulwarks in fraud defense." - Business Systems Analyst, Jovia Credit Union
Unseen fraud or attacks that are felt, but not detected	A small team of human reviewers drawing attention to an unexpected surge	✓ Yes. Behavioral analytics provides real-time fraud attack detection to help you see fraud and stop it in real-time. Real-time fraud attack tools are few and far between — you likely don't have a specific data vendor in your stack. Advanced bots and fraud rings are beating traditional fraud stacks, but real-time alerting from behavior-based signals are going to filter out these types of attacks from the very top of your funnel. Behavioral analytics provides a new level of insight. With options such as crowd views, you can see a fraud ring attack or surge in bot probes in near real-time. From there, that alert can help you figure out what to look for in potential dormant fraud or upcoming attacks. Unseen fraud can be made more visible across your fraud stack.	

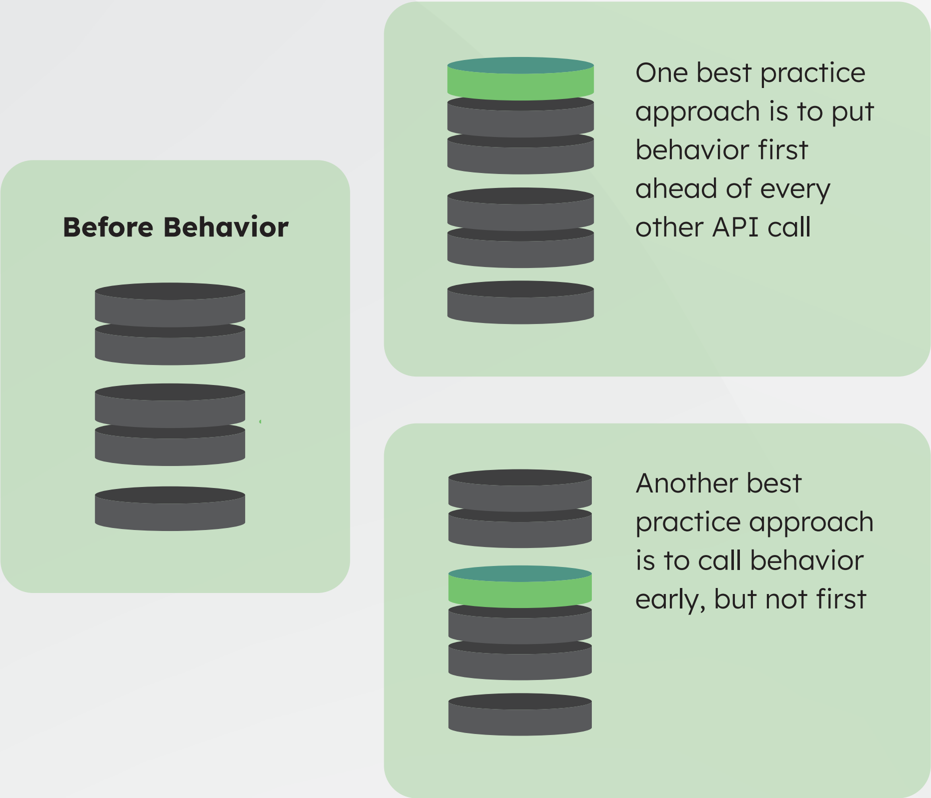
Common Challenge	Typical Approach	Will Behavioral Analytics Help?	Voice of Your Peers
Low efficiency with too many vendors	10+ vendors across different layers	✓ Yes. Behavioral analytics provides industry-specific best practices and can help refine other tools for better outcomes. Behavior is optimal when used alongside device and network signals. Together, these behind-the-scenes signals can detect risk early and build on each other for higher fidelity outcomes.	“Behavioral signals fill in the gaps in the onboarding process. At the end of the day, those gaps were small but were causing us exponentially more work and costing us in losses. We weren’t seeing those copy-pastes of data, or those rapid entries indicating bots. Now, we see it all.” - Fraud Strategy Manager, Aspiration Digital Bank
High-friction fraud detection at login, high false positives, or blunt rules that cause equal friction for all (for example, stepping up 100% of new devices)	Biometrics, CAPTCHA and OTPs are typical approaches along with other third-party authenticator tools	✓ Yes. Behavioral analytics provides the predictive ability to detect fraud risk before the user even hits submit, making it a powerful tool for uncovering fraudulent intent at login. This is a common use case for most behavioral analytics’ users and a helpful starting metric for ROI calculations. In contrast, physical biometrics can be changed if the fraudster has already taken over the users’ account. CAPTCHA is high-friction for good users and easy to cheat for fraudsters. OTP is also easy to cheat if the fraudster has taken over the user’s device. Documented behavioral patterns are highly accurate and incredibly difficult to spoof.	
High cost of onboarding/ fraud mitigation without a good view into each tools’ ROI	High-cost downstream tools, such as KYC and credit pulls	✓ Yes. Behavioral analytics’ unique ability to detect fraud at the top of your fraud funnel makes it easy to isolate fraud earlier, often before the user even hits submit at onboarding. This not only gives immediate clarity into behavior’s ROI, it adds insights into ROI throughout your fraud stack and can lower the overall cost of fraud mitigation through fewer downstream calls.	“There was an organized fraud ring that attacked our system last year, and although we caught them fairly quickly, they got through a lot of fraud checks. They got through many layers of verifications that we did at the time, so that’s when we enhanced our tools even further and began to work with behavioral analytics. Just analyzing the behavior throughout the application is so helpful because we’re able to cut out that fraud without additional hurdles on the customer side.” - Manager of Data Science, Elevate Digital Credit Solutions
Expansion and/or product launches that bring high-velocity fraud attacks	Manual review teams or real-time manual monitoring of application spikes	✓ Yes. Behavioral analytics can seamlessly handle increased volumes of transactions without performance degradation, in real-time. Market expansions, promotions and new product launches can put a huge target on your back, as fraudsters see a fresh opportunity. At the same time, you’re hoping to have a successful launch: which likely means lowering fraud barriers for more conversions. Behavioral analytics is seamlessly scalable, so even large attacks are stopped at the front door, with no impact to trustworthy applicants.	
Improved identity verification	Credit checks, first-party fraud risk models, KBAs, other standard PII verifications	✗ No, behavioral analytics cannot be used for identity verification. But, it can ensure the PII you’re evaluating isn’t stolen.	
First-party fraud prevention	Credit checks; first-party fraud risk models, KBAs, other standard PII verifications	✗ No, behavioral analytics cannot detect if a user who owns their data is trying to rip you off.	

Question 4. How Can You Bring Behavior Into Your Fraud Stack?

You've determined the problem and behavior looks like it might be the right solution. Now, there's the question of how your stack runs today and where it would make sense to add behavior. This depends on the kind of system you've built and where you can get the most visibility and value from a new signal.

Fraud Stack API Call Examples

Behavioral analytics can be collected and called anywhere user interaction occurs, although earlier calls typically bring the best visible ROI.



Before Behavior

One best practice approach is to put behavior first ahead of every other API call

Another best practice approach is to call behavior early, but not first

In our experience, here's what to look for and consider for the optimal ROI when getting ready to trial behavior. A poor start to trial can make it hard to dissect the outcomes and influence of behavior. You want to make sure it's integrated in a way that will show clear ROI (or lack thereof).

- **Don't build behavioral analytics in-house.** If your fraud and identity stack leverages custom-built models, you may be considering building behavior in-house. But behavioral analytics require more than a decade of outcome data and patented human computer interaction data in order to create trustworthy decisioning. Best practice is to find a vendor who has a high-success rate of working with behavioral data.

- **Whenever possible, ask for a top-of-funnel integration as the best way to evaluate the effectiveness of behavioral analytics.** This is easiest if you have waterfalling in your stack; but if you don't, there's no need to rework everything. You'll get the clearest view of behavior ROI at the top-of-funnel in trial, but it's not the only place to integrate — behavioral analytics can be collected and called anywhere user interaction occurs. Top-of-funnel will be more effective for proof-of-value, as it will help you save money immediately by reducing data calls that require user data.

- **Plan for the trial — but think ahead for the future.** Behavioral analytics signals can be very straightforward. After you have done your trial runs and have confidence in the data, you should integrate the behavioral attributes further into your model. Behavioral data is most powerful when combined with other data. This also will help reveal redundancies and cost-cutting opportunities.

- **If you bury behavior or put it after the majority of other data calls, it's much harder to evaluate the impact.** This is especially true if you have a custom built model (as in, all the data goes in at the same time and one solution comes out).

If you are using a third-party orchestration system for your fraud and identity stack, consider the following:

- **If behavior isn't offered, ask them to put it on the platform.** Then ask why they didn't already offer it — you might see this as a red flag to consider switching to a more modern orchestration platform. After all, when you have a third-party platform, the goal is for them to do the work for you and stay ahead of trends. Behavioral analytics is already accepted as a proven, valuable, and modern fraud tool: if it's not already offered, you're probably not on the best platform.

- **If your third-party platform does offer behavior**, then move into decision mode. If there's more than one behavior option available, test the pros and cons of both. There's a very good chance that different vendors will perform better at different places in your stack, so also don't be afraid to have more than one. After all, that's one of the top benefits of having a third-party platform: you should be able to easily make sequential or parallel calls.

For the best results, structure the trial so that behavior is called first — as a low friction, no PII data call based on live data, behavior is the best first data call. From there, use the results to decide which data vendor you call next.

Question 5. What is Your Output Flexibility?

How you use behavioral analytics will be unique to your stack and challenges. While behavioral analytics vendors may provide their solutions in a variety of outputs, only you can know what's best for your stack.

A modern behavioral analytics provider will offer you multiple levels of output delivered via a single real-time web services API:

- **Top-level signaling:** gives you an immediate, decisive answer to decline or approve.

- **Individual signal labels:** true and false output and numerical scores enable you to write your own combination of rules. If signal combination is a competency in your stack, this can be a more tailored approach for your traffic.

- **Attribute-level:** answers hyper-specific questions, which can be fed into models. For data science teams with model-building platforms that can perform feature engineering to identify the most relevant, predictive and powerful models for your unique needs. This is an excellent fit for large businesses ready to invest more deeply into behavior.

Based on the level of complexity you are prepared for, the following table provides key considerations to keep in mind.

Table 3. Output Flexibility & Signal Considerations

Signals	Considerations	How to Use it
Heuristic (Yes/No) Signals	• Easy to implement • Easy to incorporate into existing decisioning flows • Can serve as standalone rules • Likely built on the highest-fidelity outcomes the vendor has available • Easy to interpret • No model governance requirement • Great for smaller organizations or those with smaller fraud teams	• API or dashboard alerting available • Auto-decline fraudsters or fast-track good users
Signals and Standard Machine Learning (ML) Model	• May require model governance • May require minor tuning • More precise understanding of the users' behavior • Requires rules to be built based on their outcomes • Often requires some custom tuning • Takes longer to assess performance than heuristic signals • More variety and information in the larger swath of signals	• API • Dashboard drilldowns • Trigger and support manual reviews
Custom Behavioral Analytics Model	• Can solve unique problems or questions • Takes the longest to tune • Takes the longest to evaluate performance • Requires annual retuning	• API • Full waterfalling • Full fraud stack decisioning • Trigger and support manual reviews
Attributes	• Have a sophisticated model development and data science team that can support custom, sophisticated, model development • Combine internal data with behavior • Very specific internal problem-solving • Advanced experience with fraud model development and behavioral analytics required • Industries with data fields that are net-new to the vendor you're working with	Completely use case dependent, based on your modeling

Part 2: Getting the Most Out of Your Behavioral Trial

You've asked the big questions to evaluate your stack and how behavior could fit in. You know the high-level problems you can solve with new behavior-based insights. But what does that look like in reality, when you're drilling down into the actual ROI? And how can you get the most out of a trial, so you'll really know the impact of a behavioral investment?

How to Prepare for Trial: Behavior at Onboarding

Behavioral analytics at onboarding gives you insights to distinguish between genuine applicants and potentially fraudulent ones without disrupting your customer's account opening journey. By interpreting behavioral patterns at the very top of the onboarding funnel, behavior helps you proactively mitigate fraud, reduce false positives and streamline onboarding, ultimately creating a secure and frictionless experience for legitimate users (while knocking out fraud earlier).

With any trial of behavior, you'll get the best results if you go in ready to measure specific outcomes. To the right is an example of how to calculate the potential ROI of behavior when implemented at onboarding. These are all the factors behavior should be impacting, and evaluating each will show you if you're getting your money's worth from behavior.

Bring this data to your behavioral analytics vendor at the start of the trial, and at the end of the trial they will be able to tell you what the ROI is and the fraud your new signal(s) has captured.

Table 4: Numbers to Bring Your Behavioral Analytics Vendor

Onboarding Volume

- The number of new user registrations per year

Fraud Numbers

- Undetected fraud rate: fraud that is undetected with current controls (pre-recovery/collections)
- Average fraud loss: calculated as per fraud transaction
- Manual review: percent of applications undergoing any level of human touch point

Cost of Current Data Calls per Application

- Pre-PII fraud controls providers: for example device fingerprint, IP geo-location, device location, CAPTCHA
- Post-PII fraud controls providers: for example phone or email or address intelligence, fraud models, MFA
- IDV + AML screening providers: KYC process including digital + document verification, Sanctions/OFAC screening
- Credit check providers: credit score/FICO score, credit history pulls

Annualized Life Time Value Per New Approved Consumer

- Dollar value

Your behavioral solution trial should then be able to provide the following expected improvements:

- Fraud Detection Rate from Detected Fraud: % fraud the behavior vendor can detect that is currently detected by existing controls
- Fraud Detection Rate from Undetected Fraud: % of fraud the behavior vendor can detect that is not currently detected by existing controls
- False Positive Rate (% of Total Detected): number of false positives within the risky applicant population
- Genuine Rate (% of Total Population): number of users whose behavior is so low risk they can be recommend for reduced friction
- Optimization Discount Factor: Not all approved applications convert into revenue

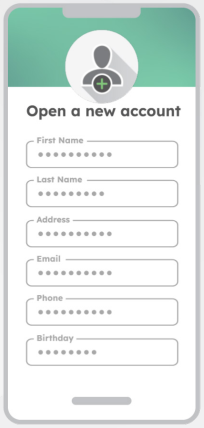


Table 5: Example of Trial ROI Numbers — Onboarding

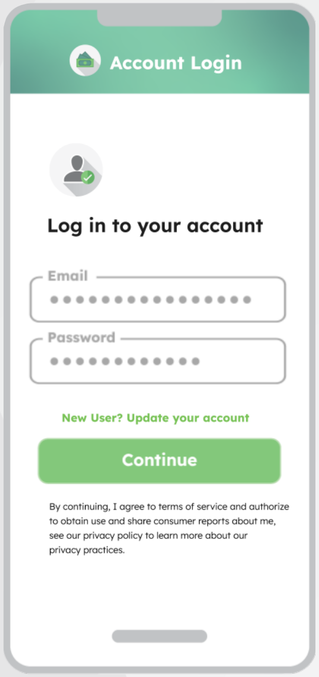
Metrics (Annual)	Examples
Annual Volume - Onboarding/Registration	1,000,000
Undetected Fraud Rate	0.50%
Average Fraud Loss	$500.00
Manual Review Rate	10%
Cost of Manual Review (on average)	$5.00
Cost of Pre-PII Fraud Controls Providers	$0.05
Cost of Post-PII Fraud Controls Providers	$0.75
Cost of IDV + AML Screening Providers	$1.00
Cost of Credit Check Providers	$1.50
Annualized LTV Per New Approved Consumer	$100.00

How to Prepare for Trial: Behavior from Login to Transaction

Perfect PII cannot mask the invisible markers left by users' data entry behavior, device and network.

Behavioral analytics detects these invisible trails at login and also at account management and transaction stages, or anywhere else that user interaction occurs.

With any trial of behavior, you'll get the best results if you go in ready to measure specific outcomes. To the right is an example of how to calculate the potential ROI of behavior, when implemented beyond account opening, at any point in the customer journey. These are all the factors behavior should be impacting, and evaluating each will show you if you're getting your money's worth from behavior.



By continuing, I agree to terms of service and authorize to obtain use and share consumer reports about me, see our privacy policy to learn more about our privacy practices.

Table 6: Numbers to Bring Your Behavioral Analytics Vendor

Login Volume

- The number of active users multiplied by the numbers of logins per year

Fraud

- Undetected fraud rate (fraud that is undetected with current controls (pre-recovery/collections))
- Average fraud loss per fraud transaction
- Percent of applications undergoing manual review (any items with a human touchpoint)

Cost of Current Data Calls per Login

- Dollars spent on the average manual review
- Dollars spent on existing login fraud control providers (on average): such as device fingerprint, IP geo-location, device location, CAPTCHA
- Dollars spent on existing two-factor authentication providers (on average), for one year

Annualized Lifetime Value from Repeat Customers

- Dollar value

Your behavioral solution trial should then be able to provide the following expected improvements:

- Fraud Detection Rate from Detected Fraud: % fraud the behavior vendor can detect that is currently detected by existing controls
- Fraud Detection Rate from Undetected Fraud: % of fraud the behavior vendor can detect that is not currently detected by existing controls
- False Positive Rate (% of Total Detected): number of false positives within the risky applicant population
- Genuine Rate (% of Total Population): number of users whose behavior is so low risk they can be recommend for reduced friction flows
- Optimization Discount Factor: Not all approved logins convert into revenue

Table 7: Example of Trial ROI Numbers - Login

Metrics (Annual)	Examples
Annual Volume - Logins	1,000,000
Undetected Fraud Rate (% of Total Logins)	0.50%
Average Fraud Loss	$100.00
Manual Review Rate	3%
Cost of Manual Review (on average)	$5.00
Existing Login Fraud Control Providers (on average)	$0.04
Existing 2-Factor Auth Providers (on average)	$0.10
Annualized LTV From Repeat Customers	$50.00

Part 3: Choosing a Behavioral Analytics Solution

Implementation and execution is likely one of the biggest looming shadows in your mind, knowing how resource-heavy, complex and high-visibility these projects can be.

At this point, you should have some good tools to figure out the key metrics to focus on, based on your unique needs. Now, it's time to find the vendor who can provide that key support, starting with implementation.

Importance of Strategic Planning

Any new technology onboarding needs a strategic approach. The good news is if you've been following along with this buyer's guide, you've already got a head start: you know the problems behavior can solve (and what it can't), how to set internal expectations on behavioral ROI, how best to prepare for trial and other key considerations unique to behavioral analytics.

For the most effective implementation, choose a vendor who provides:

□ **Unified javascript that provides information at account opening and login.** This reduces the technical investment and allows for ongoing advancement and changes to meet your needs.

□ **Unified API for any use case.** UX is fluid and interactions can blend between sign-up and login. Having a solution that assesses risk across all user interactions is crucial to ensuring the right risky sessions are getting flagged, while genuine users are left to enjoy a frictionless experience.

□ **Multiple platform integration options.** Your procurement team may have aggressive requirements for new software vendors, perhaps requiring them to be large, enterprise-sized organizations. This might limit your options — but don't let it limit your standards. You're looking for a vendor who has multiple platform integration delivery options, multiple platform integrations, and is able to integrate with your systems. Test whoever your procurement team allows you to test. Prioritize behavioral vendors who are available through multiple integration options, giving you more flexibility even if procurement limits who can buy from direct.

□ **Look for a behavior-first company.** Many models have bootstrapped behavior on top of their offerings, including device and network, IDV, etc. When that happens, it likely means behavior is an afterthought, not a core strength or investment. It's also a red flag that the behavioral signals are a very low-weighted part of their decisioning: meaning, you're actually paying for a solution that doesn't trust the behavior they provide.
A behavior-first vendor is one who weighs behavioral signals highly, because they've built enough trust in their core strength: behavior models.

□ **Look for a team who has true implementation engineers**, not just project managers. Implementation engineers' job is to make sure you're set up for success with a guided implementation and orchestration. Implementation engineers will truly understand the front end of your website and user experience goals to ensure your behavior solution will perform exactly how you need it to.

High-Level Questions to Ask

As you compare vendors, it’s important to ask the right questions — and get the right answers. Those questions will include immediate implementation questions, as well as establish a good understanding of how you’ll work together long-term. Here’s a list of best practices to focus on.

Table 8: Questions to Ask Your Vendor

What sets your behavioral analytics solution apart from competitors?

Look for industry experience and outcome-driven models. Ensure their model includes outcome data from your industry. Some behavioral providers specialize with one type of customer, such as a large bank. Their performance numbers may not be reflective for your population. Vendors with diverse customers and use cases are ideal.

How does your solution deliver real-time fraud detection?

Look for sub-second processing times and high transaction volume handling; ask for case studies.

How frequently are your signals and model refreshed?

Models should be outcome-based and refreshed at least once a year but ideally every 6 months. Look for a robust data science team that prioritizes exploration of their data. Behavioral data is cutting edge and their thought leadership should provide educational guidance about the latest trends they’re seeing in their data.

What types of data are integrated into your solution (e.g., device, network, behavioral)?

Look for a behavior-first provider who specializes in the nuance and modernity of behavior data above all other data types. Ideally, they also provide device and network signals, which work well when called at the same time (ideally top-of-funnel).

How does your solution provide insights into fraud detection events for non-technical stakeholders?

Cutting edge behavioral providers do more than flag individual users. They provide robust pattern analysis to help you visualize fraud attacks that would otherwise go unnoticed. Even better is if their client success team monitors influxes of risky users to help you detect fraud attacks while they're happening.

What level of customization and tuning do you offer for behavioral models and risk scoring?

An ideal provider offers a powerful off-the-shelf model, built on industry-relevant outcome data as well as a tuning for your specific business. They also would provide individual behavioral attributes to feed into your own custom model.

What is your integration process?

Some behavioral analytics solutions can be implemented in as little as four hours via simple JavaScript collector. This is especially true if you are purchasing behavior through an existing vendor relationship with an established API in place. Some providers will even work through the implementation live on a call with your team. This kind of low lift solution reduces pressure on your engineering team and resource requests.

Which regulatory and compliance requirements is your solution subject to?

Behavioral analytics — unlike behavioral biometrics — does not collect or store PII or other sensitive information. It does not create a behavioral profile to identify a specific person; although in some cases it stores data anonymously, matching it to the company's user ID through encryption. Behavioral analytics works exceptionally well alongside device and network intelligence, which collect information some consider PII. However, behavioral analytics does not collect or store any information subject to biometric regulations.

What is your solution's support SLA, and how responsive is your support team?

Not only should 24/7 support be expected, it ideally comes with a dedicated client success manager who proactively helps you fine tune and improve your use of the product, rather than just trying to upsell you. Look for vendors who prioritize easy communication channels.

What option is available to trial the product?

Because behavioral data must be collected in real-time, retro-analyses won't be available for new clients of a behavioral vendor. A live trial, requiring an implementation, will be required. This makes ease of implementation even more valuable. Many vendors will offer a 30- or 60-day no cost trial. Come prepared with your fraud stack waterfall diagram and volume and performance metrics to maximize the value of the trial.

What are the implementation, onboarding costs, and per decision costs?

One-time fees are standard for implementation and may be waived for large enough volumes or longer term commitments. They will likely correspond to the level of investment the vendor requires to onboard you. More complex profile and model solutions requiring tuning will likely have high implementation fees.

What support structure do you offer, and how will you collaborate with our team?

The vendor should provide a dedicated support team, including a client success manager and ongoing access to technical expertise for continuous strategy optimization.

What is your product’s accuracy?

Like all signals, accuracy and false positive rates have an exchange rate. An ideal provider should have heuristic signals with an accuracy and false positive balance. Based on your stack, they should provide multiple options with a recommendation. Some providers can detect up to 90% of fraud within 99% of accuracy with a <5% false positive rate.

What are your API response times?

Look for responses below 300 MPS.

What is your guaranteed up time?

99% is industry standard.

Continuing Your Behavioral Analytics Journey

The right behavioral analytics solution will meet your specific fraud prevention needs and beyond. Behavioral analytics can impact growth strategies, risk appetite conversion rates and much more.

We hope this guide has been helpful for clarifying your priorities and the ways a behavioral analytics solution could fill in gaps, streamline workflows and impact your business as a whole. Understanding all the details and coming to any behavioral analytics call armed with best practices strategies will help make the process smoother from the start.

Want more insights on behavioral analytics before you make the choice? Visit neuroid.com to read our resource center of white papers, trend reports, and more.

[1] 2024 Annual Report Cybersecurity Trends & Insights
[2] 3 Common Myths About Real-Time Money Movement & Fraud
[3] 2024 U.S. Identity and Fraud Report
[4] Quotes taken from NeuroID customer stories, 2024