
NICE
Actimize
2023
FRAUD
INSIGHTS
REPORT
Know more. Risk less.

Executive Summary

The fight against fraud is a never-ending battle, and the stakes are higher than ever. In our 2023 NICE Actimize Fraud Insights Report, we delved deeply into the banking and payments landscape, analyzing billions of transactions to uncover the most pressing threats and patterns impacting financial institutions.

The news is mixed, as on one hand, financial institutions (FIs) are successfully blocking unauthorized fraud attempts through advanced authentication technology. But on the other hand, fraudsters are shifting their focus to a more insidious tactic: manipulating customers into authorizing payments for them through social engineering scams. This new form of authorized payments fraud is becoming an increasingly prevalent and formidable threat: only complicating the existing fraud landscape and putting FIs at risk of double loss scenarios—both first-party and third-party victims.

And with the widespread adoption of faster payment rails, fraudsters have a streamlined and accelerated process to cash out their ill-gotten gains. As our world becomes increasingly digital and cashless, money mules have become the go-to strategy for cunning fraudsters looking to launder stolen funds. By exploiting unsuspecting individuals to open fake accounts and transfer illicit money, these malicious actors are creating a new frontier in financial crime.

But don't despair, there is hope. By leveraging the power of artificial intelligence, behavioral biometrics, and machine learning, FIs can improve their prevention and detection capabilities and stay one step ahead of the fraudsters. With the right systems in place, they can avoid reputational damage and customer attrition that often follows a successful scam.

As the fraud landscape continues to evolve, it's crucial for FIs to have adaptive and continuously updated systems that are equipped to meet emerging threats. With the potential shift in liability to FIs for authorized payments fraud, revenue protection is of the utmost importance. NICE Actimize's solutions, featuring advanced AI, analytics, and typology-specific models, can help you safeguard your institution in 2023 and beyond.

Leverage our collective intelligence to spot emerging threats and safeguard your organization in 2023.

Yuval Marco
General Manager, Enterprise Fraud Management,
NICE Actimize

Fraud is on the Rise

NICE Actimize Industry Insights

Attempted Fraud Transaction Volumes

+92%

Attempted Fraud Amounts

+146%

Year over year for 2022 vs. 2021

The battle against fraud is intensifying as criminal masterminds continue to evolve their tactics to exploit new vulnerabilities in the financial system. The global shift toward cashless transactions has resulted in a surge in fraud across all channels, from online and mobile transactions to in-person transactions. According to our analyzed data, attempted fraud transactions have skyrocketed by 92% and attempted fraud amounts have soared by 146%. This alarming trend highlights two key points: first, there is a dramatic increase in overall transaction volumes and second, fraudsters are becoming bolder and targeting higher fraud amounts. Fraud is not limited to one specific channel; it's a complex, multi-channel threat that is shaped by digital transformation, changing consumer behaviors and shifting fraud patterns. Financial institutions must stay vigilant and adapt their defenses to stay ahead of the constantly evolving fraud landscape.

For the Fraud Fighter

Optimizing reporting should be at the forefront of any fraud program. Fraud shifts and reporting must adjust accordingly. To capture stats like attempted fraud volumes and amounts, reporting needs to be tailored at both the macro and micro levels.

Macro-level reports should look at overall portfolio monitoring and fraud typologies:

- Account Acceptance Rate
- New Account/Opening
- Account Takeover (ATO)
- Channel Attack Rates
- "New" Authorized Payment Fraud (Scams)

Micro-level reporting should be from a more historical (traditional) vantage point. Reporting at this level would be more granular and looking at individual transaction types and performance of:

- Models
- Rules
- Alert Rates
- False Positives
- False Negatives
- Overall Recovery Rates

Increasingly, some fraud management teams are going the extra mile on reporting to capture "The Total Cost of Fraud", including:

- Consumer/Client Experience
- Fraud Losses
- Operational Expenses
- Regulatory Compliance

The State of Payments Fraud

Consumer expectation is that they have the ability to transact business anytime, anywhere, and from any device. Modernization has enabled this capability.

These are the four key areas of continued growth:

1. Global mobile payment market is estimated to be **$4.23 trillion** in 2022 and is expected to reach **$15.75 trillion** by 2027, growing at a CAGR of **30.07%**. [1]
2. Contactless payment market is estimated to be worth **$164.15 billion** by 2030. [2]
3. Global P2P payments market size is projected to reach **$8.07 trillion** by 2030, growing at a CAGR of **17.53%**. [3]
4. Card Not Present (CNP) continues to increase, as does the fraud losses. Projected for 2023, CNP fraud losses will total **$48 billion**, which is up **16%** from **$41 billion** in 2022. [4]

NICE Actimize Industry Insights

Individual transactions are showing significant attack rates:

P2P	Check	Wire/ACH
+40%	**+171%**	**+75%**
Attempted Fraud $ Amount	Attempted Fraud $ Amount	Attempted Fraud $ Amount

Year over year for 2022 vs. 2021

For the Fraud Fighter

As the world races toward a cashless future, payment modernization has opened the door to fraud vulnerabilities. This expansion comes with an ever-growing need for stringent security measures. Fraud risk managers must stay vigilant, ensuring their risk assessments are comprehensive and airtight. Impact analysis must go deeper to truly grasp the potential vulnerabilities and proactively mitigate them.

Fraud risk assessments are required to evaluate:

- Customer impact
- Potential increase in fraud & operational expense plan
- Incremental fraud tools or controls needed
- How new payments will equal new work volume
- If new channels require new integration points

> *"It is difficult to recover funds when they are moving in real-time online, so it's becoming more important for banks to not only put an effective fraud recovery procedure in place, but also develop rapport with other banks to speed up communication after a fraudulent transaction and stop the further flow of funds." – Shweta Ranjan, Asia Associate Director for Fraud Risk Management, Standard Chartered Bank. Dirty Dealing: Advancing the Fight Against Fraud in Asia Pacific (white paper)*

Scams are Surpassing Unauthorized Payments Fraud and ATO

24% of ATO victims had contact information changed before an ATO incident: Fraudsters want to steal funds or buy goods quickly, changing contact info so that the FI contacts the thief instead of the legitimate account holder if suspicions arise. [5]

FIs made a huge bet on authentication to secure their customers' accounts, but cunning fraudsters found a way around it. They went straight for the customers, causing authorized payments fraud (scams) transactions to soar by 30%.

The battle against this type of fraud is fierce. Fraud management teams have their work cut out for them to protect consumers from being scammed and victimized. In this fast-paced world of real-time payments, FIs are under pressure to provide a seamless customer experience while also keeping fraudsters at bay.

That's where artificial intelligence (AI) and machine learning (ML) come in. These cutting-edge technologies applied to fraud models can help FIs keep pace with the ever-evolving tactics of fraudsters. By analyzing vast amounts of data in real time, AI and ML can identify patterns, anomalies, and potential threats, enabling FIs to take action in mere nanoseconds.

By using AI and ML to enhance their fraud detection capabilities, FIs can flip the script on authorized payments fraud and turn it into a competitive advantage. They'll not only protect their customers from losing their hard-earned cash, but they'll also safeguard their own bottom line from the impact of shifted liabilities.

NICE Actimize Industry Insights

Attempted authorized payments fraud overtakes ATO:

Fraud Amount Share of Attempted Authorized Payments Fraud

56%

Fraud Amount Share of Attempted ATO

44%

Data collected in 2022

For the Fraud Fighter

When it comes to effectively combating fraud and monitoring scams, having a clear, comprehensive plan in place is crucial. This means crafting detailed reporting and playbooks that:

- Outline the measures your organization is taking to protect consumers from scams
- Track scam case progression, assessing consumer and financial exposure to losses
- Define recovery measures and return metrics

In some cases, reporting is mandatory, but this level of transparency not only demonstrates a commitment to consumer protection—it also enables continuous improvement and refinement of fraud management strategies.

As the global financial landscape shifts, so do the guidelines surrounding authorized payments fraud reimbursement and consumer liability. To a greater extent, these planned or pending guidelines favor refunding customers who are scammed. This means that fraud loss plans will need to be ramped up to meet these changes.

Fraud management teams must take a more proactive approach to fraud detection and prevention, particularly with money mules and scams. That's where multi-model execution comes in—it enables a holistic view of risk that takes into account unauthorized payments and authorized payments fraud, as well as money mule activity. With a multi-model execution approach, FIs can adapt to new fraud trends, effectively protecting consumers along with their bottom line.

> *"Most consumers are not aware of the limits of their FI's liability when it comes to reimbursement for fraud." – Trace Fooshée, Strategic Advisor, Aite-Novarica Group, from "Evolve Your Fraud Strategy: Customer Life Cycle Risk Management" (webinar)*

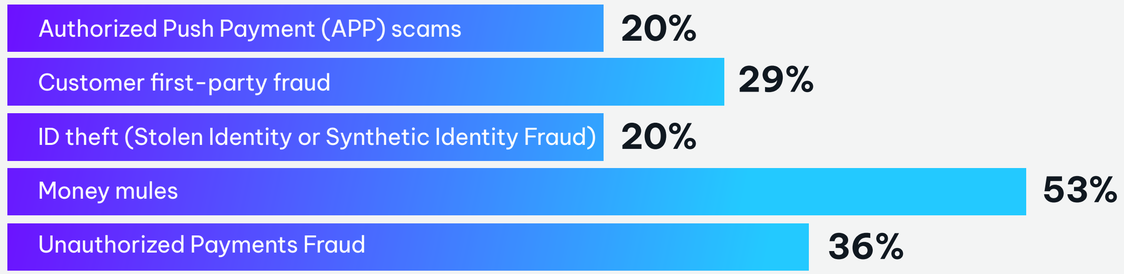
Fraud Types Gaining Traction

Fraud continues to morph, so FIs must be nimble at the changing fraud methods. The ever-changing threat vector continues to keep fraud practitioners on their toes. A recent survey of fraud leaders showed that there's continued stress in these five specific areas: **Account Take Over, Unauthorized Fraud, Authorized Push Payment (APP) scams, Mules,** and **First-Party Fraud.**

These issues could be viewed as a web of intermingled fraud tactics. Weak controls at customer onboarding fuel the flame for both first-party fraud and mules. Economic downturn and the expansion of faster payments rails add gas to the fire, resulting in higher instances of fraud events and losses. As reimbursement practices and regulations come into focus, FIs must protect their front door. It's vital to monitor customers across their life cycle, gain a complete view of risk, and interdict immediately.

Global Fraud Leaders Weigh In

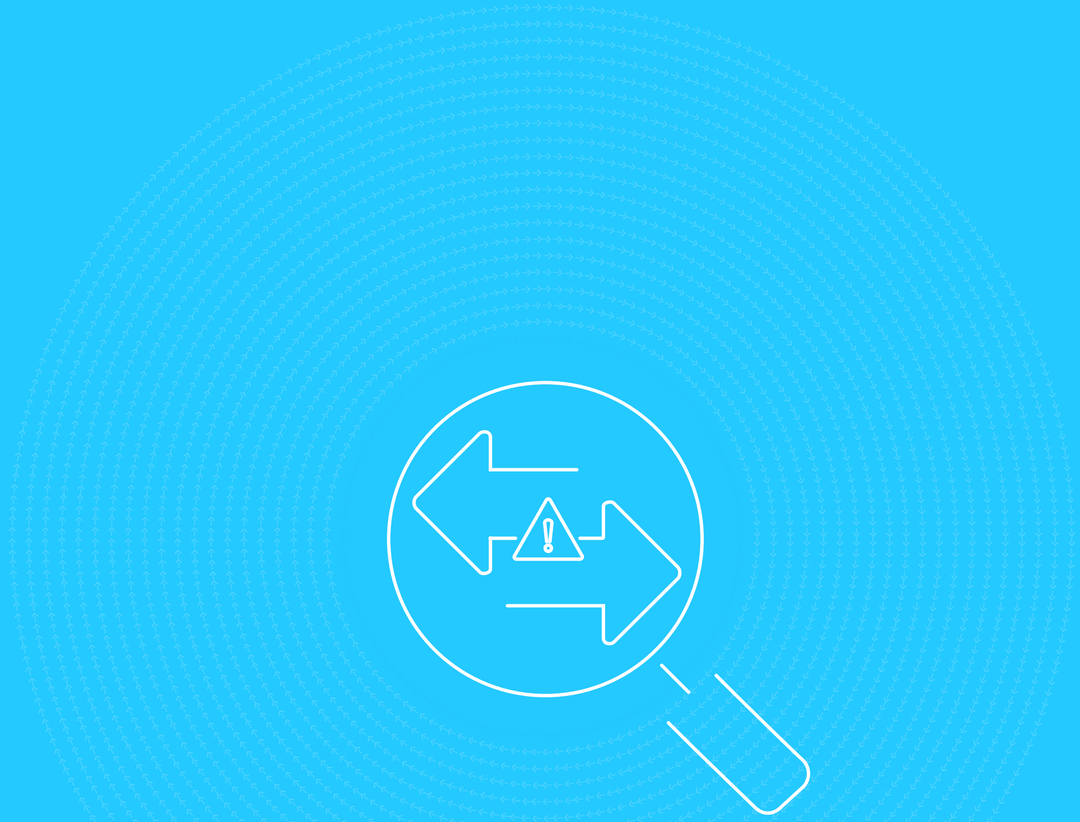
What are the top 5 challenges posing the greatest fraud threats to financial institutions today?



NICE Actimize

For the Fraud Fighter

As the digital landscape evolves, so do fraudsters' tactics. The five threats mentioned earlier are a glaring reminder of the ever-present danger that looms over digital channels and payments. Fraud fighters, it's time to fortify your defenses. Review your digital channel controls, and augment that data with both inbound and outbound payments to detect any suspicious activity, whether it's from complicit or non-complicit parties.



Fraud is Dynamic and Typology Driven

We've monitored three distinct fraud typologies: **Authorized Payments Fraud, ATO,** and **New Account Fraud.**

FIs must adopt a typology-driven approach, as each type of fraud is unique and requires its own data and models to determine anomalous behaviors. Regardless of the liability shift, FIs must implement intelligent, purpose-built solutions to protect customers from devastating losses.

This approach will also mitigate reputational damages and customer attrition: According to Javelin Strategy & Research, fraud victims are 31% more likely to leave the institution, even if the FI isn't responsible.

FIs with lacking controls are left exposed and vulnerable to the changing fraud environment.

For the Fraud Fighter

Gone are the days of treating fraud as an isolated problem. The shift from transaction-level tracking to typology-based reporting is a game changer. A more holistic approach enables FIs to target their efforts and develop tailored solutions to combat fraud.

By layering in cutting-edge technologies like ML and AI, FIs can stop even the most sophisticated fraud schemes.

Transitioning to typology-loss reporting is a strategic move. Instead of just scratching the surface, typology-loss reporting goes much deeper, providing a comprehensive understanding of the underlying business challenges to address. FIs can develop tailored solutions to combat fraud, which leads to a more efficient fraud management strategy.

NICE Actimize Industry Insights

Attempted global fraud rate:

Authorized Payments Fraud
+17.4%

New Account Fraud
-15.7%

ATO
+35.1%

Year over year for 2022 vs. 2021

A Closer Look into Authorized Payments Fraud

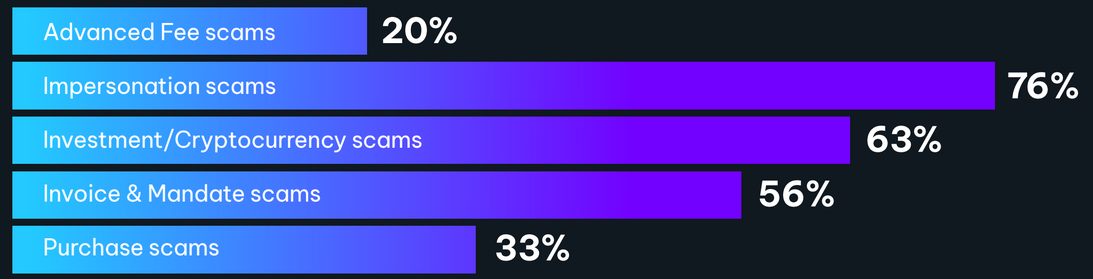
Why is authorized payments fraud hard to detect? Enhanced fraud controls and monitoring tools for ATO or unauthorized payments fraud simply aren't effective against authorized payments fraud. For example, consider this: a verified user at a verified location on a trusted device demonstrating genuine behaviors to transfer money instantly. The potential for traditional tools to detect anomalous payment behavior indicators won't work.

Diverse, sophisticated scams are almost impossible to detect with linear, traditional controls. Instead, FIs need to:

- Detect scams and typologies in parallel via advanced analytics and purpose-built models relevant to the specific typology
- Incorporate non-transactional data into detection algorithms that are risk-specific to the signals that are being monitored

Global Fraud Leaders Weigh In

What are the top 5 most prevalent scams affecting your organization?



For the Fraud Fighter

FIs need to uncover the unique fingerprints of each scam type. By capturing and analyzing these scam types, they can tailor their approach. They need to target specific client segments with precision-crafted messaging and awareness campaigns and launch focused fraud and scam controls.

> *"As the frequency and intensity of challenges to regulatory structures that govern reimbursement policies mount in the U.K., and as they inevitably find their way across the Atlantic and into markets around the globe, there can be little doubt that FIs will have to marshal considerable resources in their efforts to effectively protect their customers from scams. While daunting, it is a challenge that can be met and mastered with the right collaboration, innovation, and thoughtful strategy." – Trace Fooshée, Strategic Advisor, Aite-Novarica Group, Anatomy of the Emerging Scam Threat white paper*

New Accounts Get Better with Age

Fraudsters use stolen and synthetic identities to open up accounts to commit a crime—whether it's to cash out, bust out, or enable money mule activity. This trend raises the stakes surrounding new accounts that are far riskier than mature accounts.

New Accounts are

9.5

times riskier than mature accounts.

Accounts that are within 0-45 days qualify as new

There's also a significant application fraud issue. And while it might not tie directly to loss, it represents a foothold into maturing an identity, moving ill-gotten gains, and driving larger schemes associated with credit and loan products.

For the Fraud Fighter

It's a crucial but risky moment for both the FI and the account holder during onboarding. That's why monitoring doesn't stop at day zero. Data collected at the beginning serves as a solid foundation for continuous due diligence and monitoring. Think of it as a never-ending background check.

> *"[If they are already in the books], you might start considering fraud behavior as normal customer interactions, and that gives them free reign to commit unlimited fraud." – Benjamin Geertz, Vice President, Risk Management, Wells Fargo, "Evolve Your Fraud Strategy: Customer Life Cycle Risk Management" (webinar)*

Money Mules at the Center of Fraud

Money mules are a key factor in authorized payments fraud and scams, new account fraud, and money laundering.

While mules don't generate direct loss at their FI, they impact revenue. How? Because these accounts aren't profitable, are costly to acquire and maintain, and expose FIs to regulatory scrutiny and reputational damage. Our data shows:

- **59% of new accounts of application fraud are money mules, with the accounts going bad within 45 days, indicating that fraud is being conducted almost instantly**
- **More than 80% of fraud executives believe that more can and should be done to mitigate mule activity at their FI**[6]

Different mule types also display specific characteristics, creating further complexity:

- **Unwitting:** Anomalous account behavior versus normal transaction profile
- **Witting:** Accounts abruptly show excessive flow-through activity, with residual amounts indicated in the in/out funds ratios
- **Complicit:** New account red flags, and several accounts with similar digital footprint

Money movement will likely not trigger outbound transaction monitoring in rules-based systems, so FIs need the ability to detect inbound transactions.

NICE Actimize Industry Insights

59% of new account fraud is mule related, and the majority of these accounts demonstrate mule characteristics within 45 days

For the Fraud Fighter

When it comes to detecting money mules, looking for unusual activity on dormant or unused accounts is not sufficient. Fraud controls must be multilayered. Money mule activity often operates in rings, so the activity will be interconnected. Your models must consider many factors, including monetary and non-monetary activity and many-to-one and one-to-many relationships between:

- Account Holders
- Senders
- Receivers
- Payment Tokens
- Digital Trust Data Points

Additionally, insights from third-party enrichment sources like dark web intelligence can provide a valuable additional layer of protection.

> *"Whether the money mule knowingly or unknowingly participates in the laundering of funds transferred for fraudulent means, criminals are increasingly relying on money mules to do their dirty work." – Tracy Kitten, Director of Fraud & Security, Javelin Strategy & Research, Faster Payments For Faster Fraud: Protecting Customers In This Real-Time Environment (white paper)*

Outdated Tools Fail Against New Fraud Threats

Fraudsters are raising the bar, executing complex fraud and scams that are interrelated, accelerated, and industrialized.

New and emerging threats can't be fought with outdated tools. Collective intelligence-driven systems must be powered by:

- Advanced analytics
- Machine learning
- High-quality and diverse data
- Behavioral biometrics

This is the only recourse against modern fraud and scams.

Reputation, customer trust, and compliance are at risk. FIs need to proactively protect themselves and customers in this dynamic risk landscape.

Put these insights into action with NICE Actimize

NICE Actimize

1. ResearchandMarkets.com: Global Mobile Payment Market (2022-2027) by Pay Option, Purchase Type, Payment Type, Industry, Geography, Competitive Analysis and the Impact of Covid-19 with Ansoff Analysis (2022)

2. Grand View Research, Inc (study): Contactless Payment Market to be worth$164.15 Billion by 2030 (2022)

3. Straits Research: P2P Payments Market (2022)

4. CardNotPresent: Merchants Will Lose $48 Billion to Fraud Globally in 2023, Says Report (2022)

5. Aite-Novarica: 2022 U.S. Identity Theft: Adapting and Evolving (2022)

6. Aite-Novarica: The Emerging Case for Proactive Mule Detection: Going on the Offense to Defend Reputational Risk (2021)

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers' and investors' assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

Find us at www.niceactimize.com, @NICE_Actimize or Nasdaq: NICE.