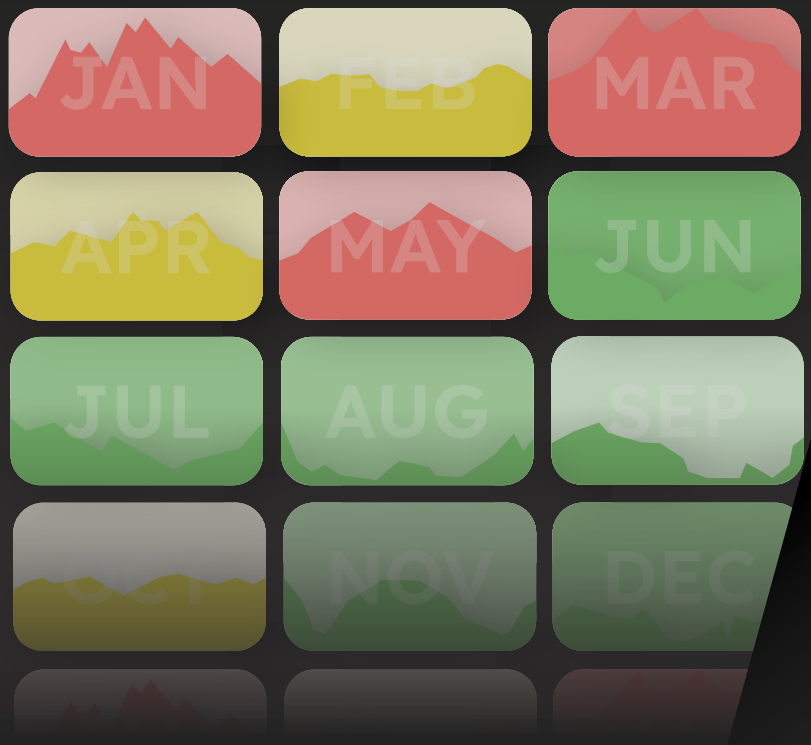
THE FRAUDSTER'S ALMANAC:

Your Guide to Preparing for Seasonal Fraud Attack Patterns



EMERGING TRENDS IN FRAUD SERIES EDITION 3

Fraudsters are constantly finding new ways to attack your stack. And unlike you, they have no budget constraints, compliance requirements, or approval processes holding them back from implementing new tools: fraudsters can weaponize AI, machine learning, and any other new tech much faster than any fraud prevention team can keep up. In fact, 83% of fraud professionals say that today's fraud schemes are evolving too quickly for them to keep pace, even ranking it as their number one challenge (this figure has nearly doubled from 43% in 2019).[1]

Despite 97% of fraud and risk professionals saying they have at least an average ability to detect and address fraud, only 19% say they can spot a fraud attack as it happens. And even if they can see the attack in real-time, only 11% say they could take immediate action to mitigate it in the moment.[2] This stark contrast between fraud-fighters' confidence in what they've built vs. their confidence in their stack's timeliness underscores the extreme difficulty of fighting fast-moving fraud and fast-changing tactics.

FRAUD & RISK PROFESSIONALS SAY THEY . . .

Have at least an average ability to detect fraud	Can spot a fraud attack as it happens	Can take immediate action to mitigate fraud
97%	**19%**	**11%**

Source: ISMG 2023 Survey

1. https://ismg.io/solutions/research/2023-faces-fraud-research-survey-results-report-pdf-7-w-12630/
2. https://ismg.io/solutions/research/2023-faces-fraud-research-survey-results-report-pdf-7-w-12630/

It's difficult—but not impossible. NeuroID's rich fraud attack data (drawn from our diverse customer pool of leading banks, emerging financial institutions, lenders, payment processors, insurers, consumer finance platforms, and more), enables us to dig deep into industry-agnostic third-party fraud trends.

About the Research

By analyzing 2023 fraud data—the timing, causes, effectiveness of response strategies, and more—we've collected best practices to proactively mitigate fraud, without adding to the noise, tailored to the risk level patterns of the year. Our research and prescriptive takeaways results will help you predict and counteract the strategies of fraud rings, bots, and other cybercriminals that would normally be most likely to slip through those unseen gaps, all without adding unnecessary complexity.

TABLE OF CONTENTS

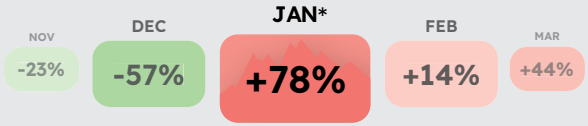
WINTER

New Year, New Fraud

Holiday shopping is the superbowl for risk teams and fraudsters. As Visa's Chief Risk Officer Paul Fabara put it, "Crooks prepare all year for the holiday shopping season, taking advantage of increased activity and consumers who let their guard down searching for the perfect gift."[3] In 2023, the 5 days between Thanksgiving and the following Monday (known as the Cyberfive), a full 3.6% of all global ecommerce transactions were suspected fraudulent. The daily average of suspected digital fraud attempts during that period was 18% higher than the same period in 2022 and 12% higher than average.[4]

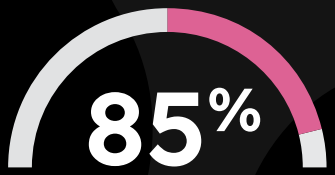
Part of the reason for the fraud increase is the fraud prevention decrease. At NeuroID, where we consult with our customers to create tailored risk thresholds, we see relaxed tolerances during the holidays, in exchange for more business coming in. But the fraud showdown doesn't stop when the last gift is purchased, or even when the last holiday decoration is taken down. In fact, according to our 2023 trend analysis, January is the most wonderful time of the year to be a fraudster.

January, so Contrary

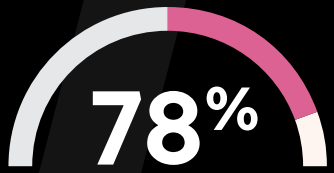


In January 2023 alone, our customers had fraud attack rates +78% higher than the monthly average. January attacks were also more all-inclusive, with +59% more fraudulent applications showing up to the party.

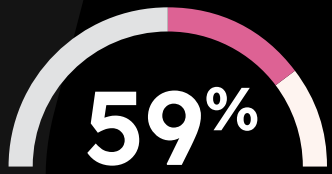
NeuroID alerts our clients to fraud attacks in real time, notifying them when we see a prolonged increase in the number of high risk users attempting to open accounts. NeuroID looks at these attacks hour-by-hour to assess their duration, potential damage, and attack patterns. In January, NeuroID clients suffered a +85% in the number of hours they had risky applicants attempting to onboard above their baselines. That +85% means a corresponding increase in manual reviews, identity checks and—if they hadn't been caught by NeuroID—fraud losses and potential credit repairs.



Increase in Hours Under Siege



Higher than Monthly Average Fraud Attack Rates



More Fraudulent Applications per Attempt

**Compared to 2023 fraud average*

3. www.paymentsdive.com/news/visa-holiday-fraud-ecommerce-store-shopping/700169/
4. newsroom.transunion.com/digital-holiday-fraud-in-2023/

Customer Story

Proactive Prevention Through Probing Detection

Aspiration

Financial Services Business with 1.2M Members

Aspiration's fraud prevention team had great data insights into their fraud attacks, but it was always after the fact. Their standard response was to trace the issue back to the source and set up controls to prevent similar methods. This worked most of the time but was frustratingly reactive. **"Sometimes there would be signals to put controls around; a certain IP range for example," says Josh Eurom, Manager of Fraud Strategy. "But we had a lot of unseen fraud we couldn't trace. We wanted to prevent fraud, rather than catch it in hindsight."** Aspiration needed to close that gap of unseen fraud and create proactive prevention.

In a trial period, Aspiration found that by utilizing NeuroID, they were able to capture 4x more fraud with a 97% confidence rate. NeuroID's new signal helped them decision in real-time and proactively capture unseen fraud that other tools missed. Read the full case study here.

> "To now be in a position where we can expect to have a fraud event is great. You're usually reacting to it and not preparing to take it on: **now, we see it coming and we're ready to respond as quickly as possible, rather than reverse engineering the solution for next time.**
>
> *-Josh Eurom, Manager of Fraud Strategy, Aspiration*

Implications and Strategies for Fraud Prevention Teams

In January, fraud stats mirror the first week at the gym: everyone shows up, newly resolved and focused. Unlike what we see in most months, every attack type went up in January, with no singular style, vector, or target standing out. From serious fraud rings to the first-time citizen fraudsters, the bad actors show up en masse and with a vengeance.

At the same time that attacks spike, increased holiday shopping has exposed more personally identifiable information (PII) to new sources, while fraud team's reduced risk thresholds—strategically designed to streamline applicants at holiday season—likely haven't had time to fully reverse. Everyone is crashing the fraud party, and the buffet table is set for easy pickings.

BEST PRACTICE Proactively Monitor for Probing

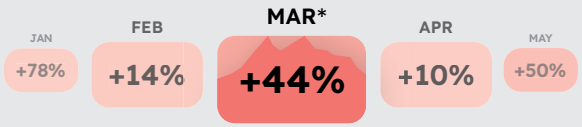
By monitoring crowd-level behavior, NeuroID is uniquely positioned to detect probing behavior on our clients applications. Probing is when a fraud ring is testing your perimeters—it often shows up as brief, fraudulent spikes in activity that stand out from baseline. Different short spikes of attack activity indicate varying probing strategies: they could be instances of ambient fraud, small-scale activity from novices and first-person fraudsters, or more focused fraud ring attacks testing your controls. Whatever the cause, these probing patterns are clear indicators of a future attack, and one that only NeuroID's next-gen behavioral analytics can detect. Incorporate real-time, unobtrusive crowd-level monitoring alerts to understand the nature of every probing threat and determine how to prevent damage from the true coming attack.

SPRING

Full Blooms of Fraud

If fraud seeds are planted deep in January, then March and May is where the attacks come to full bloom. Spring attacks are the most intense and the most dramatically dangerous. With a staggering +50% increase above fraud attack baseline, May presents a formidable challenge on its own—but before the May surge, we get a preview in March, with a +44% increase in the monthly average of fraud attacks. This one-two spring punch hits unprepared fraud teams hard.

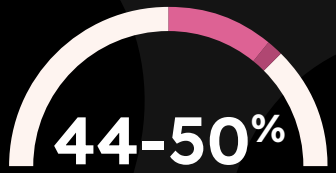
March Madness



March 2023 was the third highest month for fraud attacks, but severely more costly for any fraud team hit by one. March attacks had more than 3X the number of fraudulent applicants surging into the attack. These spikes lasted about the same amount of time as in other months, making their volume much more overwhelming.

Unsurprisingly, the fraudulent users from March attacks were also 2X more likely to trip NeuroID's fraud ring detector, a signal that looks for behavior known to be associated with fraud rings using stolen identities. Notoriously cunning, patient, and focused, often even taking the time to learn about their target's step-up policies and identity verification procedures, fraud rings are the worst-of-the-worst for aggressive cyberattacks.[5] And in March, they pop up like seasonal spring daisies. This spike of fraud ring attacks continued into April, which had the third highest month of fraud ring-specific attacks of the year (+67% above average).

With the average financial institution (FI) being attacked by bad actors every other week, these short bursts of risky activity are cues that fraudsters find an application attractive.[6] The spikes may be an exploratory probe of security systems to prepare for a more prolonged attack, or a more hopeful sign that fraud mitigation tools are successfully deterring attackers from pursuing anything further.



Increase in Hours Under Siege

3x

Number of Risky Applications Per Attack

2x

As Likely to be Fraud Ring Attacks

**Compared to 2023 fraud average*

5. https://www.neuro-id.com/resource/report/the-anatomy-of-a-fraud-ring-attack-report/
6. https://www.neuro-id.com/resource/blog/in-and-out-fraudsters-unmasking-short-lived-fraud-attacks/

Customer Story

Fraudsters Slip Through Gaps in PII-Reliant Fraud Stack

North America-based Full-Stack Payment Processing Fintech

A prominent payment processor servicing 3 million commercial U.S. customers was relying on a two-step process to mitigate fraud risk at the onboarding and transaction stage. This process was primarily PII-reliant, and they still saw a high volume of bad actors make it through. With these fraud mitigation strategies falling short, the payment processor turned to custom solutions and manual reviews, which proved too costly.

During a trial analysis of accounts, **NeuroID identified 100k+ dormant fraudster accounts, a section of unseen fraud that had slipped through their controls.** With behavioral analytics, the payment processor was able to close this gap in their fraud stack. With NeuroID now in place as part of the payment processor's account onboarding fraud mitigation, they get sub-second decisioning that also helps reduce the pressure on their overall fraud stack and manual review teams by discretely weeding out fraudsters in real-time. Read the full case study here.

Implications and Strategies for Fraud Prevention Teams

The cause of spring's surge is less clear-cut than January's jump, but there are some obvious correlating factors. The preparation for tax season, where sensitive personally identifiable information (PII) and financial details are exchanged across various platforms, creates fertile soil for digital fraud. It's also the end of the fiscal quarter for many businesses, which brings a disbursement of funds. In many U.S. states, March and May include Spring Break, Mother's Day, and the first blooms of summer vacation. This means that money is moving in large amounts online on websites not commonly frequented by most consumers (such as hotel bookings), with PII potentially exposed as travelers take advantage of public wi-fi at airports and hotels and generally go into a less-vigilant vacation-mode mindset.

Insecure PII is an irresistible opportunity for fraud rings. While today's typical fraud stack includes many different technologies, they often overly rely on the same static, historic, and highly compromised PII data. As one cyberthreat analysis report put it when discussing the PII that most anti-fraud measures rely upon: "With such a large amount of personal and private records being stored on servers that are accessible to users worldwide with an internet connection, the exploitable attack surface is vast, making it nearly impossible to secure all systems properly."[7]

BEST PRACTICE Incorporate Non-PII Solutions

As fraudsters continue to learn new ways to circumvent traditional fraud mitigation processes and use new technology to overcome modeling and rules creation, net new signals that don't rely on PII are key to finding unseen fraud and closing the gaps. NeuroID crowd alerting tracks the number of risky users coming to an application and alerts you to abnormal spikes in risk, so you can act immediately. NeuroID experts can also parse risky data signals, and show you if it's a test foreboding a future attack, or proof of a fortified system.

With most attacks lasting about a day, NeuroID's real-time risky behavior alerts ensure that fast-moving fraudsters are also stopped in real-time—closing the vulnerability gap that 83% of fraud professionals worry about and that only 11% say they can address.

7. https://www.recordedfuture.com/blog/business-fraud-sales-pii-phi

SUMMER

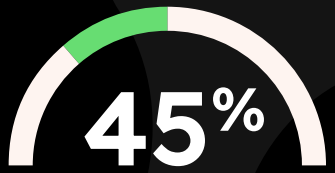
Sunny Skies for Fraud Teams

Summer sunshine brings clearer skies for teams who've been on high alert through the risky seasons. The quietest month in the fraudster's calendar, July has a striking -42% lower than average in attack numbers. July's attacks were also smaller in volume, with -69% fewer associated fraudulent applications per attack. June brought more attacks than July, but was still below baseline by 26%. June's strikes also included -85% fewer fraudulent applications per attack—even fewer per attack than July, and still far below baseline.

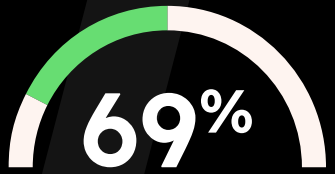
The low fraud numbers are more likely due to human nature than design: the summer months bring changes in consumer spending habits, with a shift towards outdoor activities and away from the types of online transactions that are prime fraudster targets.[8]

August: School Bells Chime & Fraud Rings Climb

As back-to-school season starts, fraudsters are back to their old tricks as well. Although summer's fraud attack volume is the lowest for the year, in August, 69% of attacks were fraud rings. August is the second-highest month of the year for fraud ring attacks as financial institutions (FIs) and ecommerce organizations boast tempting targets of back-to-school specials.



Decrease in Fraud Attacks



Decrease in Number of Risky Applicants per Attack

2x

Shorter than the Average Attack

**Compared to 2023 fraud average*

8. https://capitaloneshopping.com/research/online-shopping-trends/

Customer Story

Testing New Signals for Better Fraud Prevention

Addi

Leading financial services company with 1.2M+ customers

Addi was combating the extremely sophisticated fraud types that proliferate across Latin America (where 1-in-5 ecommerce transactions are fraudulent[9]). In addition to commonplace third-party fraud, more creative fraudsters were successfully making it past even the strenuous checks.

"One especially shady type were people who changed their name after they got to a step-up on approval, so we weren't able to contact them," said Mauro Jacome, Addi Head of Data Science. **"When I tried to gather that data from our front end so we could make better risk decisions, we did not have the capabilities. We needed a better fraud model to capture that data as well as streamline our onboarding process."**

Mauro investigated the vulnerabilities in their stack, tested several solutions, and decided that adding NeuroID to the top of onboarding would provide the net new signal that was missing. Read the full case study here.

> **We evaluated several similar vendors, and NeuroID was the best.** It has helped me out a lot in identifying those fraud patterns. Using NeuroID decisioning, we can confidently reject bad actors today who we used to take to step-up—we don't even pass them along at all.
>
> *-Mauro Jacome, Head of Data Science, Addi*

Implications and Strategies for Fraud Prevention Teams

Summer's slowdown is a time to regroup, reassess strategies, and prepare for the inevitable end-of-year uptick. Summer months provide a natural slowdown, without you adding prevention methods and heightened risk thresholds. Take this time to deeply analyze the previous seasons' data, identify emerging trends, refine fraud detection algorithms, and research new tools that could be implemented ahead of the fall/winter fraud showdown.

But don't get too lulled by summer's warm glow: Fraud attacks in August may fly under the radar because they're small in size and volume, but they can make you a bigger target for the rest of the year if fraudsters make it through.

BEST PRACTICE Summer Refresher

Summer is the perfect time to ensure that your fraud systems are agile and ready to respond to fraudsters returning from their holiday, so you can meet them with more robust and effective fraud prevention measures. It's the time to research and talk to vendors—but it's not the right time to implement change (check out Autumn for our thoughts on that distinction).

9. https://americasmi.com/insights/latin-america-payments-good-bad-ugly-2023/

AUTUMN

Fraud Fundamentals

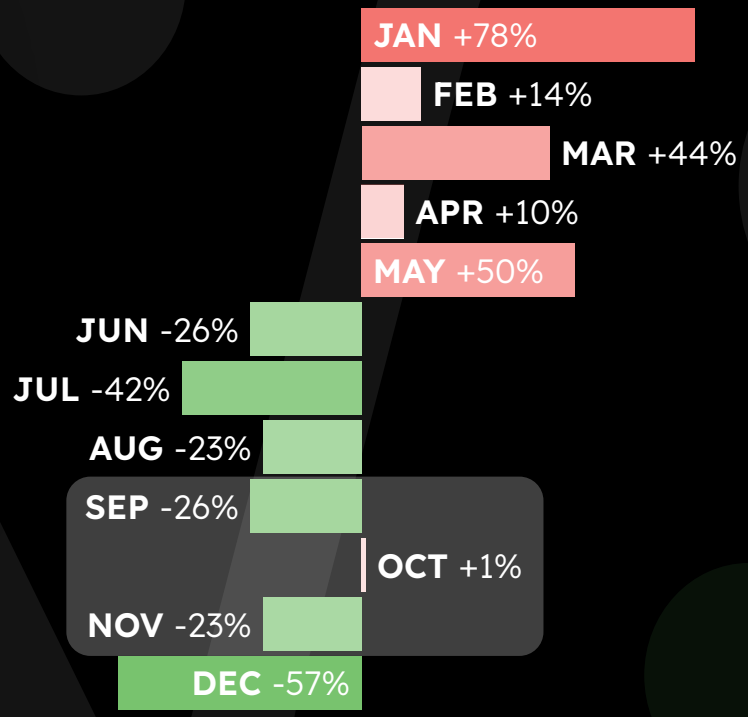
The crisp fall air hints at winter, and the fall cyberattack uptick foreshadows the coming holiday blitzes. September is nearly identical to August in terms of attack numbers, which is a +25% increase in fraud attacks compared to July (summer's lowest month).

In the lazy, hazy months of summer, every attack was at least -61% below average in fraudulent applications per attack. But in September, every attack had +13% above average attackers per attack: a 74 percentage point jump in just one month. We saw it starting in August, and even more starkly in September: fraud rings have begun to organize again. This ramp up in fraudulent applicant numbers is the first sign of the holiday fraud starting a slow boil, heating up by back-to-school shopping, end-of-fiscal year purchases, credit card offers ahead of the holiday season, and other opportunities.

The Fall Fraud Foreshadow

In October, fraud attack volume jumped from September's -26% below average to +7% above average. It's not a huge leap compared to January (where, if you recall, the hours jumped +85%), but it indicates a tug-of-war between fraud teams and fraudsters. October also has the average quantity of fraud attacks—aligning to the baseline that every other month is compared to. Again, this is ho-hum compared to January and March's fraud spikes, but significant amidst the lower activity of October's surrounding months: both September and November have at least -20% below average in attack numbers. Overall, fall is the recalibration season, where fraud numbers are closest to baseline. This makes it a crucial testing ground for both sides of the fraud game to refine their strategies ahead of the holidays.

Changes in Fraud Attack Volume from Average



Autumn Months Are Closest to Baseline for Fraud Attack Volume

*Compared to 2023 fraud average

Customer Story

Adapting to Fraud Rings With Flexible Detection

Elevate

Digital lender

Sophisticated fraud rings employed complex strategies to bypass Elevate's fraud prevention measures. These bad actors, using stolen information, would launch coordinated attacks, submitting multiple applications within a short timeframe. This overwhelmed Elevate's traditional fraud systems.

"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 NeuroID," said Ryan Prince, Manager of Data Science for Elevate. "Having something that actually looks at the behavior adds a level of security and analysis." By incorporating NeuroID's flexible fraud detection, Elevate was able to adapt to more aggressive fraud rings that other tools couldn't capture. Read the full case study here.

> Just analyzing the behavior is so helpful because **we're able to cut out that fraud without additional hurdles on the customer side.**
>
> *-Ryan Prince, Manager of Data Science, Elevate*

Implications and Strategies for Fraud Prevention Teams

By October, 56% of U.S. consumers have already started holiday shopping—both fraudsters and fraud teams alike are cracking their knuckles to prepare for what's next.[10] The fall is the time to implement what you've learned in the summer and get it ready for the upcoming risky seasons.

BEST PRACTICE Invest in Automated, Adaptive Fraud Detection

If you're looking for new vendors to add, summer is a terrible time—fraud is low, so the feedback is unreliable. The winter and spring have huge attack spikes; you don't want to risk testing a new vendor or methodology while in the thick of attack season. But fall, with its basic, baseline pumpkin spice vibes is the best time to actually try something new. You can test vendors and solutions through attacks that have impact, but not crushing volume, and anything worth implementing you can get in place before the high-risk of holiday season. This is the time to simulate attacks and address vulnerabilities, refine escalation systems, run pilot programs, and determine what thresholds should be measured or explore new data points to improve detection accuracy.

There are often signals that fraud teams can put controls around (think, a certain IP range). But there's also the unseen fraud that's untraceable and is only caught in hindsight. That's where dynamic adjustments to fluctuating risk levels come in. For example, NeuroID provides early warnings of increased activity that can't be caught with other controls. Proactive use of behavioral analytics gives you the ability to scale up automation and adjust fraud detection sensitivity and rules in anticipation of fraud ebbs and flows.

10. www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/us-holiday-shopping-2022-tis-the-season-to-be-cautiously-optimistic

Navigating the Seasonal Waves of Fraud

In a typical month, NeuroID customers get attacked an average of once every other week; in the riskiest months of the year, it's one attack every ten days, with 25% of customers having more than 3 fraud attacks in the month. Without adequate fraud capture, this would mean more cascading impacts of costly manual reviews, identity checks, fraud mitigation costs, and potential credit repairs.

Waves of fraud change with the season, and so should your risk tolerance. Dynamic fraud solutions that are flexible throughout the year help you adapt to not only high-risk periods, but new emerging attack styles.

If you're reading this in March, maybe you've just been hit hard—give us a call, we can provide immediate, day-one value to find fraud that others can't. If you're reading this in June and thinking of where to optimize your stack, give us a call—we can help all your tools work better and get more out of your insights. NeuroID next-gen behavioral analytics and device solution helps you prepare for known periods of increased fraud activity, new attack styles, and anything else fraudsters throw at you any time of the year.

Learn More About NeuroID

NeuroID combines the power of industry-leading behavioral analytics with next-gen device intelligence to secure your entire user lifecycle, starting with the very first interaction. The only solution to combine the power of behavior and device, our unique approach identifies invisible fraud from day one. NeuroID's real-time, pre-submit fraud alerts, coupled with industry-specific best practices, empowers organizations to refine their fraud detection strategies for more precise outcomes with zero friction.