NICE Actimize

DELVING DEEPER:

2023 FRAUD INSIGHTS

SECOND EDITION

Revisiting Fraud Challenges in 2023

Thank you for taking the time to read this addendum to the 2023 Fraud Insights Report. We revisited our findings from earlier this year and analyzed new trends to watch out for in 2024. At NICE Actimize, our team of fraud experts remains dedicated to closely monitoring global developments in fraud, scams, and the ever-evolving landscape of digital payments. This report delves into the ongoing trends and challenges that are tackled by industry practitioners.

Recent fraud trends are following the theme of history repeating itself, especially when considering threats related to customer onboarding and first-party fraud. In parallel, newer threats over digital channels are amplified by fraudsters developing complex new scams, recruiting money mules, and perfecting attack tactics.

The speed, ease, and varieties of scams gaining traction signal the immediate need for financial institutions to take action with next-gen technology.

This latest report focuses on FIs that combine payments innovation with a proactive approach to fraud prevention. As we reported earlier this year, across the industry, there has been measurable improvement in addressing fraud risk. However, there's a long road ahead given the sophistication of today's fraud threats.

The scale of fraud attacks along with new mandatory regulatory requirements has forced FIs to expand fraud prevention into other areas for improvement. Changes in regulation, particularly with fraud liability shifts, are top of mind—especially in the space of scams and APP fraud.

Sophisticated fraudsters persist in deploying widespread tactics that exploit individuals of all ages, demographics, and communication channels. These perpetrators target potential victims through various means, including text messages, phone calls, emails, and social media interactions. FIs that embrace a modernized strategy incorporating machine learning and AI will not only bolster their defenses, but also enhance customer retention. This ensures a stronger and more resilient position in the face of these evolving threats.

Successfully combating new fraud threats takes a multi-disciplinary and holistic approach, but also requires cross-industry collaboration. Globally and regionally, our analysis underscores how important it is for the industry to come together and collaborate with each other and law enforcement, so that we can all be stronger in the fight against fraud.

As cooperation grows within the industry, collective intelligence and innovation will be vital so FIs can protect both their organizations and customers.

To that end, use these expert insights to strengthen your fraud prevention strategy and safeguard your organization in 2024.

Yuval Marco
General Manager, Enterprise Fraud Management,
NICE Actimize

H1 2022 v. H1 2023 – Retail Fraud Continues to Rise

Overall, there continues to be an increase in the level of payment volume and fraud attacks in the first half of 2023. Globally, both fraud units and fraudulent dollar attempts have increased. Total payment volume is up 22% when compared to H1 2022. Additionally, both the value of these payments and fraud value has increased by 18%.

Global Problem Areas of Interest:

Largest Increase in Unit Attempts:
International Payments

Largest Increase in Attempted Dollars:
International Payments and Deposits

FIs Need Stricter Fraud Controls on Outbound International Payments

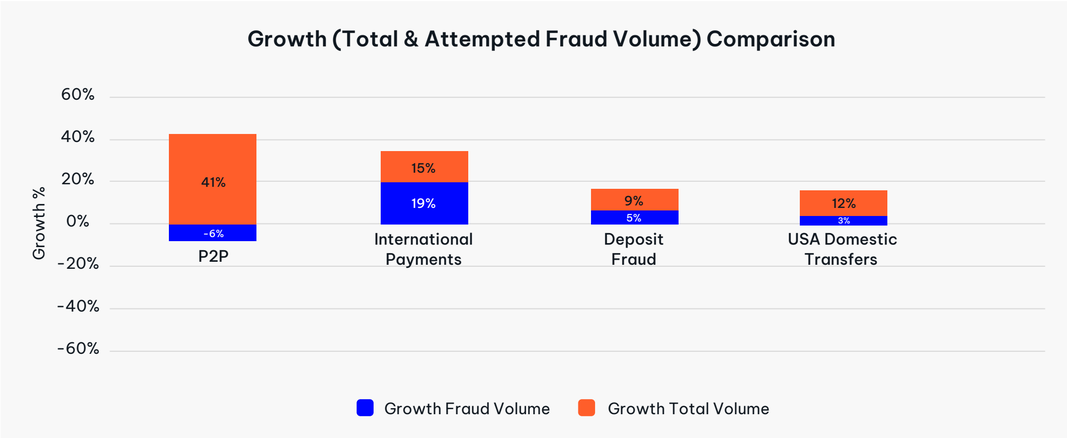
The traditional nature of international payments (high value, but lower volumes) makes any increase in attempted fraud volume within this channel particularly concerning. The attempted fraud rate for international payments increased 31% in H1 2023.

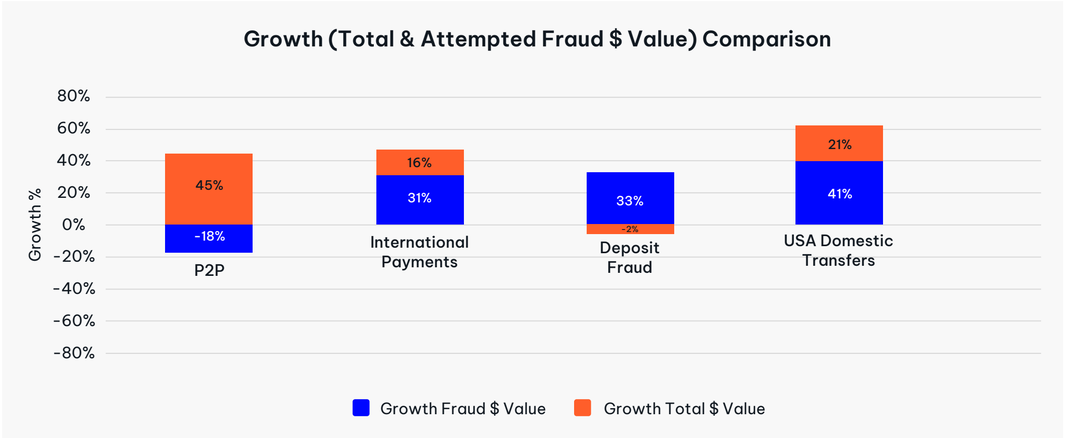
Deposits and Check Fraud Under Continued Attack

In the U.S., fraudsters continue to attack transfers and deposits. NICE Actimize trend data shows a continued uptick in fraudulent events in this space by 5%.

As expected, with the adoption of more modern payment methods, check deposits, by value, are down 2% year-over-year. The paradox is that while total deposits are down, the percentage of fraud dollars on those deposits is up a staggering 33%.

Fraudsters continue to focus on weaknesses in check in-clearing controls, particularly in the U.S. This is due, in part, to legacy fraud risk management solutions for check in-clearing and the long timeframes that can occur ahead of the receipt of check returns.



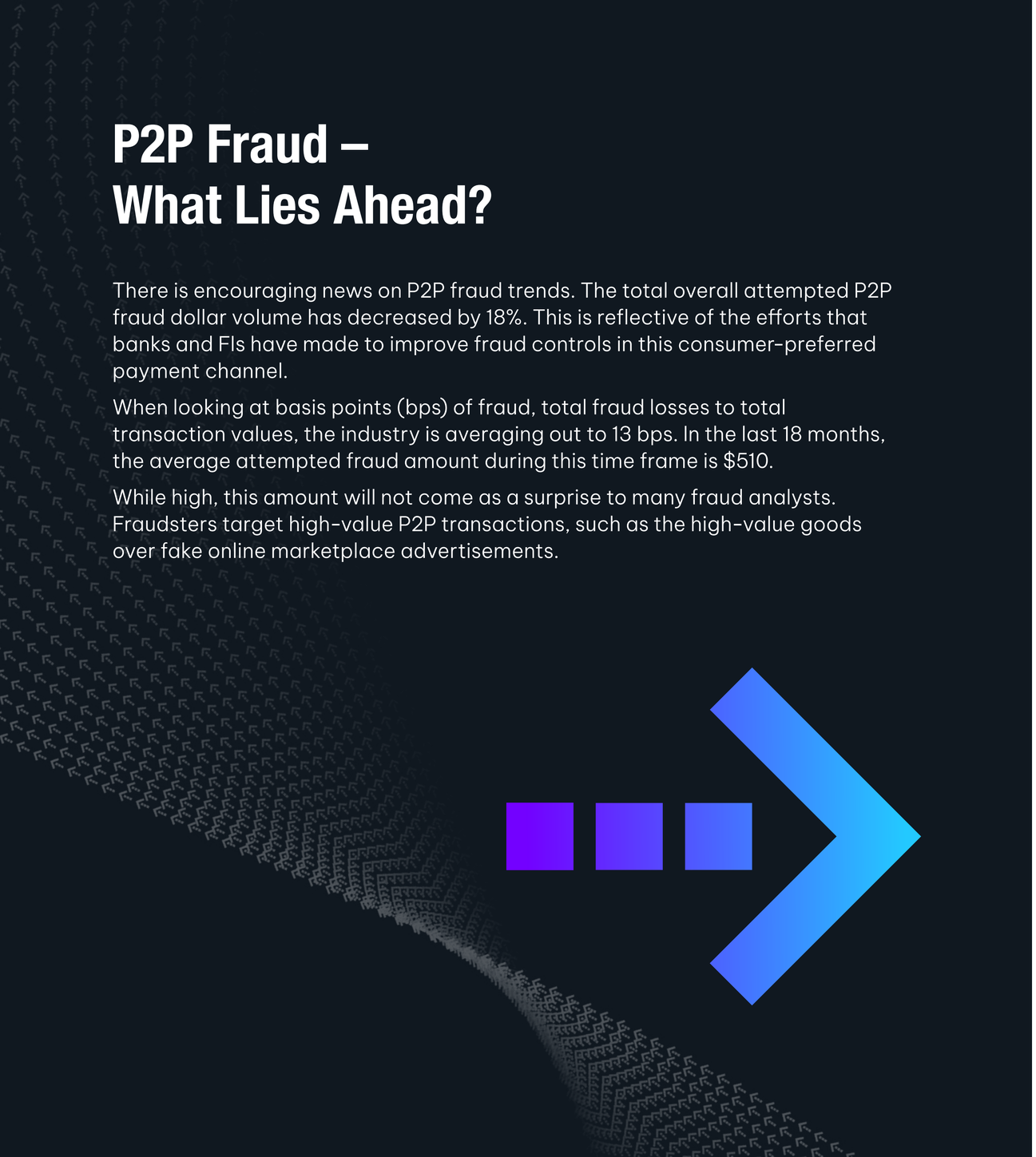


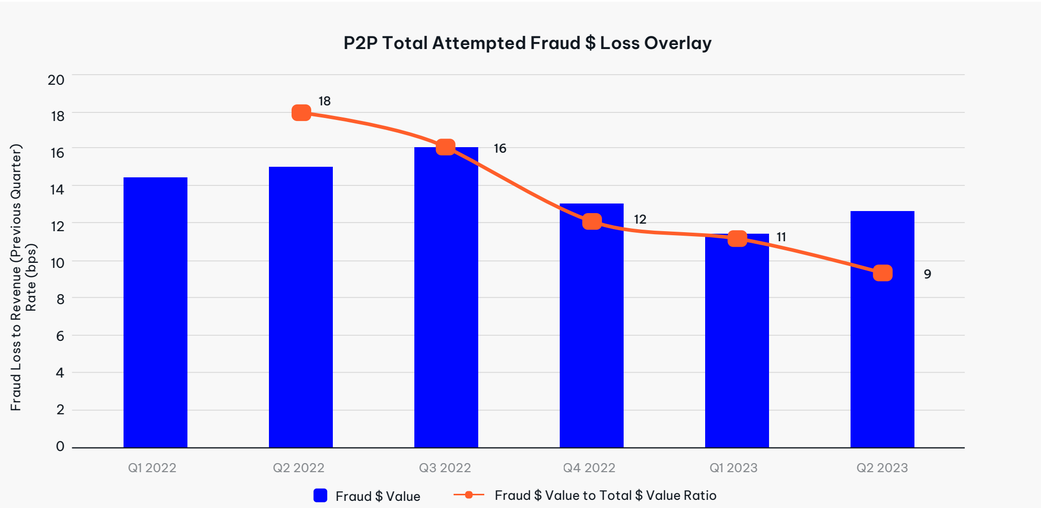
P2P Fraud – What Lies Ahead?

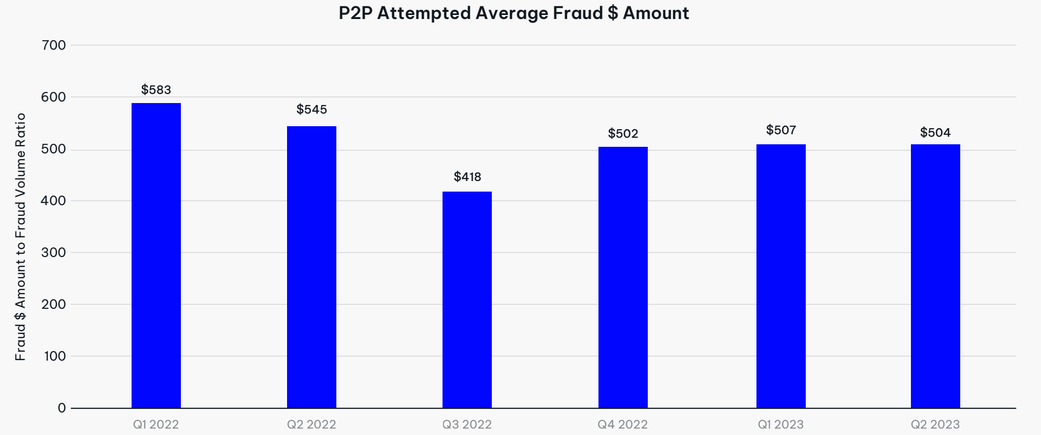
There is encouraging news on P2P fraud trends. The total overall attempted P2P fraud dollar volume has decreased by 18%. This is reflective of the efforts that banks and FIs have made to improve fraud controls in this consumer-preferred payment channel.

When looking at basis points (bps) of fraud, total fraud losses to total transaction values, the industry is averaging out to 13 bps. In the last 18 months, the average attempted fraud amount during this time frame is $510.

While high, this amount will not come as a surprise to many fraud analysts. Fraudsters target high-value P2P transactions, such as the high-value goods over fake online marketplace advertisements.





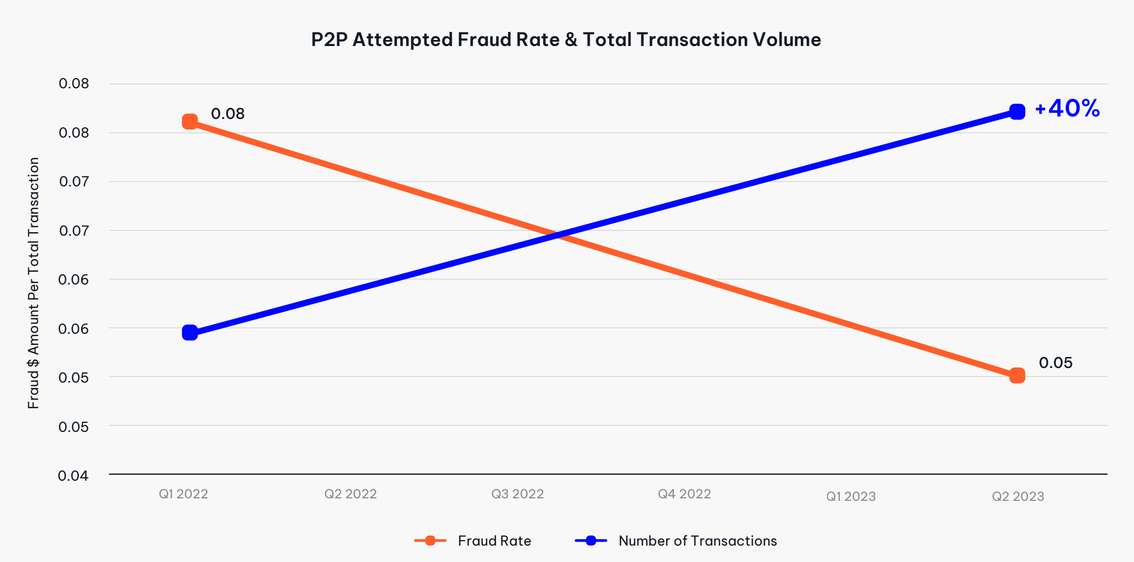


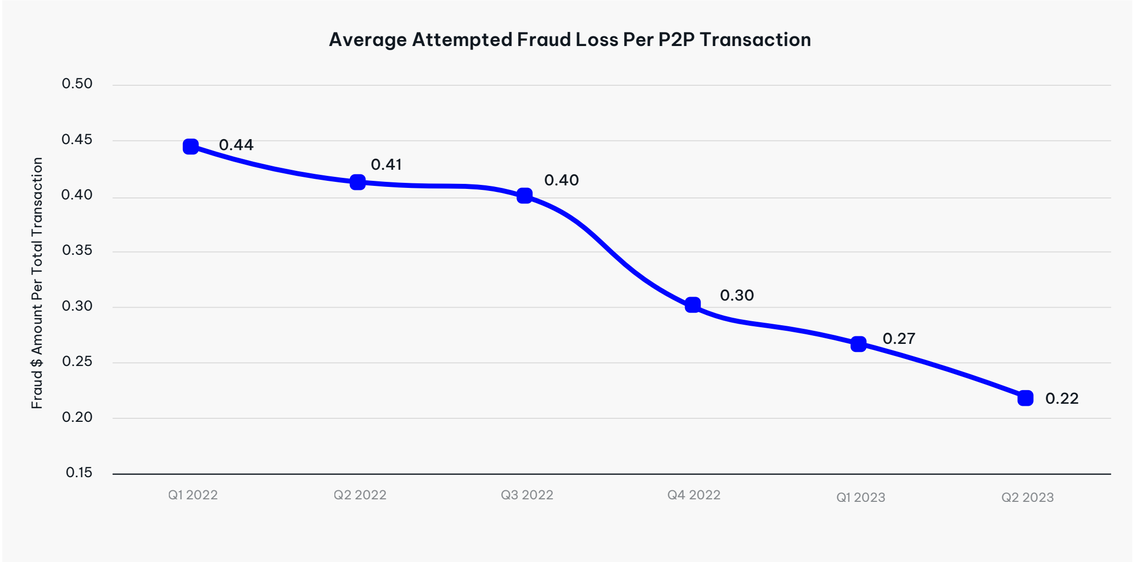
Focus on P2P Fraud – Transaction Volume Up

The average attempted fraud dollar amount per P2P transaction has notably decreased when comparing the entirety of 2022 to the first half of 2023. This decline in attempted fraud aligns with the substantial rise in total transaction volumes within this channel, indicating explosive adoption of digital payments.

Notably, the average attempted fraud rate for P2P transactions exhibited a substantial decrease of 38% when comparing the first half of 2022 to the first half of 2023. Despite this decrease in fraud rate, the total transaction volume surged by 40%, while the actual volume of attempted fraud experienced a more **modest decline of only 6%.**

These observations indicate that real-time fraud controls are working



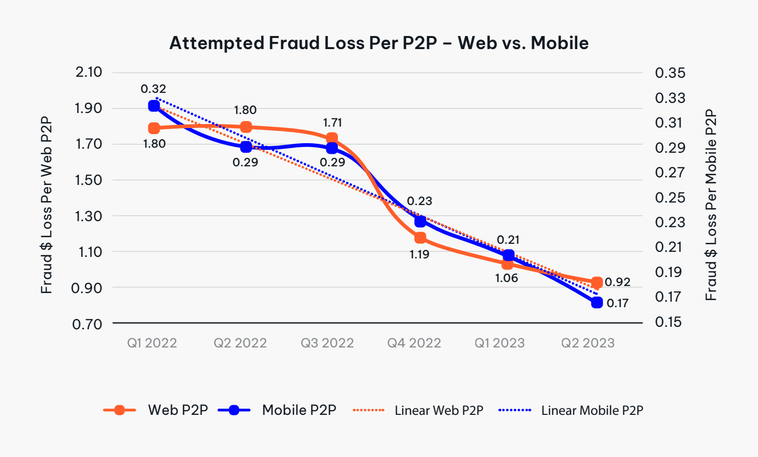


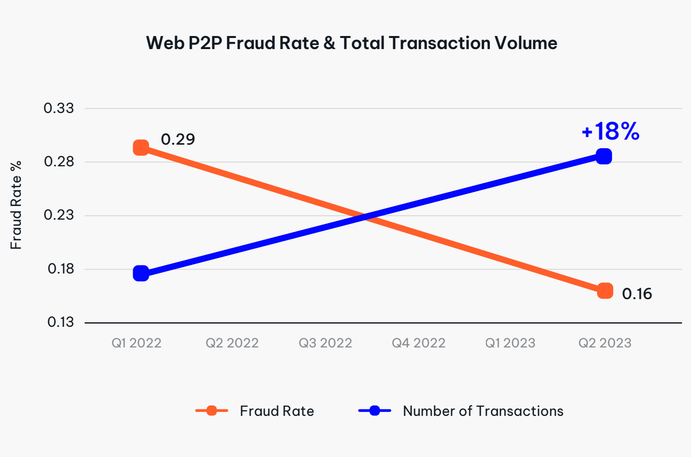
Focus on P2P Fraud – Web vs. Mobile

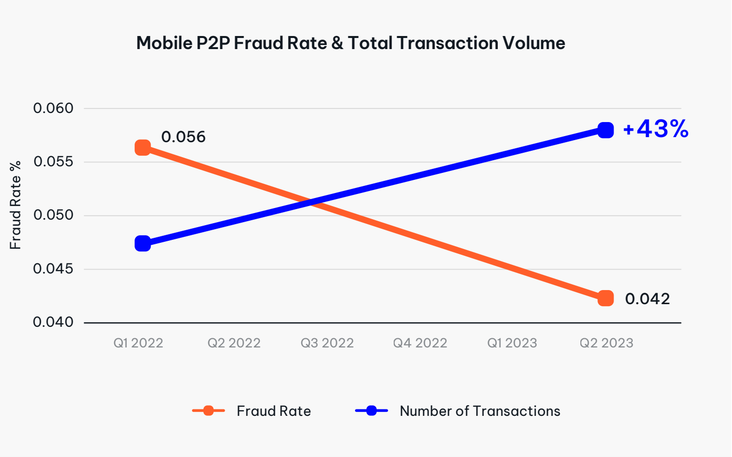
Consumer adoption of P2P payment applications, whether through online platforms or mobile apps, continues its upward trajectory. Within the P2P channel, transactions initiated over the web are identified as the riskiest. In 2023, increased transaction volumes and incremental controls have led to a reduction in the fraud rate for web-based P2P transactions, although it remains four times riskier compared to mobile-based P2P transactions.

When evaluating the potential loss due to attempted fraud in both mobile-based P2P and web-based P2P channels, significant decreases have been observed since Q1 2022. While attempted fraud loss appears to be on a declining trend, it's essential to note that web-based P2P transactions remain four times riskier than their mobile-based P2P counterparts as of the end of Q2 2023.

While there appears to be a downward trend on P2P fraud, fraudsters are leveraging P2P for scams.



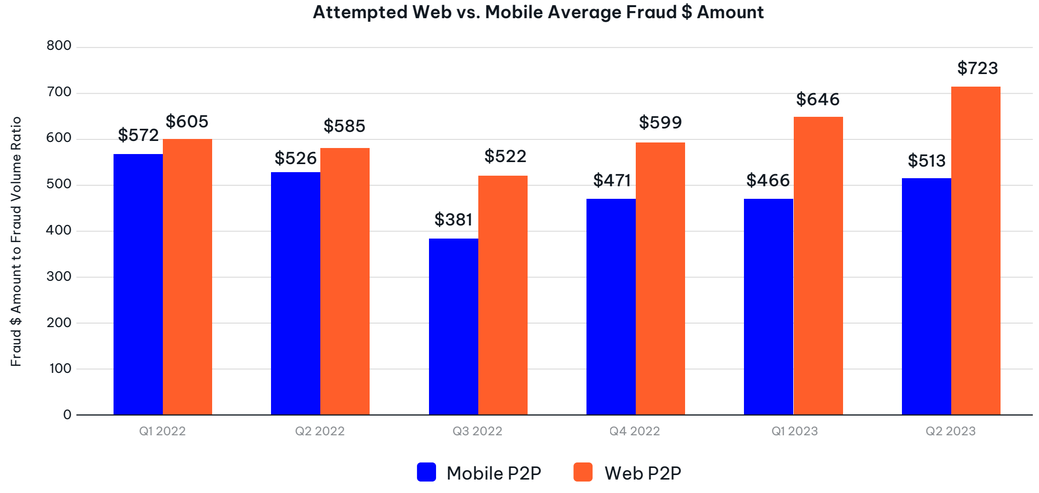


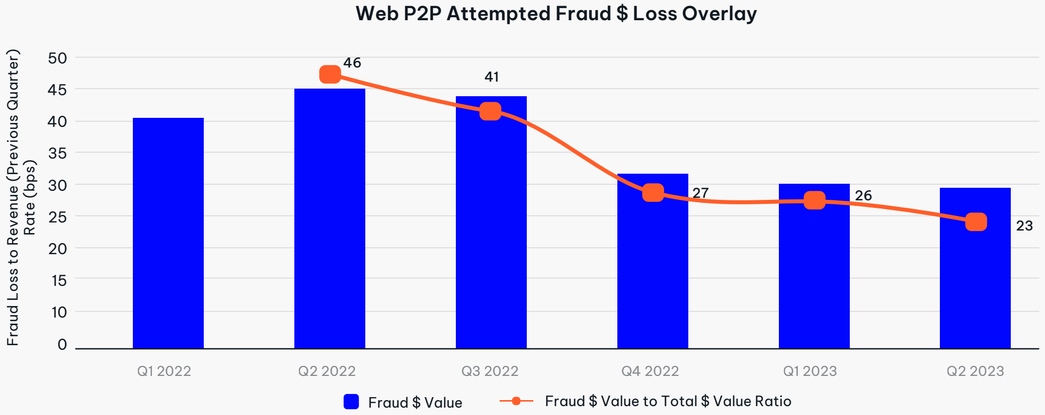


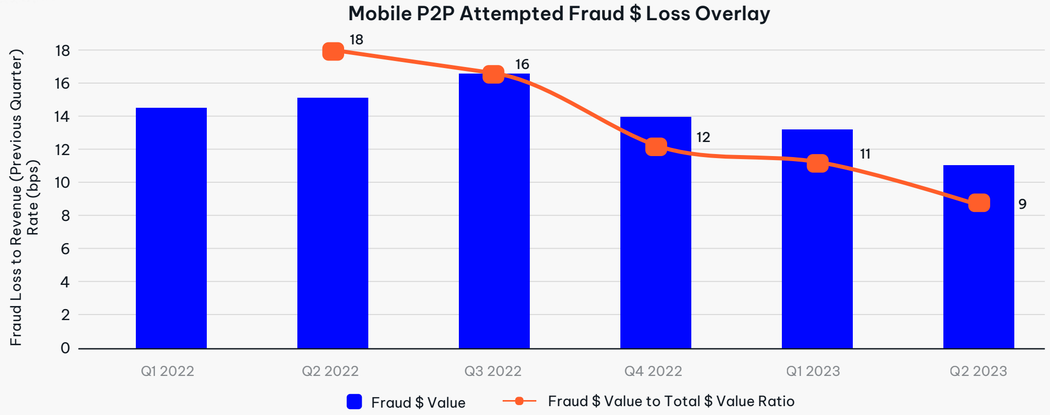
P2P Fraud – Web vs. Mobile Sending Transactions

The rate of average attempted fraud dollars to total dollars in mobile P2P transactions stands at 10 bps. In stark contrast, web-based P2P transactions exhibit a considerably higher rate of 33 bps, exceeding mobile P2P by over 300%.

Notably, the average fraud dollar amount in web P2P transactions saw a 20% increase from Q1 2022 to Q2 2023. Furthermore, the average fraud dollar value for web-based P2P transactions, at $613, surpasses mobile P2P transactions, which stands at $488. This represents a 26% difference between the two. Mobile Authorized Push Payment (APP) P2P transactions are far more secure than other channels.



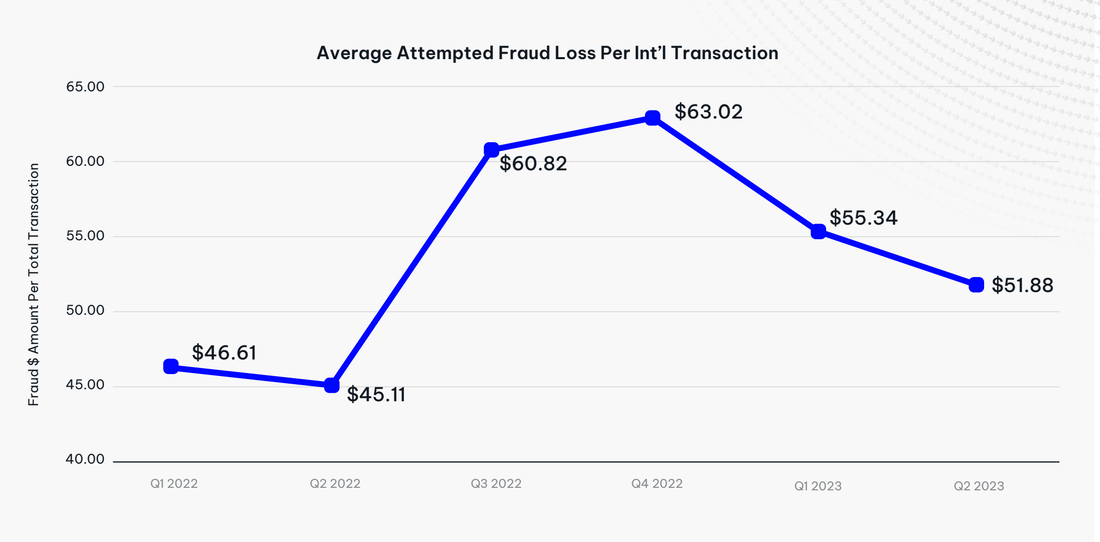




Attempted Fraud Share Per International Transaction

When examining the cumulative impact of international transactions and the corresponding fraud expenses, the figures are astonishing. The attempted fraud loss per individual international transaction grew from $47 in Q1 2022 to $52 in Q2 2023, resulting in an average fraud loss of $54 per international transaction spanning from January 2022 to June 2023.

FIs need to factor in a portion of fraud loss per every legitimate transaction. Currently, the average fraud cost per international transaction is $54.



In the fourth quarter of 2022, there was a notable surge in attempted fraud rates relative to the overall transaction volume. However, this trend has subsequently reversed and is declining.

The FBI's Internet Crime Complaint Center (IC3) noted increases for Business Email Compromise going back to 2020 of $1.8 billion to over $2.7 billion in 2022. The increases in attempted fraud loss per individual international transaction reflect these increases.

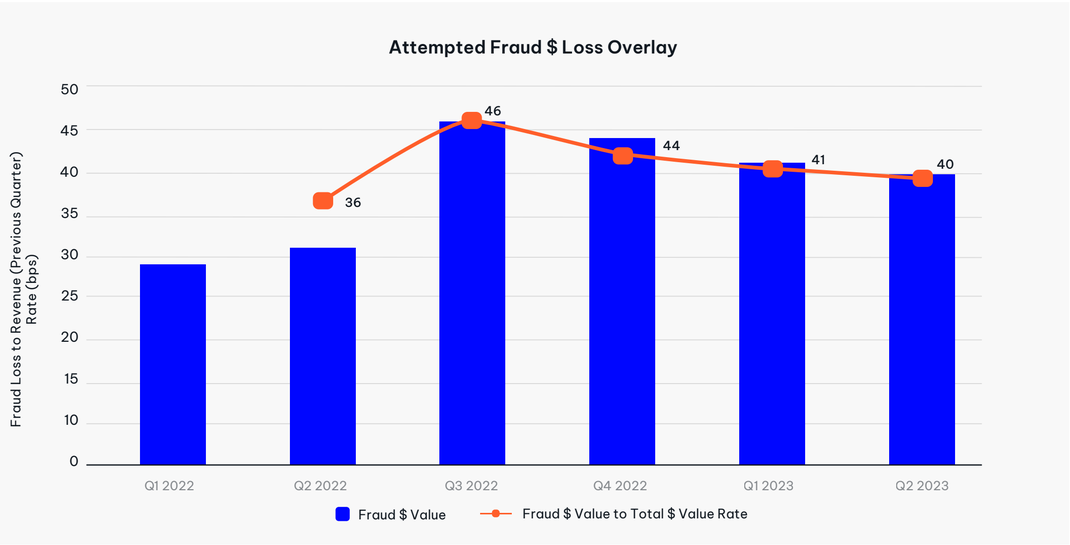
FIs must focus on uncovering trends within risky cross-border payments

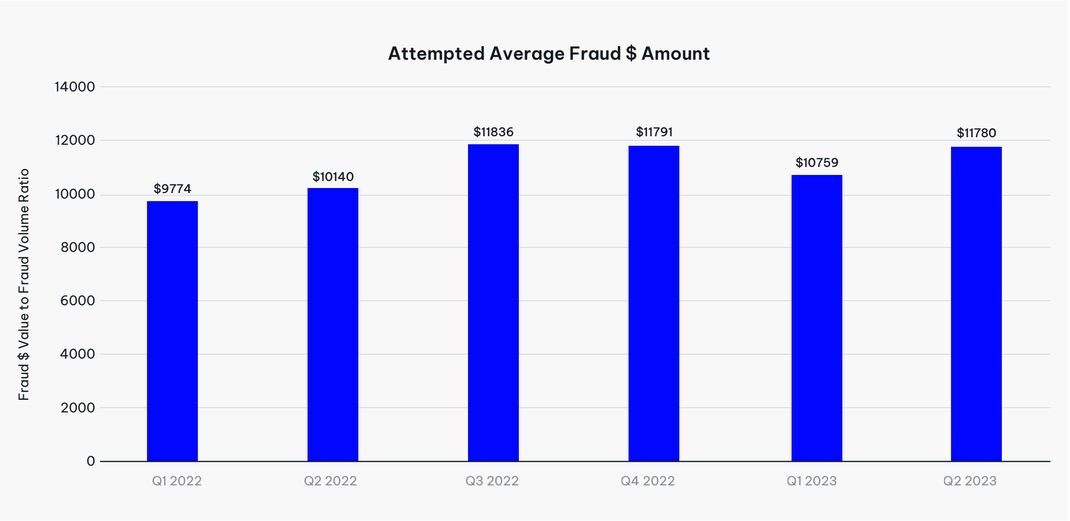
Attempted Fraud Dollar Loss & Average Fraud Dollar Amount - International Transactions

The attempted fraud dollar value associated with international transactions has surged by a significant 31%. Since September 2022, the ratio of attempted fraud dollar value in the current month to the total dollar value in the previous month has remained relatively stable when considering the linear trend.

Over the period from January 2022 to June 2023, the average ratio of attempted fraud dollar loss to revenue for international transactions stands at 40 bps.

During the span of January 2022 to June 2023, the average attempted fraud dollar amount for international transactions stands close to $12,000 USD.





Shift to Fraud Typology Prevention

This analysis was based on actively monitoring various fraud typologies, including New Account Fraud, Unauthorized Payment Fraud (commonly referred to as Account Takeover or 'ATO'), and Authorized Payment Fraud (often termed 'Authorized Push Payment' or APP fraud). One typology worth specific mention is the 'Aged Fraudulent Payee Accounts.'

The concept of 'Aged Fraudulent Payee Accounts' (payee) was introduced within the Actimize taxonomy for scams and fraud, with a direct comparison to payor accounts that are also aged. These aged fraudulent payee accounts can be the direct recipients of scam proceeds or used to support the means of other traditional money laundering activities. Due to the age of these fraudulent payee accounts, it enables detecting and mitigating money mule risk by recognizing atypical behavior in an aged fraudulent payee account.

Anecdotally, there are examples of ATO being used to recruit unwitting mules. In this case, the true account holders are unaware of mule activity unless they notice either the ATO of their own payor account, or the deposit and 'pass-through' if the consumer's account is the payee.

The significance of this typology shift is noteworthy. While the proportion of Unauthorized fraud transactions hasn't substantially increased, there has been a 5% uptick in the share of fraud dollars comparing year over year. However, it's encouraging to report an 11% decrease in the Unauthorized fraud rate.

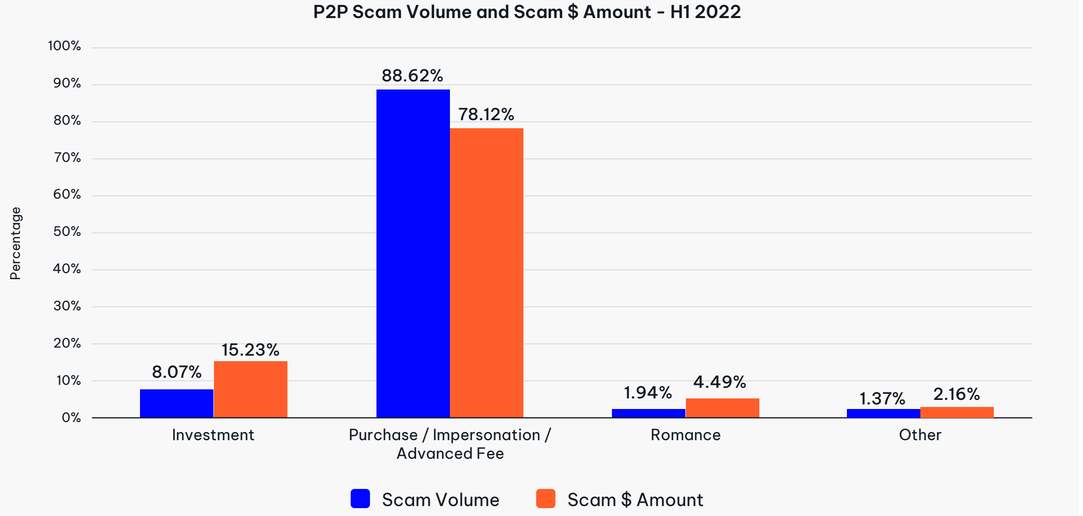
In our previous **Fraud Insights Report**, we highlighted a noticeable increase in Authorized fraud transactions, with a marginal increase in the associated fraud dollar amount. There's a notable shift in fraud volumes from Unauthorized to Authorized fraud (scams). However, in terms of fraud dollar share, Unauthorized fraud has increased twice as much as Authorized fraud.

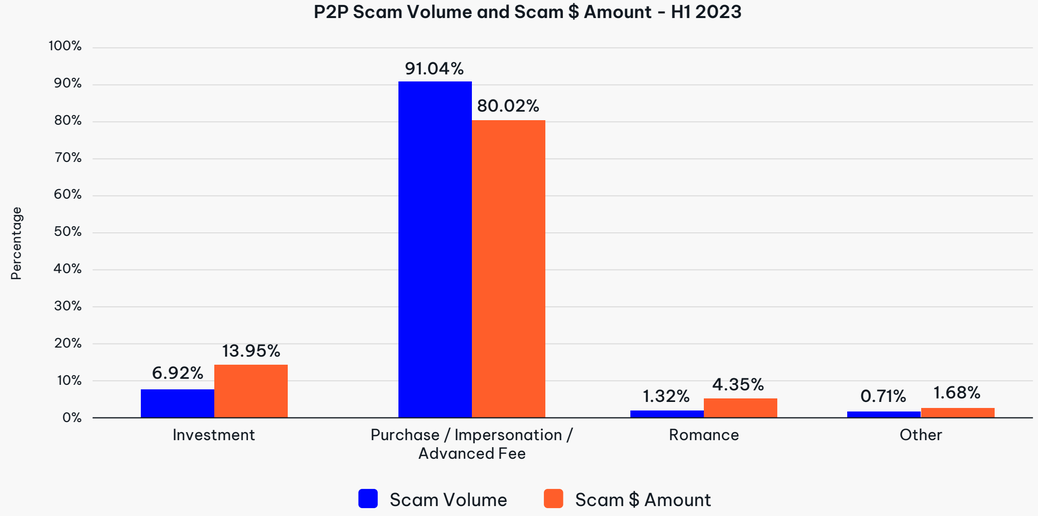
While the number of events is down, when fraud happens the losses are significantly higher. Targeted efforts with higher gains.

Authorized Payment Fraud Scam Typologies in Focus – P2P Fraud

As the lure for cryptocurrencies and get-rich-quick schemes quieted down, so have the number of scam related events. Correspondingly, there's been a decline in investment scams, commonly known as 'pig butchering' within the cryptocurrency domain.

This shift in trends contrasts with the increasing prevalence of purchase, impersonation, and advanced fee scams. This phenomenon lends credence to the hypothesis that fraudsters are redirecting their attention toward shorter-term, lower-value scams. Notably, this shift is pronounced in purchase and impersonation scams originating from social media platforms where growth is unchecked.





Payment Fraud Typologies in Focus – International Transactions

There's evidence of fraudsters shifting their focus from longer-term scams, such as romance and investment fraud, to shorter-term schemes, particularly in the realm of purchase-related scams. This is further supported by a broader transition from scam and mule-related fraud in established accounts to Unauthorized and Authorized payment fraud.

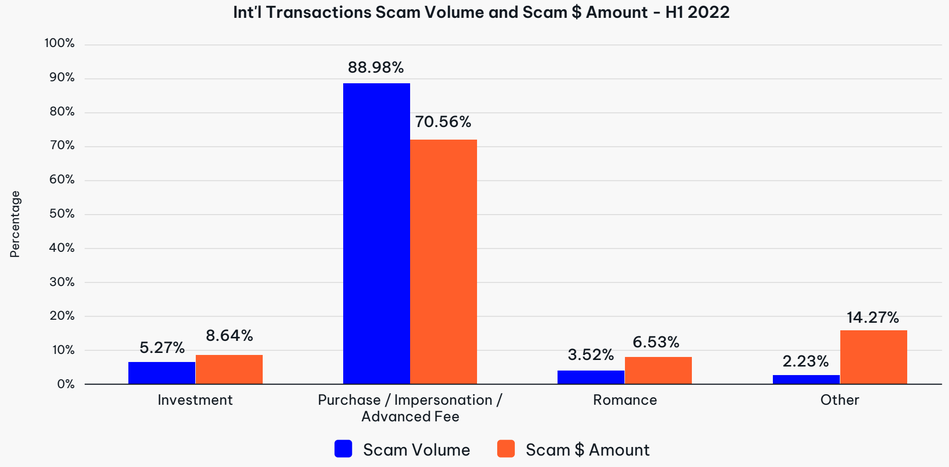
In the case of **Unauthorized payment fraud**, there's a noteworthy surge in the fraud dollar value, indicating an overall uptick in the monetary impact of these fraudulent activities. **The 35% increase** in the fraud rate for Unauthorized payment (ATO) fraud in **international transactions** serves as a clear signal, underlining the urgency for renewed emphasis and investments in fraud prevention where "old becomes new."

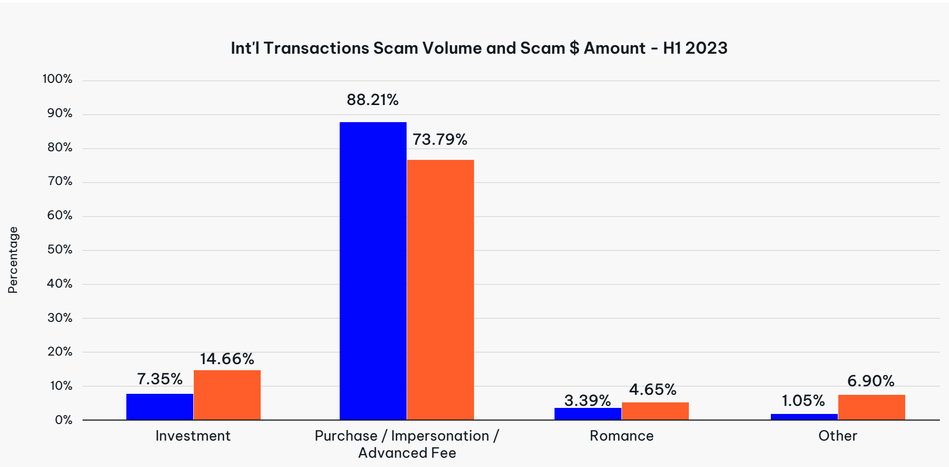
35% Increase

ATO With International Transactions

Authorized payment fraud (Scams), a prominent typology, continues with higher-than-average fraud amounts while maintaining relative number of events when comparing the first half of 2022 to the same period in 2023. Purchase/Impersonation Scam losses are up 3% compared to 2022.

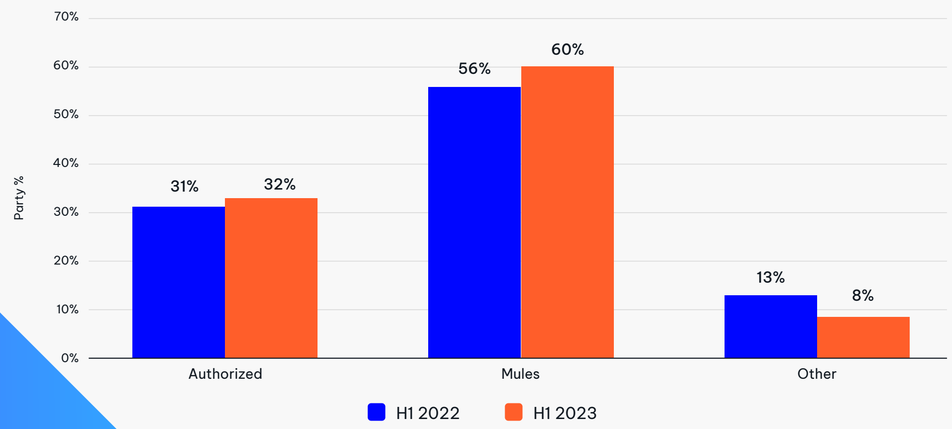
Scam Losses are Up



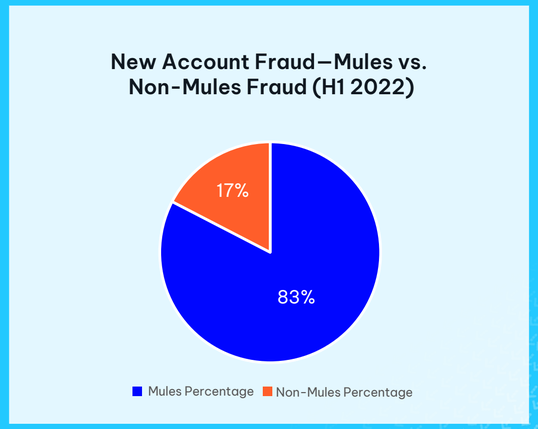


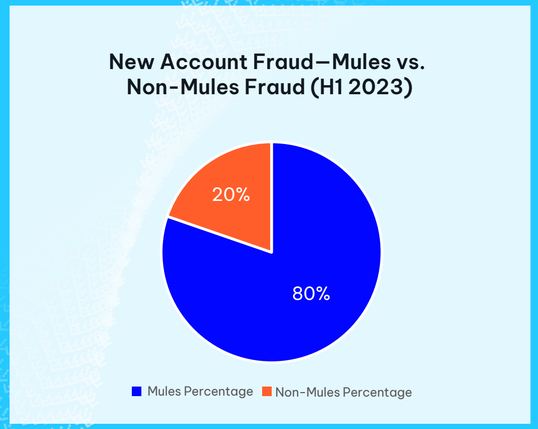
Breakdown of Aged Payor Accounts Interacting with an Aged Fraudulent Payee Account – International

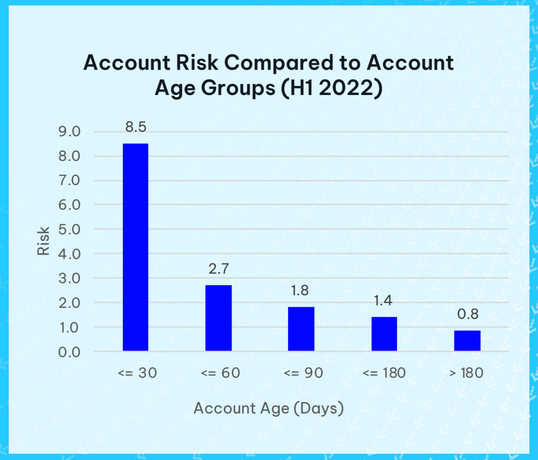
In the realm of international transactions, fraud using money mules outpaces what was observed in real-time transactions, accounting for a significant 60% of the total. This reinforces the importance of identifying and disrupting money mule activity, which is not only a ‘kill chain’ consideration for scams over real-time payments, but also for scams that use international transactions.

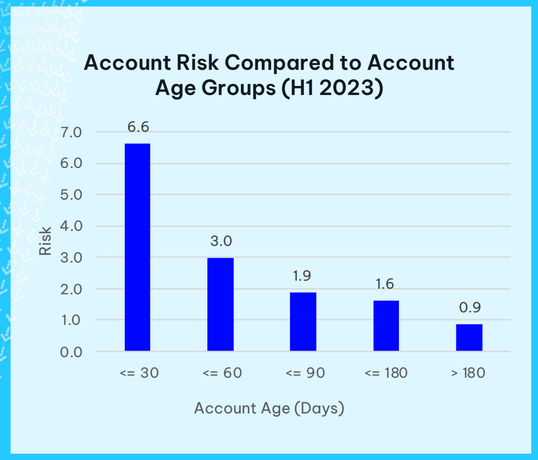


Money Muling Risk Insights By Composition and Account Age - P2P

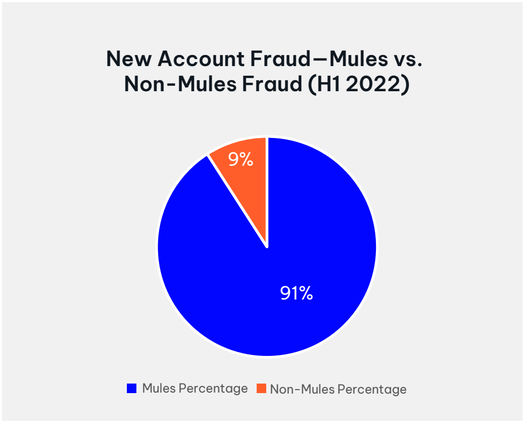


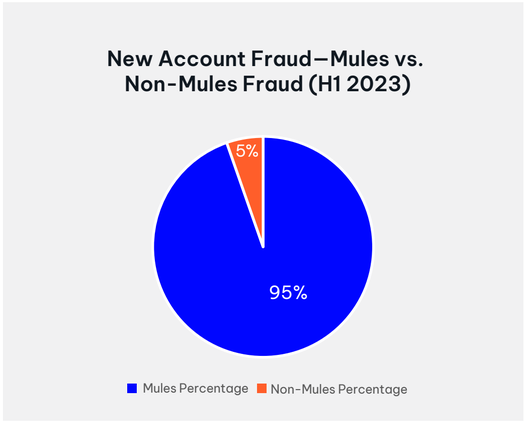


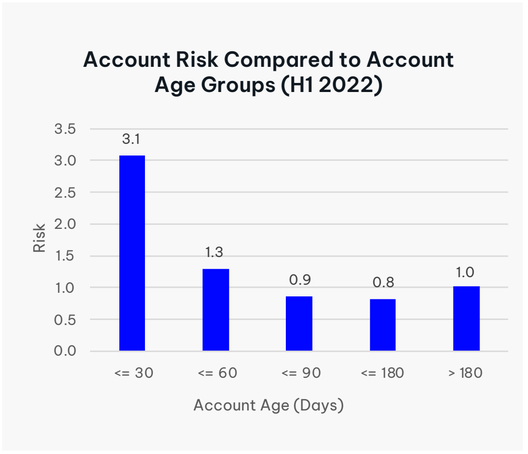


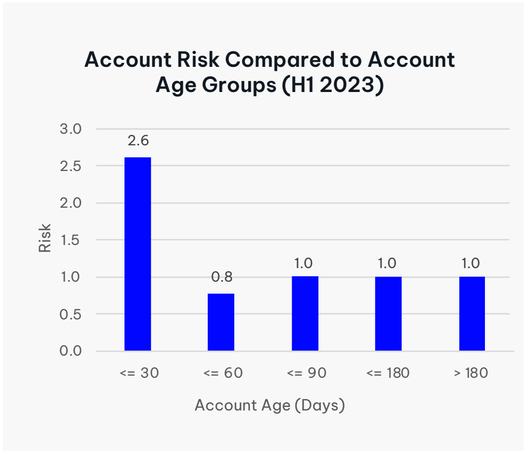


Money Muling Risk Insights By Composition and Account Age - International









3 Takeaways & Recommendations

Three Critical Insights:

1. Faster and real-time payments have gained widespread adoption; FIs must embrace real-time payments monitoring for both domestic and international transactions
2. Fraudsters attack customers directly, so FIs must prioritize the implementation of strategies to combat scams and prevent Authorized (APP) fraud
3. As fraudsters increasingly target long-standing accounts for both Authorized and Unauthorized schemes, FIs should explore strategies and models that consider various customer segments and their historical engagement

FIs are under mounting pressure due to the surge in fraud attacks, rising transaction volumes, and the ever-evolving landscape of regulatory and consumer liability requirements.

Year-over-year increases of 22% in payment volume and 18% in both attempted dollar and unit attack rates are simply unsustainable.

In order to combat looming threats, FIs need to evaluate current fraud execution practices.

NICE Actimize

Execution advancements need to be centered around three key areas to combat fraud:

1. **Implement next-gen fraud prevention** (real time, automated, AI/ML) to respond faster to threats
2. **Modernize fraud analytics** with intent based typology-centric detection, and data enrichment that leverages advanced tech to achieve increased detection and reduced false positives
3. **Harness the cloud** for its scalability, network analytics, and lower operational costs, to achieve consistent, good results

NICE Actimize

DELVING DEEPER:
2023 FRAUD INSIGHTS
SECOND EDITION

Address today's fraud challenges with NICE Actimize

Discover more here

info@niceactimize.com
niceactimize.com/blog
@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.

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