vyntra

A guide to handling fraud alerts



We take you through the three different frameworks for qualifying fraud alerts with real-life bank examples.

Fraud remains a huge challenge for banks. Not only does it cost them in terms of losses and reputation, but digitalization has increased the ways in which they can be attacked.The perpetrators, often orchestrated by organized criminal networks, are increasingly sophisticated and constantly evolve their attack methods.

On top of that, regulators are paying growing attention to fraud, and the cost of addressing it has become significant. As if that weren't bad enough, fraud rates continue to rise, despite the best efforts of the regulators, law enforcement and the banks themselves.

The banks' approach has historically been dictated by compliance concerns and balancing the cost of detection and prevention against the risk of losses. But with fraud rates increasing and fraud typologies constantly changing, internal units can find themselves under-resourced and/or inappropriately structured, becoming overwhelmed.
Banks monitor for fraud in many different ways, but however they approach it, their processes will throw up hits – or alerts – for suspicious transactions. These hits must be qualified as to the level of risk they pose.

Depending on the case, the transaction may either be released or stopped while it is investigated and resolved, with the payment either being refused or passed to settlement. This paper looks at how banks structure themselves to handle the alert review process for these hits.

Three approaches to handling fraud

Essentially, there are three frameworks for handling hits, each with its own advantages and disadvantages.

The **centralized framework** involves a dedicated team that qualifies the alerts and the level of risk they pose.

The **decentralized framework** has dedicated team members who sit in different departments and liaise with colleagues across the bank to qualify alerts.

Lastly, the **hybrid framework** typically sees a central team handle critical and high-risk alerts while less complex alerts are handled by other people in other departments.

The best approach for a bank comes down to its circumstances, organizational structure and client-relationship culture.

Established processes, available resources, volume of transactions, speed of the bank's growth, level of digitalization, skills, customer type, market, geography and business maturity all play a part. And as circumstances change, the bank may need to consider altering its approach.

The centralized framework

Attributes

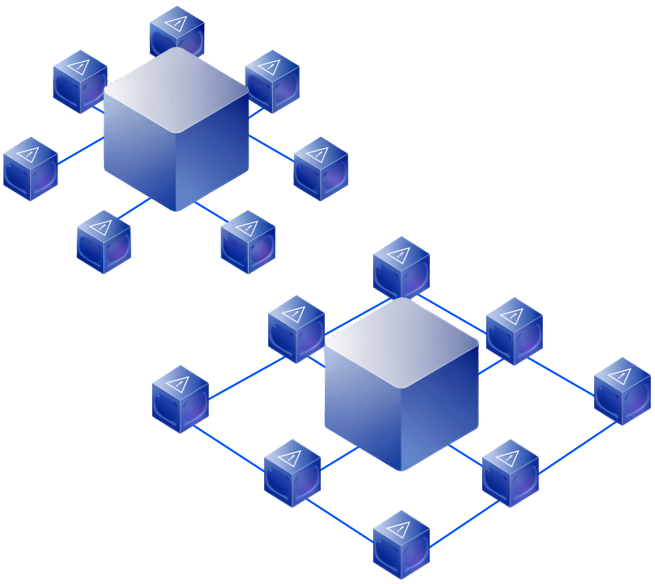
- A dedicated team qualifies alerts
- Cases are managed centrally
- Alert ownership is at system level (all controls are owned and monitored by one team)

Pros

- Normally recommended to ensure maximum utilization of the system
- Speed
- Internal fraud becomes more difficult

Cons

- Implementation costs can be high
- The dedicated unit requires resources
- Can be hard to scale
- Central team members need to understand different functions of the bank to successfully and efficiently resolve alerts
- Requires interdepartmental co-operation for digital access to systems to halt transactions and suspend accounts
- Lack of customer knowledge may lead to erroneous callbacks



The decentralized framework

Attributes

- Dedicated team members sit in relevant units/departments to qualify alerts
- In advanced markets, alert ownership is at the module level (departments owning specific modules – ie digital modules to digital team, callback procedures with relationship managers)
- At big retail banks in emerging markets, ownership is at the sub-department level
- Cases are distributed for qualification according to module ownership

Pros

- Cases can be dealt with by staff members who know the account best
- Cases can be moved across departments to smooth workloads
- Draws on existing resources so they can improve efficiency
- Easier to scale

Cons

- Alerts can pile up when staff are busy with their other activities
- Can leave the door open to internal fraud
- Compliance demands segregated data between business units and branches so analysts can't see inappropriate data

The hybrid framework

Attributes

- Central team handles critical and high-risk alerts
- Decentralized team handles fewer complex cases

Pros

- Draws on a broader range of knowledge and skills within the bank
- Can provide a more flexible response appropriate to the level of risk posed in respect of individual customers

Cons

- Complex to manage
- Can be more expensive Alerts
- Can be handled by the wrong team (inefficiency)

vyntra



Ownership – how to get it right

Every institution has its own characteristics, strengths and weaknesses, priorities and risk-appetite. That means each must review its own situation and the pros and cons of each framework to help decide which best suits them. But one thing is certain: **fraud prevention has to be embedded as a core pillar of a bank's governance and enterprise risk management strategy** and the framework it chooses must be integral to that.

Some banking characteristics appear to favor one framework over the others. For example, the more digital the bank is, the more a centralized framework makes sense as the technology can hold relevant information centrally to be accessed as required. Similarly, large banks tend toward a centralized framework. They may have more resources at their disposal, making it feasible to operate dedicated fraud-management teams.

For smaller banks, which may have fewer specialist teams and more generalists performing more than one role, decentralized fraud-handling tends to work well. Similarly, a bank working with legacy systems or with close personal relationships between banking advisor and client may have siloed information, which also plays to a decentralized framework.

The third category – hybrid – tends to favor larger banks that treat fraud prevention as a core pillar of their governance. They may well have more resources than smaller banks and can afford to run a centralized team, as well as ensure specialists elsewhere in the bank have the time to address more complex cases. Indeed, they work best when the centralized fraud team handles confirmed or suspicious cases, while manual investigation capabilities in the back office assess edge cases.

It's important to note, however, that the above are tendencies, rather than hard and fast rules. When a bank is deciding on a framework, it needs to look at the whole picture and how various characteristics interplay. It's also important to hold regular reviews to make sure that the adopted framework is still the optimal one. For example, a large, well-established bank that is digitalizing more of its operations and has an increasingly younger customer base is currently moving from a centralized to a decentralized framework. Its rationale is that local teams will have local knowledge, helping to bring context and speed up decisions.

Whether centralized, decentralized or hybrid, the fraud teams should operate 24/7 – fraudsters often target out-of- hours periods to increase their chances of success – and communication with clients should be in real time over a secure network during the transaction. Dynamic questioning based on the suspected typology – phishing, investment scam, romance scam, for example – is important, while the best way to define the fraud type is to use a balance between automation and human insight.

Given all the parameters mentioned above, many banks are unsure which framework would deliver the best results for them. After more than 13 years successfully fighting fraud, Vyntra has the experience and insight to help banks identify the right framework for them.

European Tier 1 bank

A Tier 1 bank based in Europe has adopted a hybrid fraud-detection model for alerts.

Up to 90% | Of fraud alerts are centrally managed by a specialized fraud unit

The balance (high-touch or special clients) is handled in a decentralized way by dedicated client-relationship managers

The bank chose this model to take advantage of operational efficiencies and to draw on and benefit from the experience of client-facing staff.

- Centralized experts are fraud specialists, handle cases daily and are highly efficient
- Decentralized advisors have closer relationships with clients and can communicate more personally and persuasively

Current client communication is primarily through phone calls as this enables human analysis and tailored questioning depending on fraud type.

However, the bank plans changes to automate and personalize communication based on:

- Fraud type
- Risk score
- Client history

The goal is to send targeted messages that reflect the likely fraud pattern (eg, phishing vs. investment scam). For example, clients sending money to known crypto scam addresses would receive alerts written for investment scams.

vyntra

vyntra

Transaction Intelligence powered by Intix & NetGuardians

Internal Fraud Prevention

NETGUARDIANS



A proactive and continuous approach to internal fraud detection. Offers a complete internal fraud detection cycle, from detection and triage to investigation and closure within a single platform.

The rising cost of occupational fraud

In 2024, the banking and financial services industry accounted for 19% of all occupational fraud cases - the highest among all sectors. These incidents resulted in an average loss of over $1.5 million, with a median undetected duration of 8 months.

Traditional approaches - based on static rules, manual controls, and fragmented oversight - not only fail to detect fraud early, but also generate overwhelming volumes of false positives. Even when initial red flags are raised, the time it takes to move from suspicion to grounded, actionable evidence is often too long. This delay allows harmful activity to continue, increasing financial loss and reputational risk.

Next-Gen Internal Fraud Protection

NetGuardians' Internal Fraud solution offers a proactive and continuous approach to internal fraud detection, going beyond traditional rule-based systems. By employing our advanced 3D AI combined with business logic, it can detect suspicious situations without relying on predefined scenarios. The solution leverages behavioral signs from employees and customers profiling to enhance detection accuracy. This adaptability ensures that even previously unknown fraud techniques are identified.

85%
reduction in false positives

10x
faster investigations

Key benefits

Delivers effective results quickly, with minimal setup or overhead.

Discourage opportunistic fraud by introducing continuous and proactive monitoring.

Detects fraud without relying on predefined scenarios, thanks to AI anomaly detection.

Drastically improves operational efficiency, by streamlining investigations.

communications@vyntra.com

Core capabilities

1. Drive Operational Efficiencies

Our AI does all the heavy lifting, offering deeper insights, reducing false positives, and improving operational efficiency. Alerts are aggregated by risk actors, e.g. employees, filtered according to business logic, and presented by degree of significance, enabling experts to focus on what matters most. Customizable workflows ensure full transparency, with proper documentation and segregation of duties.

2. Unrivaled Investigative Tools

Standardized, intuitive, widget-based dashboards support fast, effective case assessments by presenting at a glance all business-relevant information about employees and customers. Filtering, drill-down, and correlation capabilities enable more sophisticated and proactive investigations, helping analysts manually detect intricate cases across transactional, employee, and customer data.

3. Powerful Analytics and Adaptive Monitoring

Advanced AI models work alongside business logic to detect anomalies and suspicious patterns. The system combines pre-packaged use cases with agnostic analytics to uncover unknown fraud schemes, while an adaptive monitoring framework ensures new patterns and behaviors are easily integrated. Full customization guarantees flexibility across any business environment.

Fraud we Stop

- Misappropriation of assets
- Unauthorized Funds Transfer
- Internal-external collusion
- Client Statement Manipulation / Performance Misrepresentation
- Window Dressing / Temporary Fund Movement
- Account Takeover
- Check and Payment Tampering
- And others

Some References

UOB · PICTET · Bank of Africa · CBG · Banque Cantonale de Fribourg · VermögensZentrum · BCGE · Republic Bank · Dashen Bank

About Vyntra

Vyntra is a global leader in transaction intelligence, formed from the union of NetGuardians and Intix.

Combining deep expertise in financial crime prevention, Vyntra equips over 130 financial institutions in 60+ countries with intelligent tools to detect fraud, ensure AML compliance, and gain real-time visibility into every transaction.

Contact us

For more information on internal fraud prevention, please contact us: communications@vyntra.com

vyntra

Transaction Intelligence powered by Intix & NetGuardians

Payment Fraud Prevention

NETGUARDIANS



Prevent scam and fraud attempts in real time with a comprehensive solution for banking fraud operations.

Stop payment fraud in real-time.

✓ **Instantly stop fraudulent payments**
✓ **Quickly uncover new fraud patterns**
✓ **Reduce your false positives**

Fraud on the rise

As digital interactions take the lead, instant settlement is the new norm for payment schemes. Fraudsters are stepping up their game, getting more cunning every day. It's time to act swiftly and stay ahead. You need a proactive approach that identifies both known and emerging fraud patterns, ensuring real-time detection of fraudulent transactions.

Protect your customers

Meet Vyntra's payment fraud solution: real-time monitoring, less fraud, and fewer false positives. Pre-built AI models, robust case management, and intuitive investigative dashboards. Detect and stop fraudulent payments from authorized push payment scams, device compromise, account takeover and more. Ensure compliance with SWIFT CSP and PSD2 requirements.

Key benefits

Detect & prevent in real-time with pre-built AI models.

Uncover new & emerging threats using 3D AI

Reduce false positives using powerful behavioral profiling

Faster, flexible deployment to suit your needs - In cloud, on premise

85%
reduction in false positives

75%
savings in operating costs

100 million
Individuals protected worldwide

communications@vyntra.com

Core capabilities

1. Stop fraudulent transactions in real time

NetGuardians' payment fraud prevention solution integrates within your payment processing flow and analyzes payments through 3D AI risk models to accurately detect suspicious behaviors. It monitors large volumes of transactions in real-time, offering deeper insights, reducing false positives and improving operational efficiencies.

2. Pre-built AI models

Our AI risk models do all the heavy lifting. Forget complex and expensive data science projects. These pre-built models more accurately detect fraud with lower false positives, helping you to quickly start preventing fraud. By continually learning and through feedback, the models keep your fraud prevention controls optimized and relevant, even when facing changing threats.

3. Powerful case management

Alerts are raised in real time, routed to the appropriate team and intuitively contextualized. Explainable AI, supported by natural language visual 'Evidence Cards' ensures you can immediately understand every alert. You can even target and automate customer callbacks.

4. Unrivaled investigative tool

Standardized and intuitive widget-based dashboards help you visualize, understand and contextualize transactional behavior. Powerful forensic capabilities help you easily and accurately make informed decisions. If required, you can quickly adjust or extend these dashboards from a widget library.

Frauds We Stop

- Invoice scams
- Social engineering fraud
- APP fraud
- SWIFT network fraud
- Malware compromised eBanking sessions
- Hijacked eBanking sessions
- SIM swaps
- Identity theft from phishing
- CEO fraud
- Love scams
- Fake mBanking apps
- And others

Some References

UOB · PICTET · Swissquote · CBG · Bank of Africa · Zürcher Kantonalbank · NBK · Lombard Odier · ALEXBANK · VermögensZentrum

About Vyntra

Vyntra is a global leader in transaction intelligence, formed from the union of NetGuardians and Intix.

Combining deep expertise in financial crime prevention, Vyntra equips over 130 financial institutions in 60+ countries with intelligent tools to detect fraud, ensure AML compliance, and gain real-time visibility into every transaction.

Contact us

For more information on payment fraud prevention, please contact us: communications@vyntra.com