NICE Actimize

2022 NICE Actimize Fraud Insights Report

Welcome

Financial fraud prevention is dramatically evolving thanks to technological advancements. One of the fundamental shifts is in the transition from relying solely on fraud expertise to combining data-driven fraud strategy, such as machine learning, with deep fraud understanding.

As data-driven insights are critical to successful fraud prevention, you can leverage the financial fraud intelligence we gathered and analyzed from the collective industry to effectively combat new fraud and financial crimes. Our mission at NICE Actimize is to deliver these expert insights to the market to achieve our shared purpose—protecting financial institutions and their customers from fraud threats.

Definitive fraud trends and developments shaped the 2021 threat landscape. This report details the essential insights we've uncovered, including the impact of digital acceleration on fraud and the high-risk attributes associated with new threats that emerged during the year.

Together, we can stop fraud in its tracks.

Yuval Marco

General Manager
Enterprise Fraud Management

YEAR IN REVIEW

FASTER PAYMENTS IS LEADING IN PAYMENTS FRAUD

- P2P
- New and Emerging Payments
- eWallets

DIGITAL ACCELERATION AND THE IMPACT OF MOBILE DEVICES

- Device Type
- OS Version
- Geolocation
- Jail Broken

HIGH RISK ATTRIBUTES ASSOCIATED WITH BEHAVIOR AND LOCATION

- Transaction & Behavioral Attributes
- Login Changes
- Location/ Destination

Fraud ON THE RISE

+41% ATTEMPTED FRAUD RATE

P2P

+38%
Transaction volume

+63%
Attempted fraud dollar value

For the Fraud Fighter: Fraudsters use SIM swaps, malicious VPNs, social engineering and other tools to perpetrate account takeover (ATO) and scams. Advanced analytics help financial services organizations (FSOs) distinguish between normal and anomalous customer behavior—allowing them to quickly stop fraud before it happens.

CHECKS

+8%
Transaction volume

+106%
Attempted fraud dollar value

For the Fraud Fighter: To combat check fraud, particularly over Remote Deposit Capture (RDC), FSOs need external account verification tools to confirm funds availability and account status, in addition to the information to fight duplicate presentment. Image capture tools must be robust and continually updated to detect altered and/or fictitious items.

CNP BILL PAYMENT

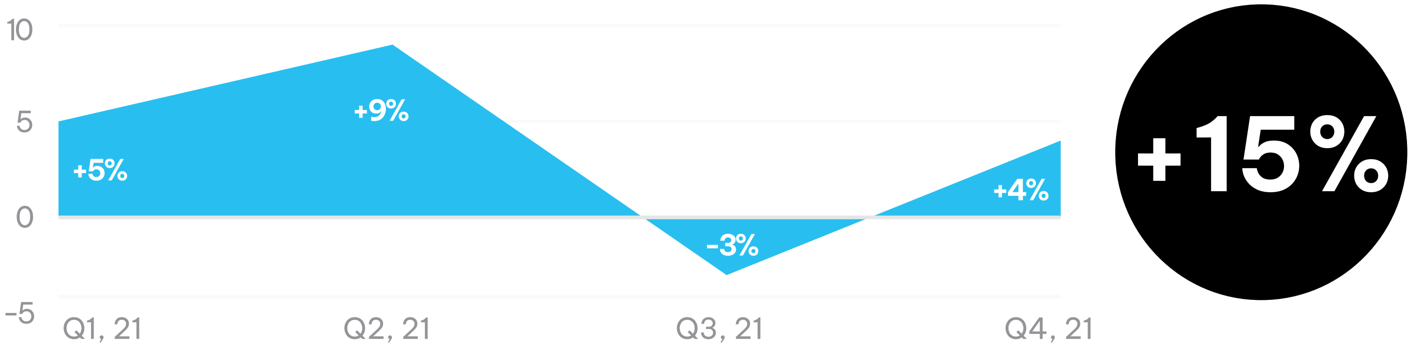
-5%
Transaction volume

+20%
Attempted fraud dollar value

For the Fraud Fighter: Third-party billing services for card-not-present (CNP) transactions are a vehicle for ATO and ID theft because PII, such as a current address, is needed to authorize these transactions. These fraudulent activities can be overlooked as legitimate transactions during an ATO review, and customers often fail to recognize and dispute these transactions early on. If the bill payment is facilitated without card details through a direct transfer, such as ACH, NACHA's Web Debit Account Validation Rule (March 2021) should be considered. Banks will receive additional authorization requests from originators to meet this requirement. Without a means to automate these signals, institutions and customers will likely experience increased bill payments fraud.

ACH Payment Trends

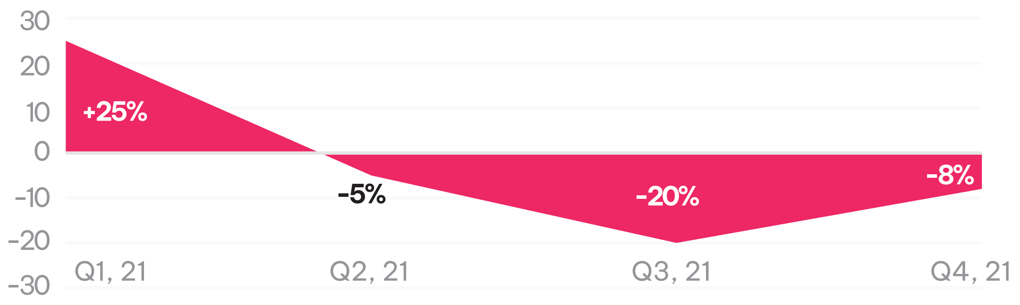
Quarterly Change in COMMERCIAL ach payments



FOR THE FRAUD FIGHTER:

Because there are monetary limits on tellers in banks for issuing checks, more corporations are moving to ACH usage. Using ACH for corporate payments (B2B) gradually increased in volume from the start of 2021. With higher limits in corporate accounts, social engineering scams and business email compromise (BEC) pose greater fraud risk.

Quarterly Change in PPD ACH Payments



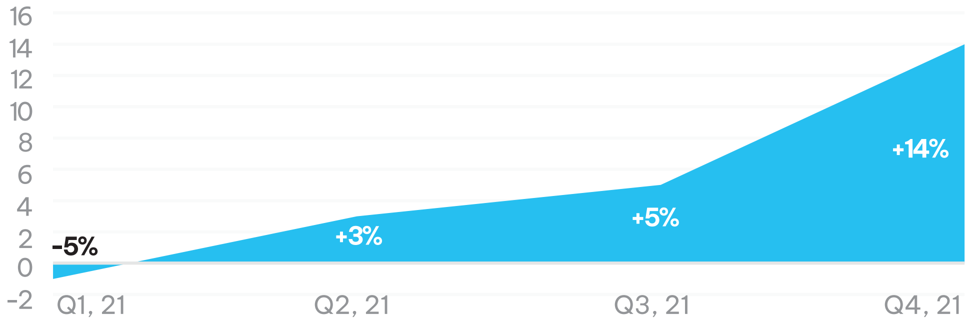
-6%

FOR THE FRAUD FIGHTER:

In Q1 2021, there was a surge in ACH activities in the segment of prearranged payments and deposits (PPD), mainly due to the significant unemployment and other government benefits rollout for U.S. customers. This increase follows reports by central clearinghouses (e.g., NACHA), which raises several fraud concerns. Pandemic-related consumer and employment pressures marked the increase, particularly in insurance claims fraud for worker's compensation, auto insurance, and other benefits.

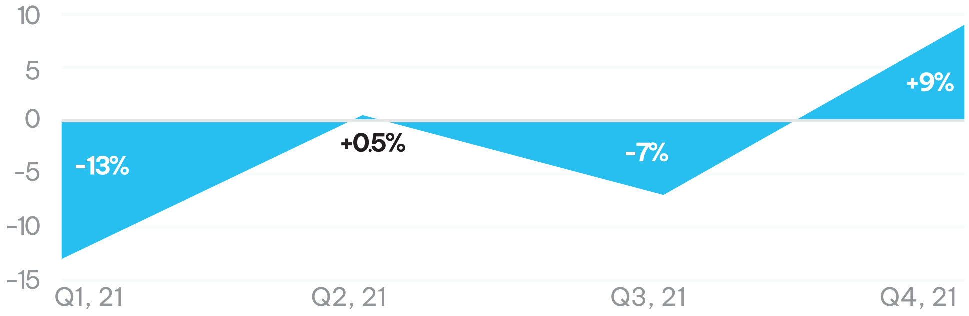
Wire Payment Trends: **Commercial**

Quarterly Change in Online Commercial Wire Transfers



+29%

Quarterly Change in Offline Commercial Wire Transfers



+7%

FOR THE FRAUD FIGHTER:

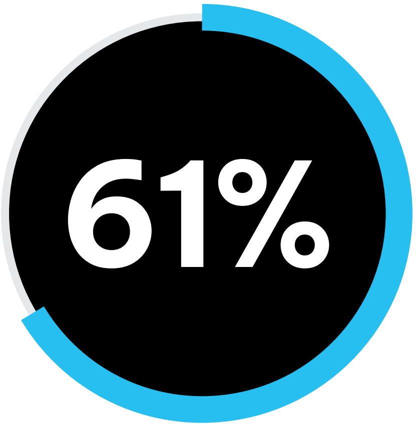
In response to in-person operational challenges due to COVID-19 restrictions, there were varied responses seen from FSOs. Some were able to shift entirely to a virtual model, while others continue to physically staff operations partially, albeit within a context of increased fraud risks.

For wire transfers, our data shows a consumer shift to online channels over traditional offline channels. This is seen in our YoY report, which reveals a gradual increase in wire transfer activities using the web channel.

With this switch from offline to online activities, we expect fraudsters to leverage social engineering to further BEC fraud and ATOs in the web wire segment.

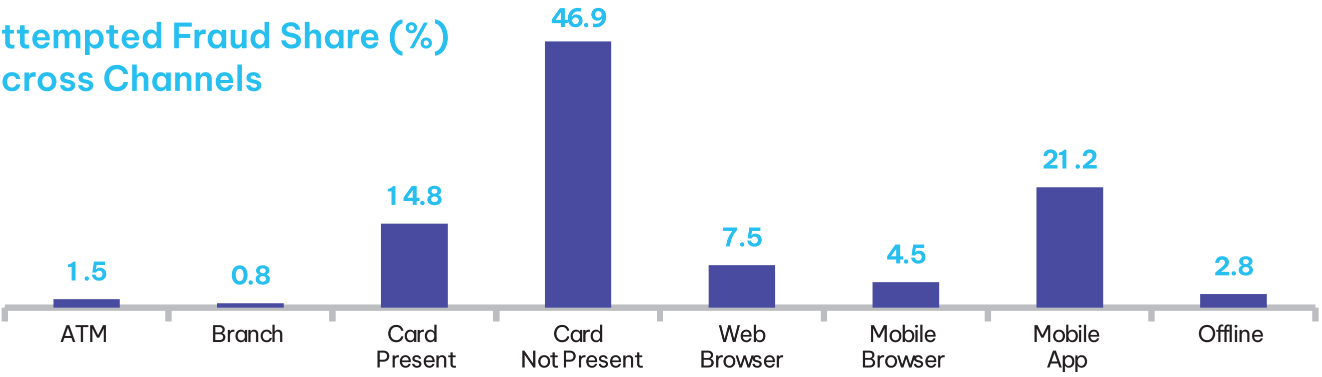
Mobile Device Risk

Attempted fraud attacks through mobile apps trending up



of attempted fraud attacks through mobile apps are account takeovers (ATOs)

Attempted Fraud Share (%) Across Channels



FOR THE FRAUD FIGHTER:

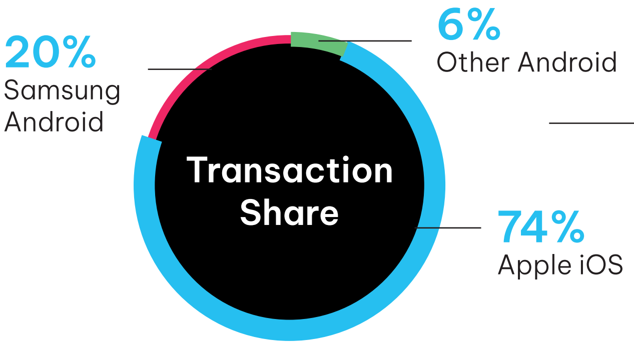
In relation to this increase, it's widely known that mobile and web browsers are the preferred tool for nefarious, trans-national criminal third-party fraudsters looking to hide from tools that identify unusual login or device factors, with defense against ATO a specific risk focus in this consideration. While not ignoring risks through the mobile and web channel, the same risks apply to mobile apps, especially when we see multiple accounts and associated transactions all tied to the same device.

With the surge of pandemic-relief unemployment insurance and Paycheck Protection Program (PPP) fraud, we also saw a shift in the industry toward markedly brazen "citizen" or amateur fraudsters.

These domestic actors are less likely to use proxies and will login into accounts through the mobile app channel. Because they are less concerned about being caught, they often take the most convenient route to access funds. Mobile app channels at the account-to-account comparison are much easier for the citizen fraudster to access as they quickly move around and exit funds. In addition, the industrialization of fraud has led to success for organized fraudsters in recruiting mules and facilitating large, human-at-the-control "bot-farms" to get around transaction monitoring and behavioral biometrics tools that are used to address scam-risks. Unfortunately, the mobile app channel is not immune to these attacks.

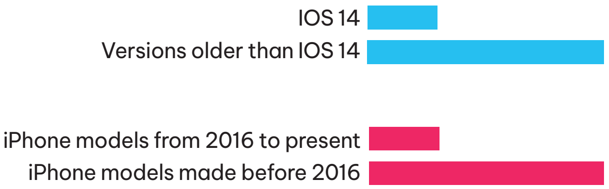
Mobile Device Risk

Older mobile devices are vulnerable to fraud attacks



Android devices other than Samsung have twice the attempted fraud rate.

Apple iOS and Device Model Fraud Risk



iOS versions older than 14 are 3x riskier

Device models made before 2016 are 3x riskier

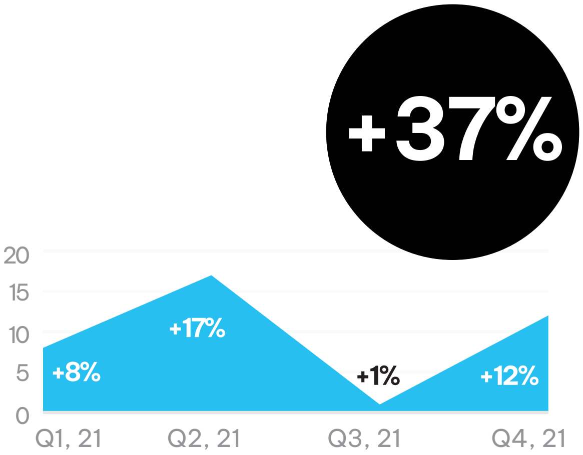
FOR THE FRAUD FIGHTER:

Older devices are cheaper and easier to infiltrate, making them the favored choice of fraudsters. Past iOS versions are not supplied with the latest security patches, rendering them more vulnerable to attacks. To strengthen fraud and device-based risk strategies, FSOs must add risk signals associated with older versions of mobile OSs and device models – especially devices that don't support higher mobile data bandwidths of 4G and above. Segmentation of devices and OSs based on their age could also prove to be helpful.

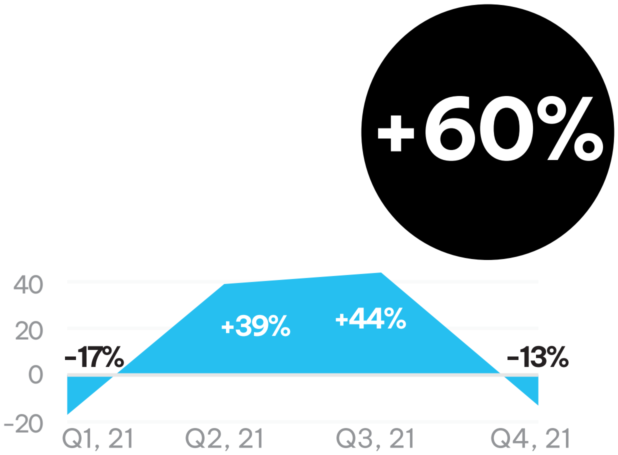
Apple Pay

Fraudsters focus on payment methods like Apple Pay

Quarterly % change in transaction volumes



Quarterly % change in attempted fraud



FOR THE FRAUD FIGHTER:

Fraudsters use stolen credit card data to make fraudulent purchases using Apple Pay. With Apple Pay adoption increasing as an essential new payment method, it's no surprise that fraudsters have turned their focus to this channel.

Apple Pay provides two pathways for authorizing new cards on an Apple device; one for instant authorization and one that requires additional checks. Apple provides the same information to all participant banks for risk qualification, and each participant can interpret the data and assign a risk score on its own.

Fraudsters have found that some issuing banks issue cards that are easier to register with stolen identity information than others, mainly if 3D Secure is not employed for card-provisioning risk.

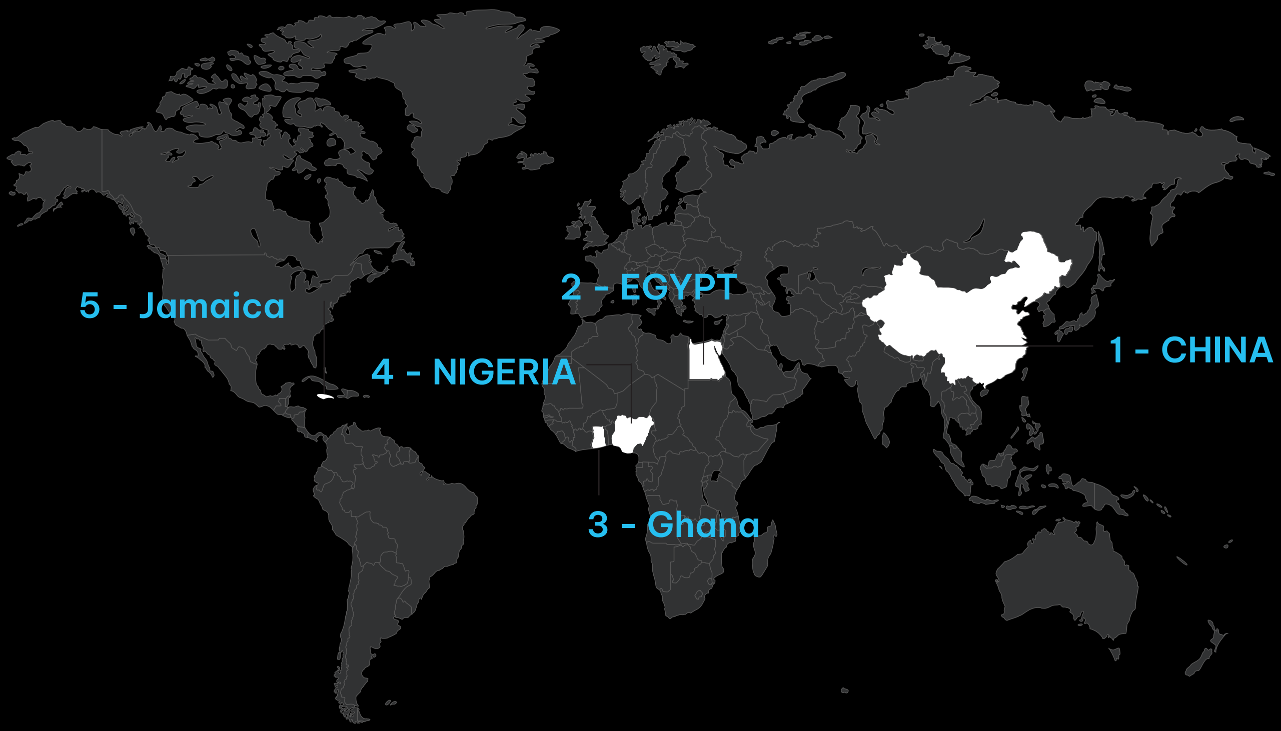
Apple ID phishing scams represent a genuine danger. For scammers, your Apple ID is the ticket to using anything Apple-related and provides access to a wealth of personal information on the cloud.

A diligent authentication mechanism for Apple Pay enrollment events, such as asking for a one-time password (OTP) sent on a registered mobile number, could significantly suppress these attacks. Firms can strengthen protection against these attacks by enriching the Apple Pay risk score with additional data points to ascertain risk without increasing customer friction.

Top 5 Riskiest Geo-Locations

The connection between regions and device time zone

Originating from Non-US Time Zones via U.S.-based ISPs/Proxies



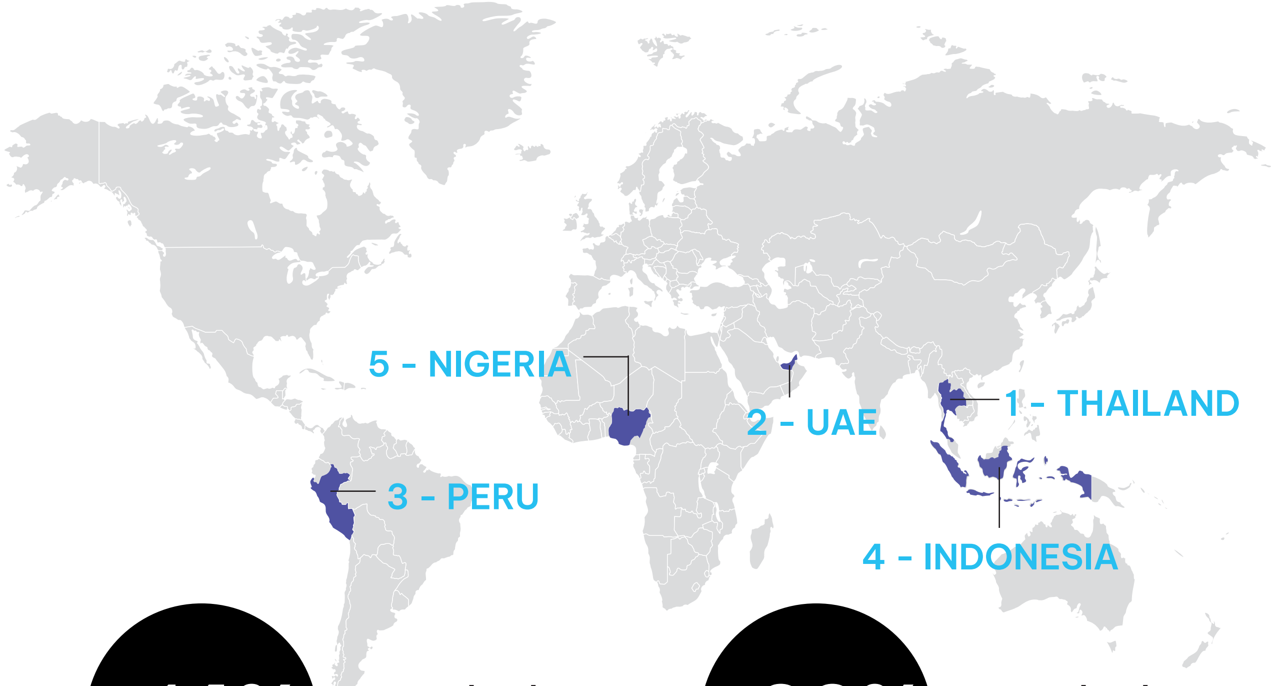
FOR THE FRAUD FIGHTER:

Our data revealed a higher risk of fraudulent activities in online channels where connection regions do not concur with the mobile device time zone. Attacks originate from a device in a remote time zone, but the connection region is in proximity to the victim's location. Fraudsters are likely taking advantage of proxies that make transactions look legitimate. We strongly advise establishing strategy rules to identify the misalignment between connection origination region and mobile device time zone, language and SIM country to mitigate these attacks.

Top 5 Riskiest Countries

Rise in remote access scams

Payments Originating from the U.S.



+14% **- cross-border attempted fraud**

+20% **- cross-border payments**

FOR THE FRAUD FIGHTER:

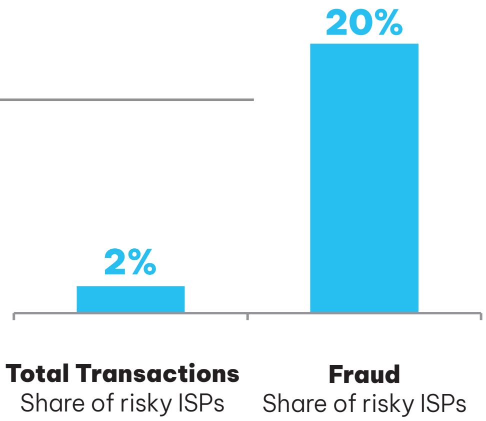
Our data indicates a significant rise in remote access scams wherein fraudsters gain access to customers' personal information and bank account details. The fraudsters disguise themselves by calling as tech support or sharing a malicious link in a phishing email. Customers should be educated not to access any link in emails from suspicious senders and not allow anyone to gain remote access to their system. Additionally, FSOs should apply higher risk attributes to high-value, cross-border payments to a new payee right after payee setup to help monitor these events efficiently.

RISKY INTERNET SERVICE PROVIDERS

Actual fraud rate of risky ISPs is high

Payments Originating from the US

Risky ISPs have an average fraud rate of 4%, whereas common/ low-risk ISPs have an average fraud rate of less than 0.5%


The Risk of “Risky” ISPs

FOR THE FRAUD FIGHTER:

We estimate actual fraud rate of risky ISPs to be much higher than 4%, as many of the non-fraud transactions passing through these risky ISPs are suspected of missing fraud reports.

Many ISPs use high-speed content delivery networks (CDNs) for high availability and better performance. In a CDN, hundreds or thousands of domains in the nearby geographical location may resolve to the same IP of an edge server, complicating fraud risk scoring considerations. A malicious domain, whether it be a proxy or VPN attempting to mask the user's location, will share the same IP as other benign domains in the same CDN, acting as a cover for malicious domains.

We recommend profiling ISP traffic to determine risk and creating a strategy based on ISP risk level, rather than IP addresses. Judicious monitoring of traffic from these ISPs to identify suspicious behavior is of utmost importance. A customer that typically logs into their bank account from a mobile device or residential ISP over the web and then suddenly starts to use one of these risky ISPs would be a strong signal for identifying attempted ATO, money mules, or activation of fraudulent or dormant accounts.

NICE
Actimize

Put these insights into action with NICE Actimize fraud solutions.

www.niceactimize.com/fraud-authentication-management

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.