# Ushering in a new era for behavioral analytics applied to fraud, fraud ring detection, customer experience, and synthetic identity fraud

RTInsights.com
Accelerate Your Business with Real-Time Insights

neuroID

## Introduction

Digital identity fraud is growing, and those committing it are changing. There is an increase in organized efforts by sophisticated fraud rings as the scale and scope of fraud opportunities has grown. These organized cybercriminals carry out highly coordinated attacks that use large amounts of compromised data. They often start with attacks specifically focused on identifying the fraud controls in place, then rely on overwhelming blitz-style approaches to break through vulnerable systems and steal en masse.

The Association of Certified Fraud Examiners estimates that total global fraud losses total nearly $5 trillion, and fraud rings are a large part of that.

Financial institutions have been the traditional target for fraud, and as the industry has evolved towards more of a digital strategy via neobanks and FinTechs, fraud ring approaches have also adapted. But financial institutions are not the only target. For many industries, the COVID pandemic contributed to an increase in fraud. More business was moved online. Bank offices were completely closed, as were physical retail stores. Additionally, employees worked remotely, call centers were dispersed into individuals' homes, and many processes were quickly implemented or changed to accommodate the shift. The combination of speed and stress behind those factors created weaknesses that could be exploited.

According to the latest data in *Occupational Fraud 2022: A Report to the Nations*, released by the Association of Certified Fraud Examiners (ACFE), half of all fraud cases it examined were affected by the pandemic in some way. For example, early on in the pandemic (May 2020), 68 percent of survey respondents had already experienced or observed an increase in fraud levels, with one-quarter saying that the observed increase had been significant.

And even as things return to more normal conditions, many systems that were rushed into place and processes that were rapidly implemented remain in use today. Those systems and processes are ripe for exploitation.

## Evolving attack methods require new thinking

Traditional approaches to fraud prevention that look for transaction anomalies or anomalies in Personal Identifiable Information (PII) are outdated. The bad actors are often a step ahead. They are more sophisticated. Many create accounts and try to commit fraud based on PII that is submitted through an online form, which itself is vulnerable to complex fraud schemes such as synthetic identity fraud. Sometimes referred to as post-submit data (data seen after the submit button is pushed), that PII can contain elements of real identities based on the vast amounts of valid data available to malicious actors via major data breaches, phishing scams, eavesdropping on data transmissions over public Wi-Fi services, etc. That makes it harder to sort out bad actors from real prospects.

Additionally, fraud rings are taking such techniques to new levels. Using a mix of stolen and synthetic identities, they can nurture a stolen or synthetic identity to build fake identities that are hard to distinguish from valid ones.

Making matters worse, fraud rings often work in advance, targeting companies to see what purchase instruments they accept and which they reject. Knowing that, they then set up purchases that are typically accepted.

They might look for a variety of vulnerabilities in a site, such as dollar thresholds for when fraud screening steps up. They might attempt basic hacking and analyze how a site responds. And they might examine how time and seasons impact change by looking for the times of the day, month, or year when an organization is more lenient. For example, a retailer might rush credit card applications for new customers during a holiday season.

Such fraud ring attacks are often coordinated among many participants, overwhelming businesses with a surge in, for example, credit card applications. Detection and mitigation of these attacks must be done in real time. And unfortunately, again, traditional methods to fight fraud fail against the virtual armies of cybercriminals who can easily buy your customers' PII on the Dark Web and pretend to be genuine applicants at scale. Simply put, businesses need a modern way to confirm that customers are who they say they are in real time.

## Overcoming the shortcomings of traditional approaches

Traditional fraud-fighting relies heavily on PII verification and matching, either using it alone or with other data to gauge the likelihood of an individual being a fraudster.

The problem is that almost all PII is widely available online. Fraud rings frequently create synthetic identities that do not correspond to any real person but contain enough tidbits of a real person's PII to get past traditional systems that match PII to identities.

The volume of data available from breaches is staggering. A LinkedIn breach in 2021 exposed the data of 700 million users. There have been multiple Facebook breaches over the last few years. Some collections of PII data have been essentially curated over the years from multiple breaches. For example, in 2019, the so-called Collection #1 database surfaced that contained 773 million unique email addresses. The data was a collection of credentials acquired in previous high-profile company data breaches over several years, including those of LinkedIn and Dropbox. Fraudsters can also turn to the Dark Web, which routinely sells compromised PII data.

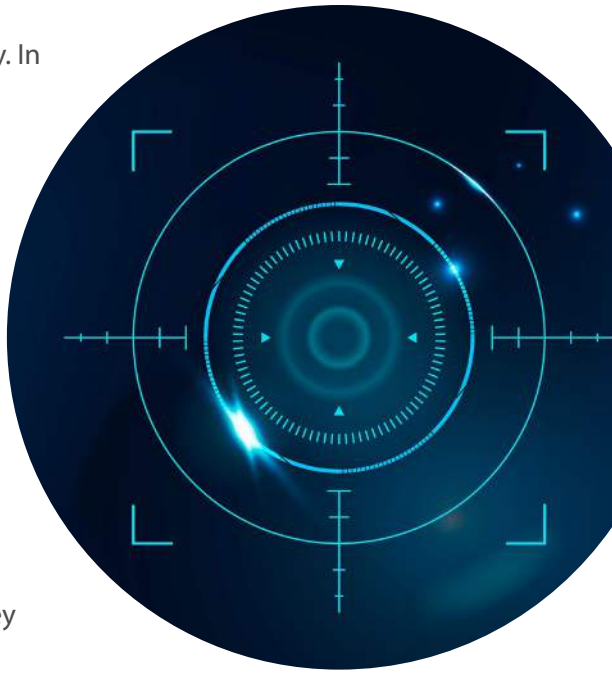
One of the most troubling aspects of synthetic ID fraud is that it can go undetected for a very long time. When a real person's identity is stolen, that person often notices that there are extra charges on a card, withdrawals on an account, accounts opened that were never requested, or other suspect activities. They then report it to the business. With synthetic ID fraud, because the identity is cobbled together from actual people without one sole victim, there is no real person to complain to.

That was the case in one frequently cited example of a fraud ring where a group established more than 7,000 synthetic identities, all of which were not detected by PII-based identity and fraud verification systems. The fraud ring ran up $200 million of losses for banks before it was caught.

Another dangerous aspect of fraud rings is that they are willing to take their time and build on any entrees they achieve that are recognized as legit. In contrast, a lone hacker might try to cash in immediately and run up charges across different accounts. A fraud ring often behaves like a normal customer, even building credit over time.

## Fighting back

So, what's the solution? How can businesses combat fraud rings and synthetic ID fraud?



Businesses must look beyond basic PII checks to know a person's identity. In particular, they cannot rely on an analysis of post-submitted data that is comprised of breached data.

Increasingly, digital businesses are using real-time behavioral analytics on pre-submitted data to enhance their fraud prevention strategies. Pre-submit behavioral data can spot applicants unfamiliar with the PII they're claiming as their own. For example, it might involve looking for things like a user misspelling their own name or not knowing their phone number.

If a fraudster were trying to open an account in person, there might be telltale behavioral signs that something is amiss, like nervousness or excessive sweating. Similarly, businesses need to examine the digital body language of those engaging online. That might include examining taps, keystrokes, swipes, backspaces, pastes, tabs, clicks, and more as they complete online forms. That could reveal inauthenticity (or authenticity), malicious intent, fraudulent behavior, bot activity, and more.

That makes detecting fraud rings before they get a chance to submit their application all the more important. As noted, fraud rings are working en masse, so the technology must be able to detect fraud in the crowd and by the individual user, all without collecting any PII.

Using behavioral analysis on pre-submitted data can not only help defend against fraud based on synthetic IDs and fraud rings, but it can also be used to benefit real customers. For instance, it might be used to help make a genuine customer's experience easier.

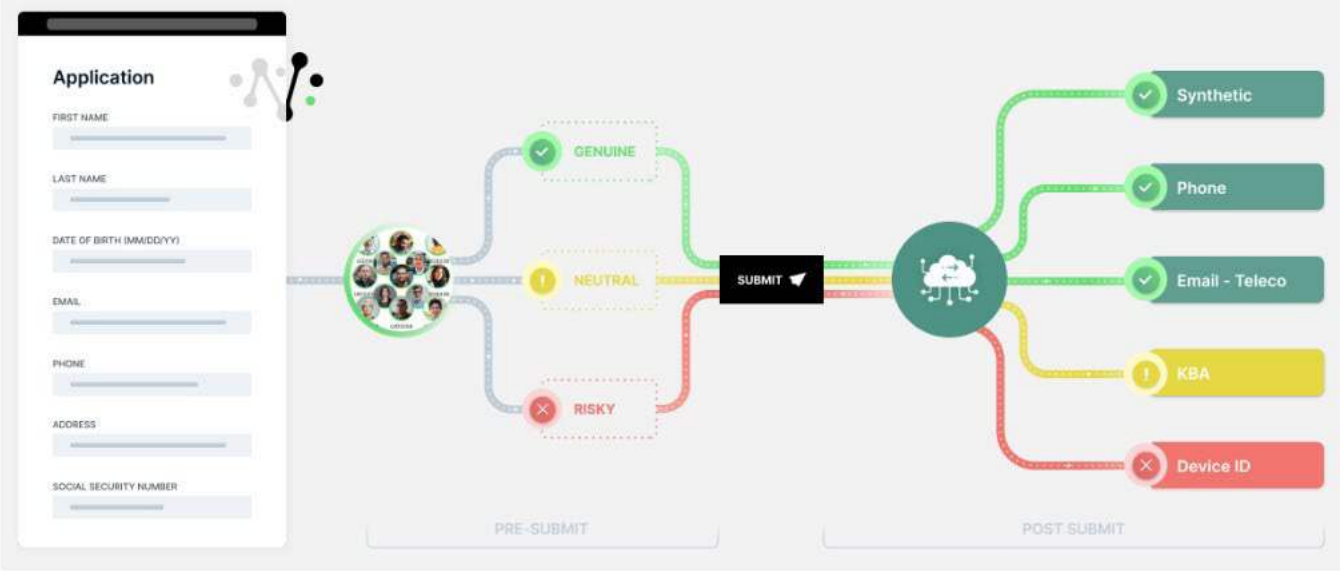
## Teaming with a technology partner

Digital businesses that could greatly benefit from such behavioral analytics technology often do not have the time, resources, or internal expertise to implement it. As a result, many are looking for a partner that brings technical expertise in human behavioral analytics and deep industry experience in fighting fraud.

NeuroID can help. It offers a dynamic set of tools to help detect fraud even before the submit button is pushed. Its solution sits behind existing online forms and complements existing fraud prevention processes by interpreting real-time digital body language.

To start, NeuroID monitors in-session online behavior. It tracks a customer's movements and behavior during the digital encounter, collecting data in real time as they fill out forms, submit applications, or respond to questions.

It then analyzes that data using proprietary neuro-cognitive technology and real-time prescriptive analytics for each interaction based on behavioral attributes that can be applied in real time to inform internal decision engines and risk models, making the current fraud stack even more efficient and effective.




The NeuroID technology is incorporated into different products for different use cases. ID Crowd Alert™ is designed for crowd-level monitoring, alerting, and visualizing fraud rings and bot attacks. Specifically, by monitoring the behavior of a crowd, ID Crowd Alert identifies fraud rings and bots. It lets a business visualize the behavior of a crowd. It allows a business to look at an entire applicant pool segmented by risky, neutral, and genuine behavior.

Another NeuroID product, ID OrchestratorTM, applies these technologies and methodologies to pre-submit behavior. It enhances an existing authentication or verification process with behavior-based digital intent insights, allowing a business to make better decisions on which customers to flag for additional verification screening and which ones they might be able to fast-track through the onboarding journey.

ID Orchestrator includes ID Crowd Alert fraud ring detection, session-level behavior analytics dashboards, digital intent signals delivered directly via NeuroID's API, and an every-session ID for every applicant.

## Fraud and other applications

NeuroID assesses several attributes of an online encounter. As users enter a variety of personal information such as first and last name, email, Social Security Number, annual income, street address, employer name, employer phone number, and credit card number, it collects and analyzes behavioral data. It then analyzes attributes of the session, including interaction time, hesitancy, typing fluency, time to the first answer, etc. The result is actionable insights that can be used in conjunction with existing processes to **detect fraud** and give advanced notice of fraudulent behavior.

Additionally, the insights provided by NeuroID solutions can help **improve conversion rates**. By understanding the patterns of a genuine customer, a company can identify serious customers, send fraudsters away, and focus attention on the real customers. Such an approach has helped NeuroID customers increase conversion by 200 percent and reduce historical fraud rates by 35 percent. That is a win-win for sure.

## Bottom line

Fraud rings and other identity fraud attacks are on the rise. Traditional methods of protecting against online fraud do not address the evolved tactics. Traditional screening processes and techniques do not detect fraud rings using ill-gotten PII.

What is needed is a new approach to fighting modern fraud. NeuroID makes use of real-time behavioral analytics on pre-submitted data to weed out fraudsters from real customers. That helps significantly reduce modern fraud, fraud rings, and bot attacks.

Simply put, NeuroID products bridge the gap between businesses and the hidden customer behaviors in real time so that businesses can make better identity decisions. As a result, NeuroID's intent detection products offer a new level of visibility into the intent of every customer or prospect.

RTInsights.com
*Accelerate Your Business with Real-Time Insights*

**About RTInsights**

**RTInsights** is an independent, expert-driven web resource for senior business and IT enterprise professionals in vertical industries. We help our readers understand how they can transform their businesses to higher-value outcomes and new business models with AI, real-time analytics, and IoT. We provide clarity and direction amid the often-confusing array of approaches and vendor solutions. We provide our partners with a unique combination of services and deep domain expertise to improve their product marketing, lead generation, and thought leadership activity.

neuroID

**About NeuroID**

NeuroID is solving the global digital identity crisis. The industry-redefining behavioral analytics company applies patented neuroscience technology to measure how familiar users are with their inputted PII before they click 'submit' and enter a company's fraud stack. NeuroID analyzes this pre-submit data in real time and determines if users are genuine or risky without adding any friction. This proprietary process enables deep visibility into a user's unique digital interactions and helps optimize identity verification orchestration, yet never collects customer data. NeuroID's dynamic behavioral intelligence is fully compatible with all anti-fraud software and is endlessly scalable against any advances in fraud technology. Visit NeuroID.com to learn how fintech, insurers, eCommerce, traditional banks, and others use ID Crowd Alert™ and ID Orchestrator™ to help safeguard their most valuable asset, the customer onboarding funnel.