

NICE Actimize

2024

**FRAUD
INSIGHTS**

FIRST EDITION

Executive Summary

As a fraud prevention professional, you know that nothing stays the same for very long in the world of fraud. Fraud prevention teams must navigate the increased speed of payments, open banking, and new technologies such as AI or ISO20022—this all points to fraud teams needing to adapt at breakneck speed.

This 2024 NICE Actimize Fraud Insights Report, First Edition, explores the evolution, rather than revolution, of fraud attacks financial institutions' (FIs) experience. Fraudsters are moving away from Account Takeover (ATO) to authorized fraud. There's also a shift in fraud typologies toward increased investment and romance scams.

This is fueled, in part, by fraudsters harnessing the power of AI for themselves, whether to craft better phishing emails, to create deep fake voices, or to perfect videos that execute impersonation frauds. This poses issues for FIs and their customers alike, as these scams are far more difficult to defend against.

When set against a backdrop of evolving payment trends—more payment options, new platforms and increased payment speed—additional challenges are seen. Faster payments are now the norm. Regardless of whether payments are Peer-to-Peer (P2P), Real-Time Payments (RTP), SEPA, FedNow or SWIFT—both volumes and values are growing fast.

However, there's good news, too. Investments in fraud technology are showing success, with overall P2P fraud rates decreasing in 2023. In addition, many other fraud typologies have reduced in either in volume or value. While this is encouraging, it's crucial that we don't get complacent, as fraud typologies that were on the backburner are on the rise now.

Perhaps the greatest force for change that FIs must contend with is the global shift in the regulatory mindset, toward greater liability for authorized fraud and scams. Later this year, the U.K. in particular will have the strongest regulatory regime in the world. FIs will have 100% liability, splitting payment to the victim 50/50 albeit with a few exceptions. This requires increased investment in both detection and case management to meet the regulations, while also safeguarding against the anticipated surge in first party fraud from re-imbursalment claims.

When taken all together, there's a need to manage fraud at the institution level. Removing payment type and channel silos while providing comprehensive coverage has never been more important.



Yuval Marco

General Manager, Enterprise Fraud Management,
NICE Actimize

Table of Contents



Overview

4



Authorized Fraud / Scams

5



Social Media's Role in Scams

9



P2P Fraud

10



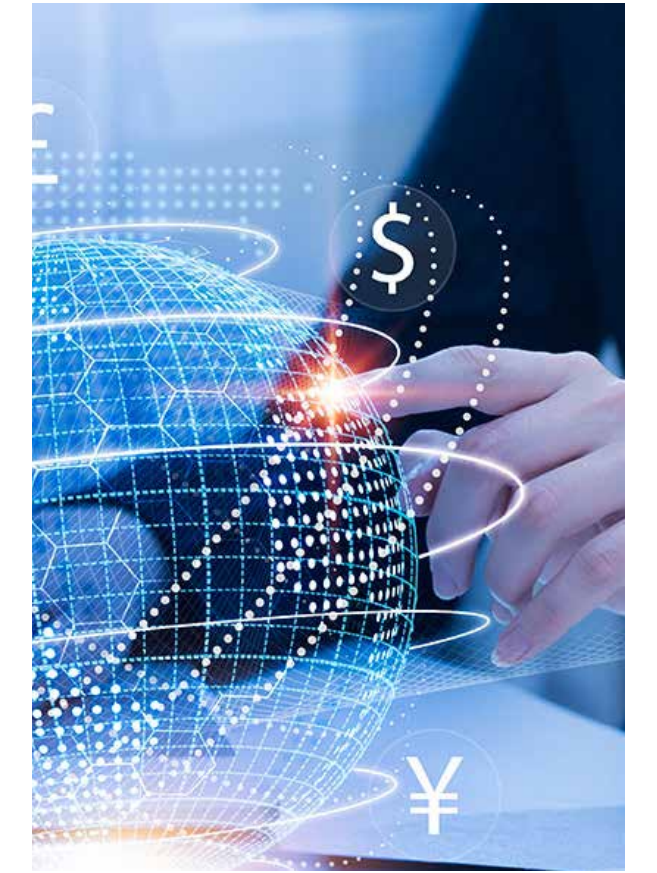
New Accounts & Mules

12



Check & Deposit Fraud

13



Account to Account

15

State of Fraud

NICE Actimize Industry Insights 2022 vs 2023

Total Fraud

Value **+6%**
Volume **-26%**

Authorized Fraud

Value **+11%**
Volume **+22%**

Unauthorized Fraud

Value **-33%**
Volume **-12%**

P2P Fraud

Value **-24%**
Volume **-36%**

Check Deposit Fraud

Value **+31%**
Volume **+4%**

International Wire Fraud

Value **-36%**
Volume **+2%**

Domestic Wire Fraud

Value **+7%**
Volume **+34%**

Authorized Fraud Continues to Outpace Unauthorized Fraud

Fraud, particularly authorized fraud, continued to rise across the globe in 2023. The fraud typology and payment type mix saw notable changes, particularly a continued shift away from account takeover (ATO) and P2P fraud towards authorized fraud, domestic wire fraud, and check & deposit fraud.

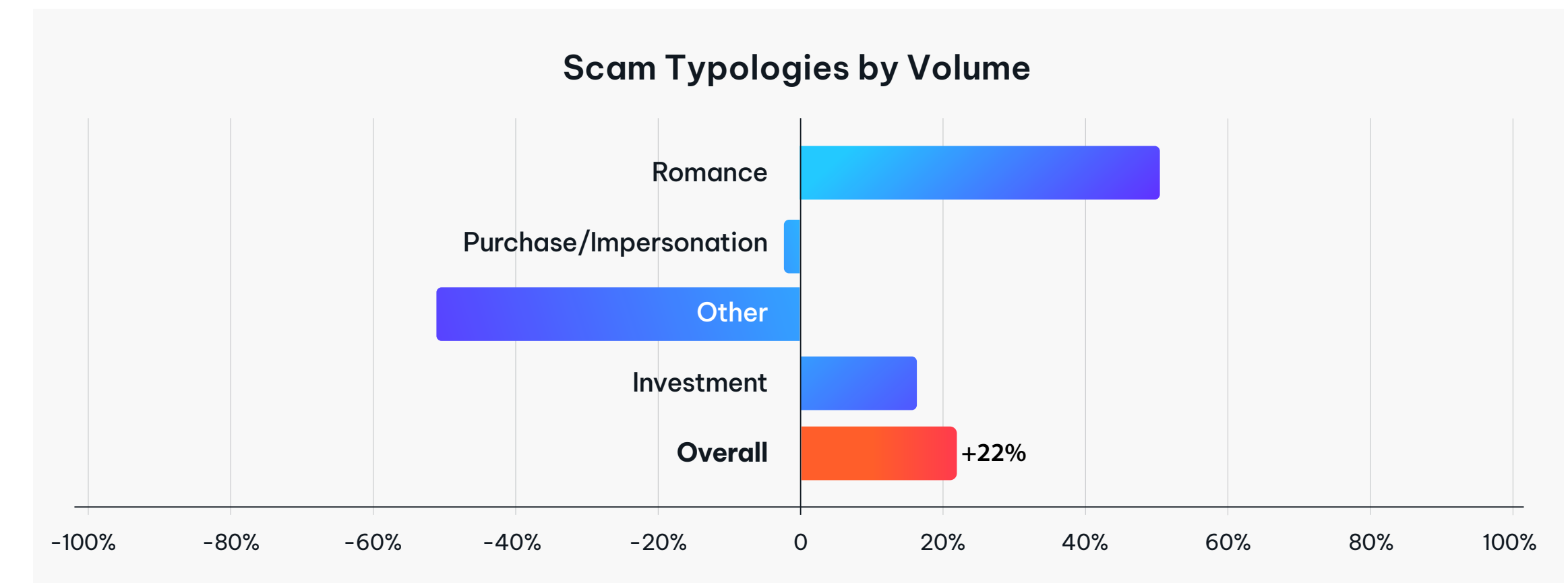
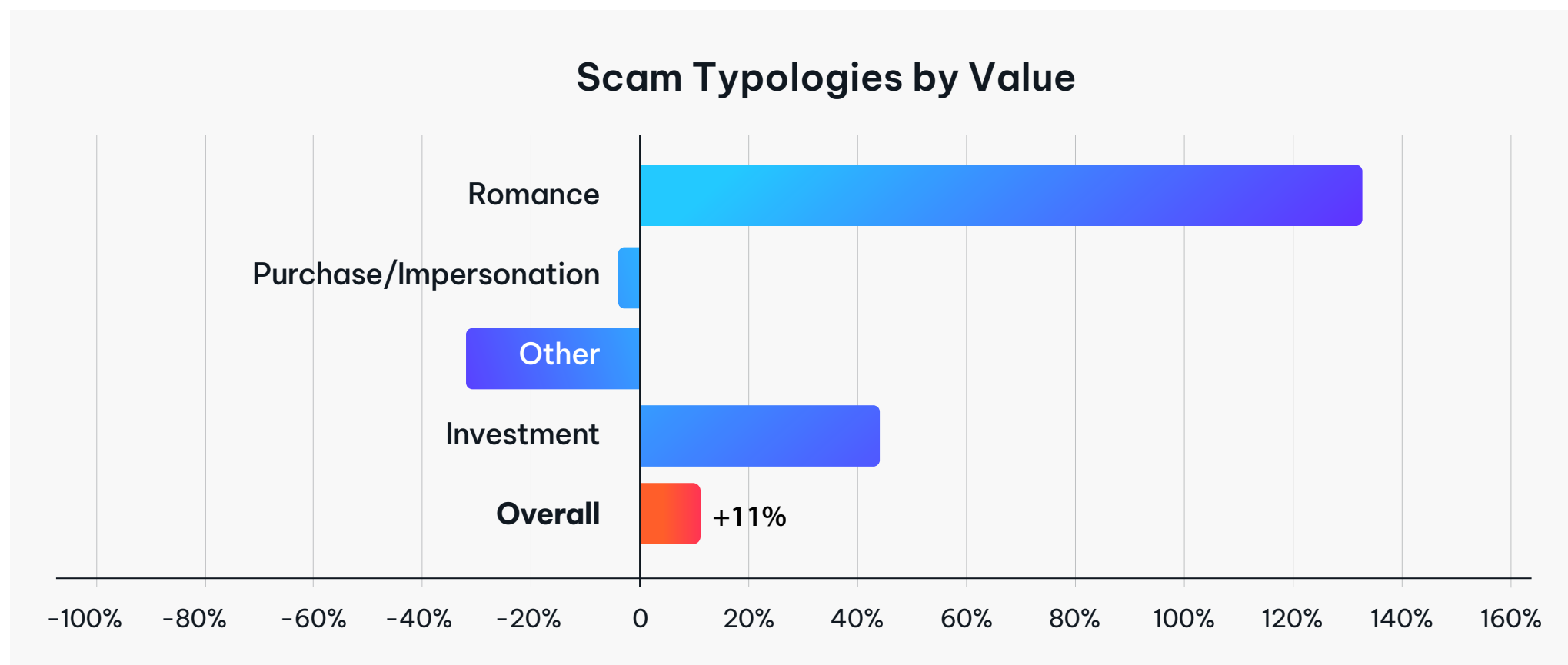
Attempted fraud increased in value (+6%) but decreased by volume (-26%). This change reflects the shift towards payment types and fraud typologies traditionally higher in volume and lower in value, as well as improvements in detection and prevention—especially in P2P.

The total P2P fraud value reduced significantly (-24%) as fraudsters shifted towards scams, reflecting the impact of lower average fraud values associated with P2P scams.

For other payment types, such as wires, fraudsters were more likely to use authorized fraud typologies, such as investment fraud, to conduct scams. The higher average value of these typologies, coupled with the increasing occurrence makes for higher losses.

Scams now make up a larger share of fraud than unauthorized fraud, and it's an increasing trend. While in many cases there are high-volume, low-value scams, such as purchase scams, there are also much higher value authorized frauds such as investment fraud or business email compromise (BEC) that impact authorized fraud's overall fraud mix.

NICE Actimize Industry Insights H2 2022 vs H2 2023





NICE Actimize industry data shows a large shift in domestic wire payments related to scams: a 44% increase in investment scams by value and 17% by volume and increases of 133% in romance scams by value and 50% by volume, away from purchase and impersonation fraud. These fraud typologies are often of higher value which results in increasing losses. However, the lower value typologies remain the lion's share of fraud.

Fraudsters increased use of AI across multiple fronts. Many criminals make use of generative AI to improve the grammar and believability of their phishing emails and scripts. Deep fake video calls have been leveraged for BEC fraud along the lines of impersonating a CEO or CFO. It's likely we will see increased sophistication in fraud attacks thanks to AI.



The FBI's latest IC3 Report¹ showed a 10% increase in reported case volumes, after a 5% fall in 2022. However, this was eclipsed by a 21% increase in value to \$12.5bn. This may only be a fraction of the real numbers, as it's highly likely that there's significant under-reporting.

The report highlights the scale of authorized fraud with the top three typologies totaling \$8.77bn, 70% of the total:

Investment
Fraud at
\$4.6B

Business Email
Compromise (BEC) at
\$2.9B

Impersonation Fraud (both tech
support & government) at
\$1.3B



On October 7, 2024, the UK will implement a 100% refund requirement², split 50/50 between the paying and beneficiary banks. With this liability shift, FIs need to take a different approach to how they mitigate losses, especially for authorized fraud.

This poses a few challenges:

- Circa £400M of liability, before any increases, will be shared by UK FIs, with £200M moving from customers and paying banks to beneficiary banks
- Claims processes must be amended to meet the new regulatory requirements, including customer vulnerability assessments and required SLAs
- Paying FIs must identify risk signals indicative of a scam before the payments are paid away
- Increased scam claims from both organized first-party fraudsters and opportunists need to be identified before refunding to prevent increased losses
- Beneficiary FIs need to monitor all inbound payments for key indicators of a scam or money mule

Anecdotal evidence from the UK suggests there is already a shift in purchase scams away from faster payments towards card payments. This reflects the effectiveness of controls added to payments and fraudsters' efforts to circumvent the UK's increased authentication measures using card.

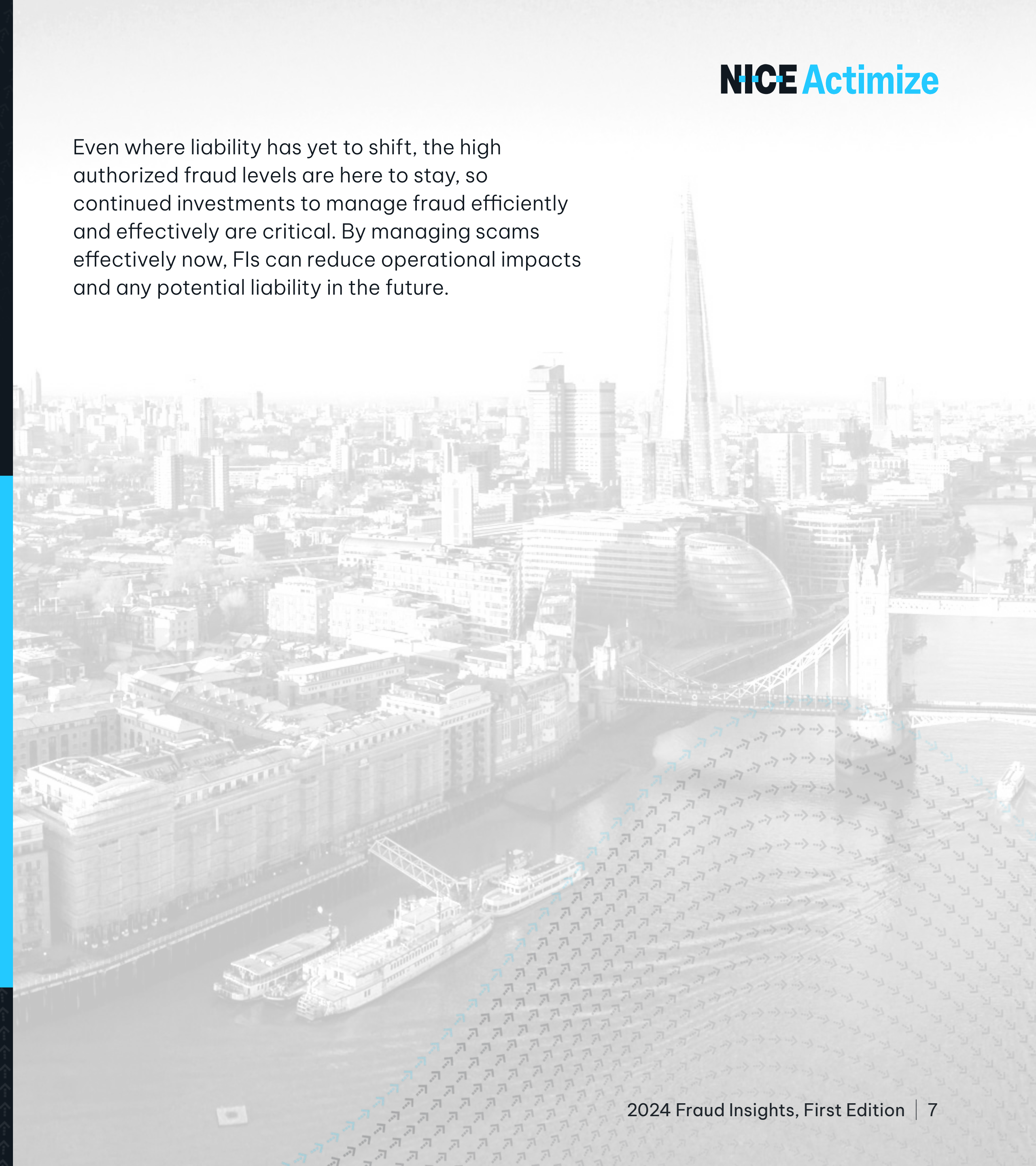
The size and growth rate of authorized fraud losses have garnered global regulatory attention, with a range of actions being put in place. In October 2024, UK refund requirements will shift, bringing liability to receiving banks for the first time. Other countries may look to the UK and implement similar measures to shift liability away from victims towards institutions. Failure to invest in stronger controls related to mules, from onboarding to inbound and outbound payments, will result in a surge in losses.

The escalating level of authorized fraud and a fast-changing regulatory landscape means fraud fighters must take a revised approach. FIs require a multidimensional strategy—one that covers unauthorized fraud, authorized fraud, mules and first-party abuse—to limit the level of liability and protect customers.

Even where liability has yet to shift, the high authorized fraud levels are here to stay, so continued investments to manage fraud efficiently and effectively are critical. By managing scams effectively now, FIs can reduce operational impacts and any potential liability in the future.

FIs Need a Multi-Layered Strategy

- ➡ 1 Customer education
- ➡ 2 Targeted warning messages
- ➡ 3 Real-time profiling for both outbound and inbound transactions
- ➡ 4 Typology-specific analytics and scoring
- ➡ 5 Entity-specific assessment of scams vulnerability
- ➡ 6 Integrated case management with high levels of automation



For the Fraud Fighter



Capitalize on External Intelligence

Use additional external intelligence to ascertain beneficiary risk, target first-party fraud and aid in authorized fraud detection:

- Mule account numbers
- High-risk entities
- Bad beneficiary names and URLs
- Device intelligence
- Behavioral analytics
- Persona data, telco data and geolocation information



Use Distinct Processes for Fraud Investigations

Offset liability with distinct strategies for each type of fraud that can:

- Detect first-party authorized claims
- Manage cases and refunds within regulatory timescales where regulated

Tailor Analytics and Strategies

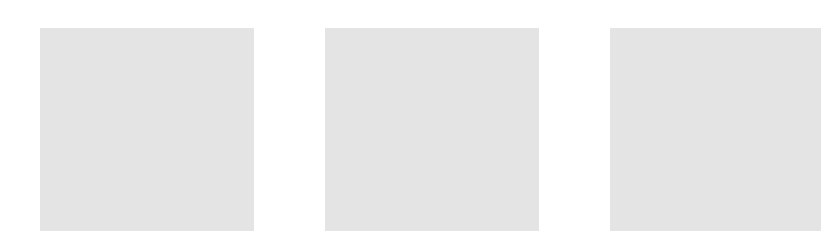
Simultaneously target each fraud type to maximize fraud findings while reducing false positives:

- Create multiple risk profiles to aid models and rules, including both beneficiary and institution risk and the payer and payers' institution risk
- Have separate machine learning (ML) models and scoring for ATO and authorized fraud
- Bring in holistic insights, beyond your own FI, using industry or collective intelligence
- Create strategies specific to each fraud type. For example, set up distinct step-up authentication for ATO and scams.



Strengthen Reporting

Improve reporting capabilities to better measure scams separately from unauthorized fraud and claims fraud rates.



Social Media's Role in Scams

Scams that originate from social media can cover a multitude of typologies and can span the entire fraud chain, from compromise to cash out. The latest UK Finance numbers show that 76% of frauds originate online, with social media being a key part of this.

The scams can be conducted via platforms, social media or messaging apps. Many investment scams in particular are conducted using messaging groups. Victims may be searching for investment opportunities online and discover these scams.

One such scam involves wire from card fraud. Wire from card fraud occurs when someone wires money to a payee bank account using a credit or debit card as the funding source. This is problematic because the protection of the credit or debit card to claw back those funds is removed since the fraudster can instantly access the funds. This feature makes wire from card fraud an ideal payment type for bad actors to exploit as part of a scam.

Examples of social media related scams include:

- Fake advertising on social media that takes a customer to a fake website that leads to an investment scam using a sophisticated web of interconnected companies
- Fake profiles that lure people to purchase products or services
- Job scams or enticements to become a mule drop account

The growing trend of embedding payments into social media is increasing fraudsters' ability to speed up funds transfer. Over the past several years, fintechs experiencing hyper growth lacked strong KYC processes and fraud controls that traditional FIs would apply to accounts. According to NICE Actimize research, this has translated into a growth in mule accounts.

For the Fraud Fighter

Significant changes can happen quickly, requiring careful monitoring to avoid large losses in a short timeframe. This can be achieved through improved machine learning to highlight small, but fast-changing fraud rates for detailed root cause analysis. In addition, self-learning fraud models can detect and interdict on new fraud typologies without retraining.

NICE Actimize Industry Insights 2022 vs 2023

Wires from card accounts - Fraud

Value	Volume
+168%	+235%

Wires from card accounts - Genuine

Value	Volume
+54%	+42%

NICE Actimize industry data shows a marked increase of 235% in wire transfer (MCC4826) volume from card accounts, now making up in 12% of CNP fraud. The recipient accounts are very often fintechs, and frequently related to social media-based revenue streams.

- **Root cause analysis can help identify key data attributes to stop fraud:**

- Track http headers to check origin of traffic to the payment type, e.g., has it been referred from high-risk websites/apps (where possible)
- Track fraud rates to specific beneficiaries to spot new trends and respond fast
- Build out institution scores to highlight higher risk FIs

- **Create specialist teams to discuss scam cases with customers to help prevent them from continuing to make scam payments**

P2P Fraud in Focus

NICE Actimize Industry Insights 2022 vs 2023

Total P2P Volume

Genuine + Fraud

Volume	Web	Mobile
+36%	+16%	+38%

P2P Channel Share

Genuine + Fraud

Web	Mobile
6%	94%

P2P Fraud

Value	Volume
-24%	-36%

P2P Fraud
\$ Avg. Amount
+13%

P2P Web Fraud
\$ Avg. Amount
+17%

P2P Mobile Fraud
\$ Avg. Amount
+12%

P2P Web Fraud Rate is
5X greater than Mobile

Genuine transactions on P2P have surged 36% by volume and 38% by value. This shows that consumers value the benefits of faster payments and feel that they are safe to use, despite the constant talk of fraud.


While fraud alert volumes (+14%) are not keeping pace with transaction volumes (+36%), they're still increasing, so continual model improvements are required to catch more fraud while ensuring false positives remain low.


A Success Story


Web based P2P transactions constitute only 6% of the total P2P transaction volume, yet have a fraud rate over 5X that of mobile based P2P transactions. Despite growing transaction volumes and the higher fraud rate, fraud fighters have been able to reduce web P2P fraud alerts 20% in the past year.


Faster payments are now the dominant non-card payment type and continue to see strong growth globally. P2P transaction volumes are only going to continue to grow as new rails are added, existing payment types are cannibalized, and user behavior changes deliver organic growth.


To put this in perspective:

 US P2P volumes were up **28%** (volume and value) to **2.9bn & \$806bn** respectively³ in 2023

 An EU mandate⁶ to enforce faster payments, covering **36 countries**, comes into force around end of 2024 and into 2025

 Real-time payment volumes⁴ were up **70%**, with value up **51%** (Q4 22 to Q4 23) running at around **\$40bn** per quarter

 Switzerland and Canada are poised to add faster payments rails in the next two years

 UK Faster Payments⁵ are up **14%** by volume and **15%** by value to **£3.7tn** even after 15 years of growth

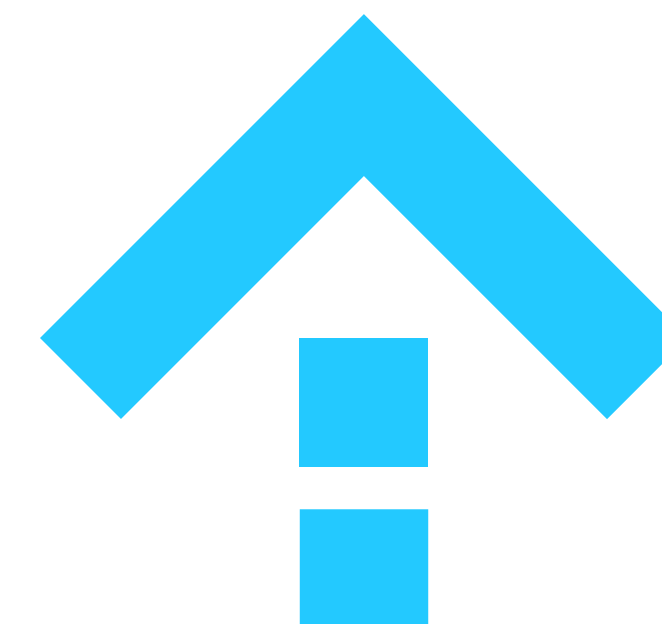
For the Fraud Fighter

Higher overall P2P volumes can make it much easier for fraudsters to hide their transactions within the genuine volume. Therefore, taking steps toward lower false positive rates (FPR) on models becomes as important as finding the fraud.

To manage this, along with the extra difficulty authorized fraud brings, organizations should consider developing multilayered strategies rather than a basic accept/decline strategy.

Strategies for Reducing FPR

- Decline the highest risk payments outright
- Refer and review payments in real time
- Where legally allowed, build in delays
- Develop specific warning messages and content, both within the customer journey and out-of-band, to encourage customers to think twice about transactions
- Ensure there's a true single view of each customer to minimize false positives. Knowing how the customer behaves across all channels can provide valuable insights to remove genuine transactions and identify cross-channel frauds prior to the final money movement
- Leverage network risk scores and scheme risk data, whether positive or negative, to aid in differentiation and help reduce FPR



New Accounts & Mules

Money mules continue to be a key mechanism in both unauthorized and authorized payments fraud. Preventing and detecting mules must become an integral part of an FI's fraud prevention strategy.

Money mules in P2P

Improvements in P2P fraud due to increased controls has led to the reduction in volume and value of mule frauds in 2023 versus 2022. Given the data showing increases in wire from card frauds going to fintech accounts, it's safe to assume that mules have migrated to these types of providers.

However, not all mules appear the same. They are a mixture of identity theft, synthetic and first-party perpetrators.

Even within first-party, there is a mixture of types that makes detection difficult:

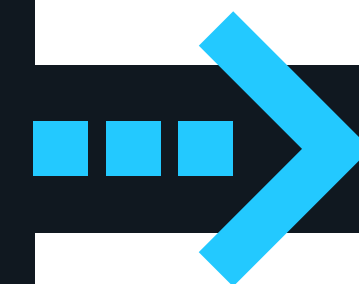
- Witting and unwitting, e.g., a 'friend' asks to move some funds through an account is a witting mule
- Accounts of previously genuine customers that may have been sold on or 'rented' out to act as mules, hiding the real abuse
- Victims of job scams who believe they are working for a legitimate company (unwitting mules)

Age of Accounts

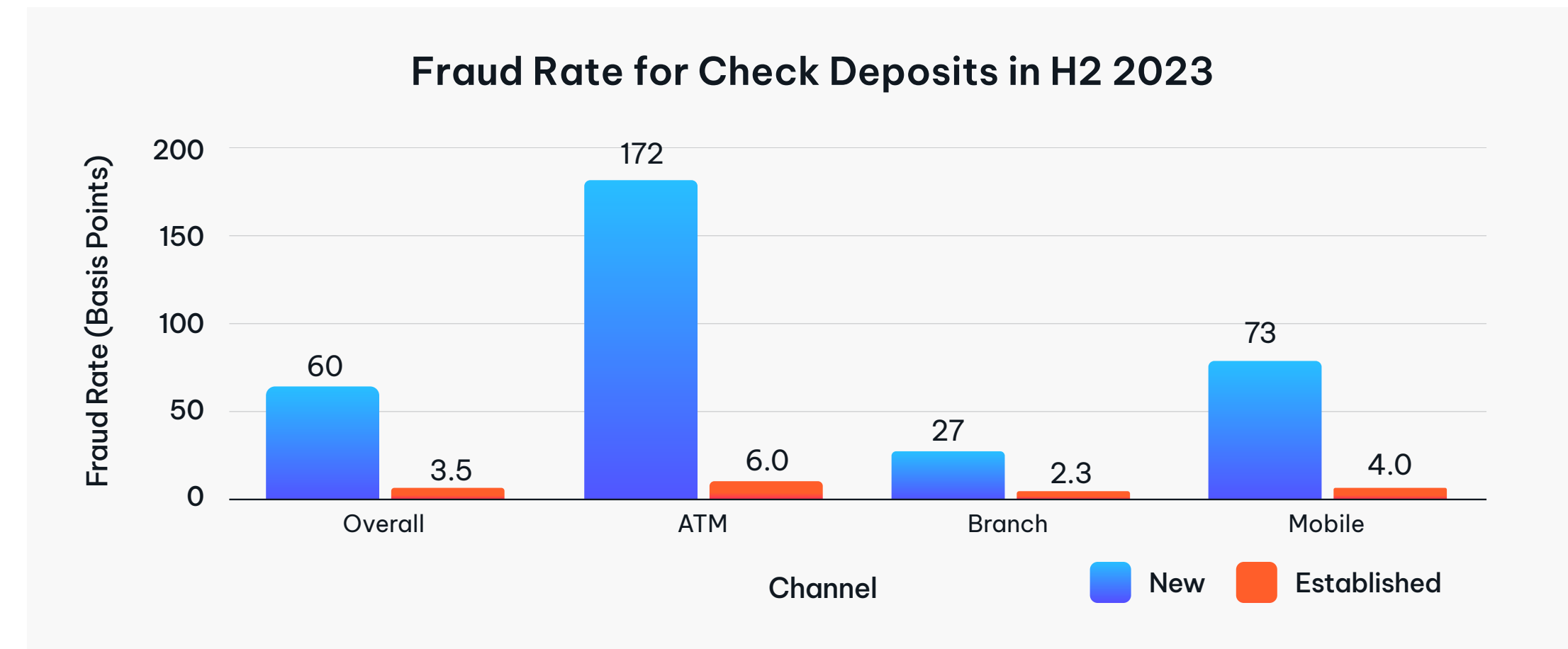
Not all transactions and channels carry the same level of risk, but new accounts are far more likely to be involved in fraudulent transactions across the board.

For example, for deposits, remote channels such as ATM and mobile are higher risk than branches. When adding age of account into the mix, the differences are stark.

The fraud rate increases from 2.3 bps to 172 bps when comparing the lowest risk deposits (branch deposits for established accounts) to the highest risk deposits (ATM deposits for new accounts). All types of fraud, including mules and bust out, exhibit this trend, increasing for new accounts.



NICE Actimize Industry Insights



For the Fraud Fighter

Money mules and new accounts represent a high level of risk to FIs. As the regulatory landscape changes, accurately managing mules and new accounts is even more critical.

Strategies to consider include:

- Improve application fraud detection and early account monitoring to prevent onboarding money mules at the earliest stages, limiting the scope of abuse
- Ensure inbound payments are profiled in real time, looking at the sender and beneficiary risk profiles, and link to further outbound payments to prevent onward transmission of funds
- Undertake extensive link/network analysis, using network scores within models and rules
- Improve model performance and highlight fraud rings with data sharing and the power of collective intelligence
- Develop processes for exiting accounts to ensure exits can be achieved, while not tipping off fraudsters

Check Deposit Fraud in Focus

NICE Actimize Industry Insights H2 2022 vs H2 2023

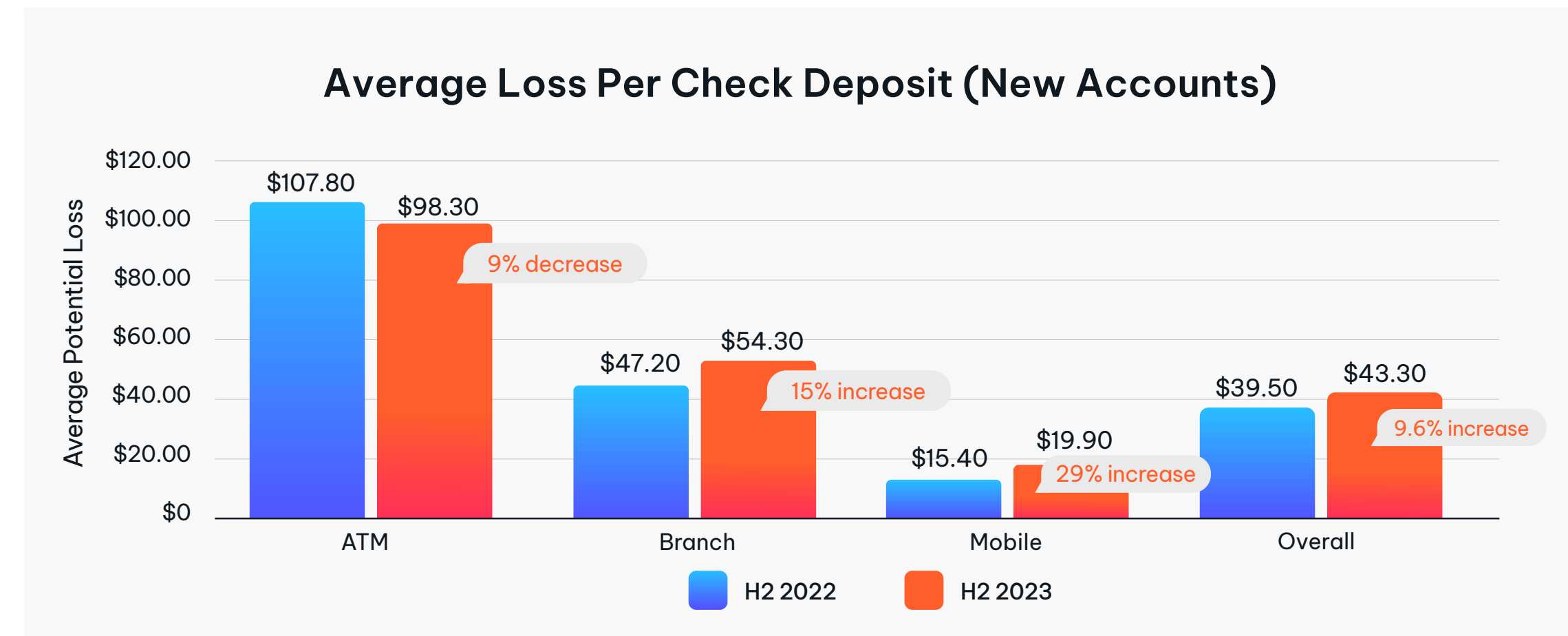
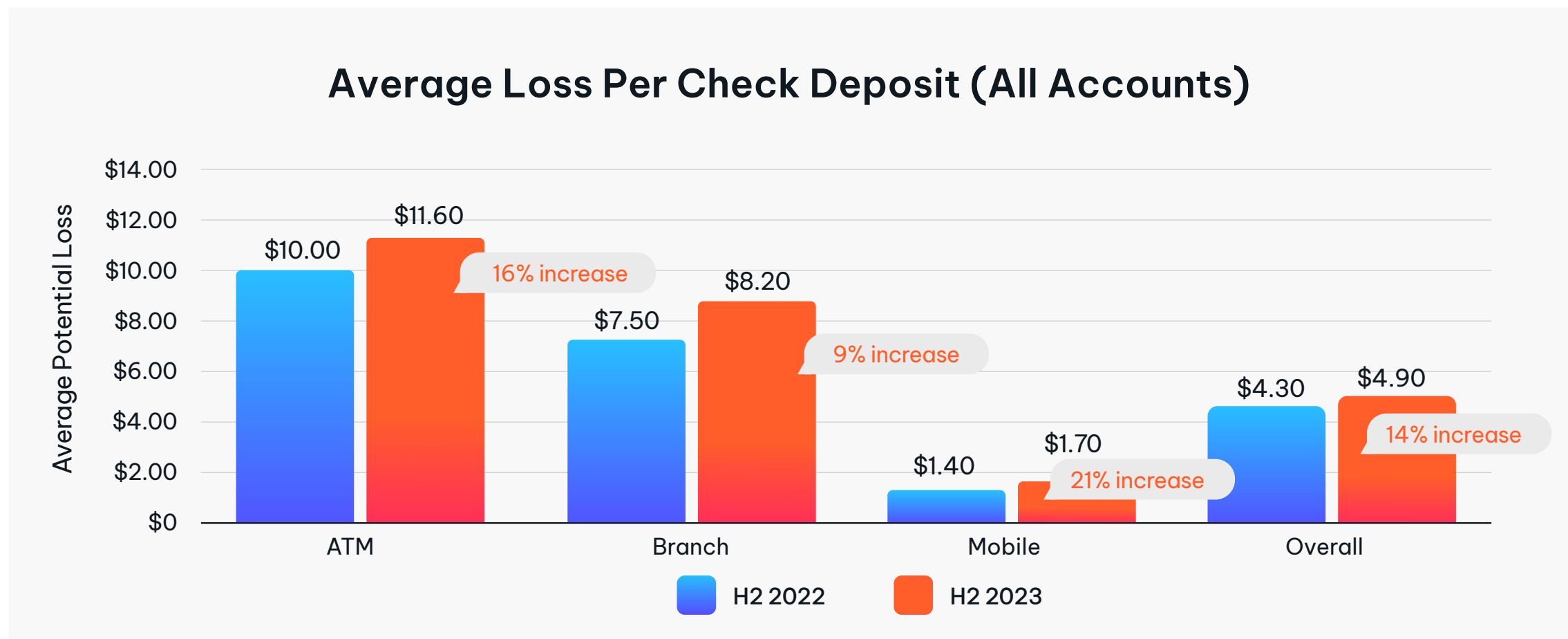
Check Deposit Fraud

Value	Volume	Fraud Rate	Avg. loss per check deposit
+31%	+4%	-11%	+14%

Check deposit fraud refuses to go away. NICE Actimize data shows that check deposit fraud increased 31% by value and 4% by volume, despite an 11% decrease in the fraud rate from H2 2022. These changes have not been distributed evenly across channels and account tenure.

New accounts are still much riskier than established accounts with a higher fraud rate (17x) and average loss per check deposit (\$43.30). However, Actimize data shows progress with a 25% reduction in the new account check deposit fraud rate and a 43% reduction in the branch-based deposit rate. These decreases more than offset the increase in average loss per check deposit.

Fraudsters have turned to established accounts. While the branch-based deposit fraud rate has decreased 21%, both ATM (+4%) and Mobile (+17%) fraud rates by volume have increased. When coupled with increases in the average loss per check deposit, this results in the growth of fraud by value for established accounts.



While check deposits at ATMs are part of a wider move to reduce operating costs, the fraud rates mean that the average fraud cost per check deposit is \$11.60*, up 16% year over year. This is high and must be factored into an FI's strategy, but is still relatively cheap compared to the branch staff costs.

The fraud rate by volume is worse for mobile than branch, however, the loss per deposit for mobile is the lowest overall at \$1.70, likely reflecting channel limits.

For the Fraud Fighter

Clearly, fraudsters are starting to use established accounts to recruit mules and evade controls targeted at new accounts. These established accounts are either synthetics fraudsters have aged or real accounts they've gained access to using job scams among other efforts. So, while best practice is to put channel limits in place that are tied to the age of the account, the real solutions lie elsewhere:

- Ensure customer profiling is conducted prior to the check deposit, to highlight customers who are at high risk of being or becoming a money mule
- Use network analysis and changes to customer profiles over time to identify behavioral shifts. This may include shifts in both transaction data and behavioral biometrics & device data that may indicate an account has been sold for use by a "mule herder"
- Integrate specialist check fraud imaging within your fraud scoring solutions to identify counterfeit, forged or altered checks



* Gross potential loss per check deposit

Account to Account in Focus

International Wire Fraud

Value
-36%

Volume
+2%

Domestic Wire Fraud

Value
+7%

Volume
+34%

As faster payments usage evolves, how wires are being used and abused is changing.

International wires particularly have seen significant drops in genuine usage. The average fraud values have also dropped nearly 40% as fraudsters became more cognizant of abiding by payment limits and rules to safeguard against detection.

The fraud rates on international wire typologies have experienced big shifts. The authorized fraud rate jumped 40% only to be beat by unauthorized fraud which soared 76% to 277 bps, or 2.77% of international wires by value. This trend moves counter to that of overall payments fraud which is trending towards authorized fraud. International wire unauthorized fraud now has a fraud rate four to five times higher than authorized fraud.

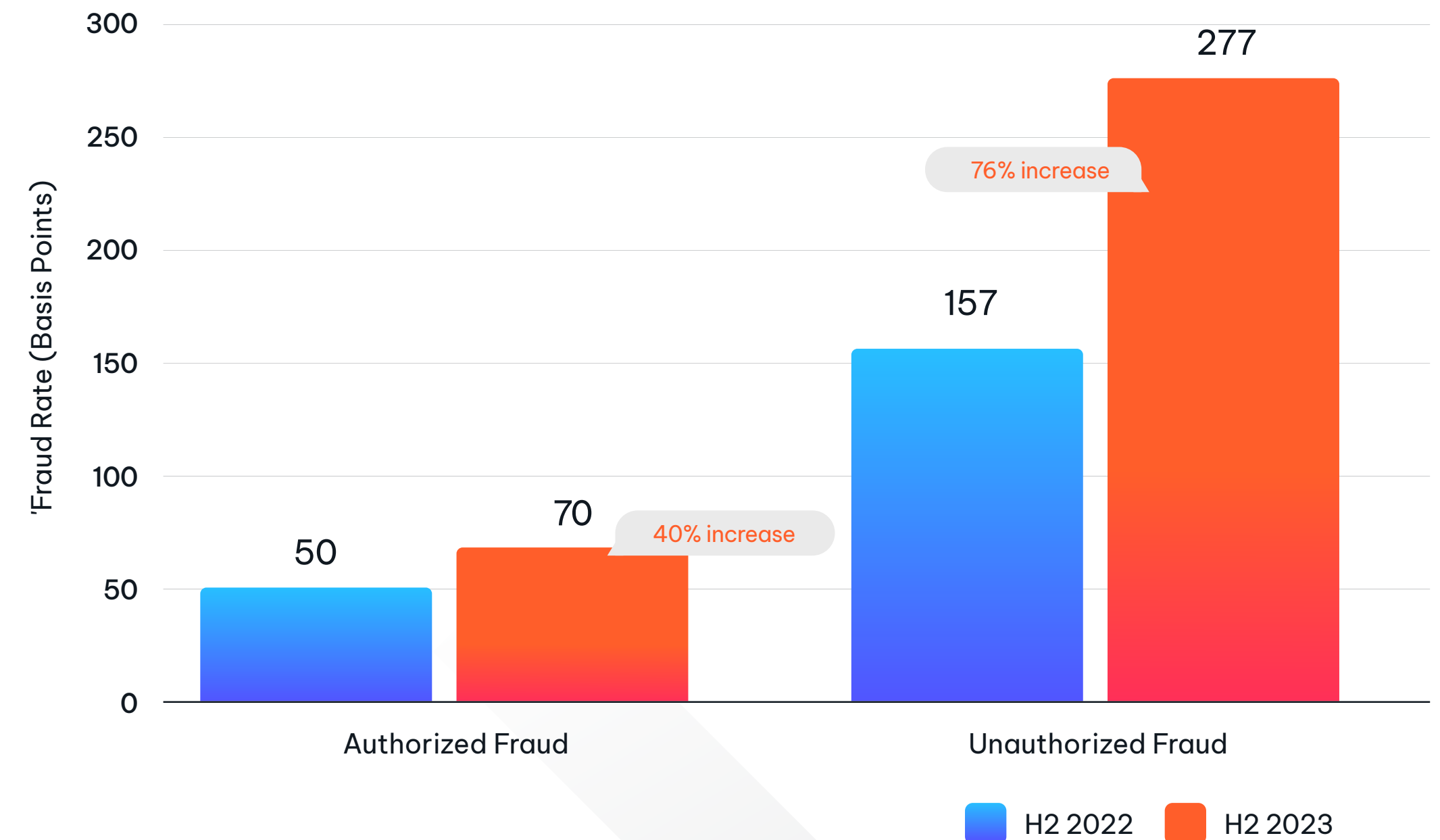
Domestic wire fraud volume increased nearly 34%, almost five times more than the fraud growth rate by value (+7%), reflecting a decrease in average values.



It's not just domestic payment rails that are getting faster. SWIFT is linking up domestic rails internationally, which brings faster payments cross border, with over 50% of SWIFT GPI traffic crediting beneficiaries within 30 minutes⁷.

NICE Actimize Industry Insights H2 2022 vs H2 2023

Fraud Typology Fraud Rate - International



Now is the Time for Fraud Solutions to Evolve

In today's digital age, financial institutions face a relentless surge of fraud threats that require sophisticated, agile prevention. NICE Actimize harnesses AI and the latest technologies to provide comprehensive fraud prevention and management, with its solutions Integrated Fraud Management (IFM) and Xceed. By leveraging advanced AI for real-time detection, decisioning, and continuous adaptation, you can ensure fraud is identified fast and mitigated.

With intelligent data orchestration and industry-wide collective intelligence, NICE Actimize provides a robust defense against evolving fraud tactics, safeguarding both institutions and customers. Transitioning to NICE Actimize means implementing a proactive, scalable, and adaptive solution that enhances detection capabilities, ensures compliance, and ultimately secures your institution's ecosystem from bad actors.

[Explore Enterprise Solutions](#)

[Discover SMB Solutions](#)

References

- ¹ FBI: [Internet Crime Report 2023](#)
- ² PSR: [PSR Confirms New Requirements for APP Fraud Reimbursement \(2023\)](#)
- ³ PR Newswire: [Zelle soars with \\$806 billion transaction volume, up 28% from prior year \(2023\)](#)
- ⁴ The Clearing House: [Real-Time Payments for All Financial Institutions \(2023\)](#)
- ⁵ Pay.UK: [Annual Summary of Payment Statistics 2023 \(2023\)](#)
- ⁶ European Commission: [Proposal for new mandate \(2022\)](#)
- ⁷ Finextra: [Swift Connects Instant Payments Systems to Bring 24/7 Processing Across Borders \(2023\)](#)

2024
FRAUD
INSIGHTS
FIRST EDITION

info@niceactimize.com
niceactimize.com/blog
[X @NICE_actimize](#)
[/company/actimize](#)
[NICEactimize](#)

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.

© 2024 All rights reserved.

Find us at www.niceactimize.com, [@NICE_Actimize](#) or Nasdaq: NICE.