NICE · ACTIMIZE

Prevent Authorized Push Payment Fraud

eBook

NICE · ACTIMIZE

Authorized Push Payment (APP) fraud is an urgent fraud threat facing financial services organizations (FSOs) today. Fraudsters are relying on a variety of clever techniques to capitalize on escalating online activity, market uncertainty and digital vulnerabilities. This creates complex new challenges as FSOs address a rapidly changing post-pandemic risk landscape.

APP Fraud Cases are on the Rise

APP fraud has steadily grown alongside the surge of real-time payments and the growing adoption of digital channels. The United Kingdom in particular has become a hotbed of APP fraud in recent years, with the COVID-19 pandemic amplifying the threat.

Fraudsters leverage a diverse toolkit to execute financially devastating crimes against businesses and individuals who are manipulated into sending money directly to an account controlled by the criminal. Though digital fraud has accelerated over the past few years, the pandemic has presented abundant opportunities for criminals to use both the rising dependency on digital services and widespread uncertainty to defraud people.

APP fraud represents a reputational challenge for both sending and receiving banks, and as liability shifts, amplifying pressure to reimagine fraud prevention.

> **APP fraud cases increased by 22 percent to nearly 150,000 in 2020, and associated fraud losses were up 5 percent from the previous year.[1]**

NICE · ACTIMIZE

Losses due to authorized push payment scams were

£479 million in 2020

This was split between personal

£387.8 million

and non-personal or business

£91.3 million.[2]

APP Fraud Proliferates in a Real-Time Payment Landscape

Criminal use of real-time rails gives them a distinct advantage, as they can make off with funds before the victim realizes they have been defrauded. Once the payment has been authorized, the victim cannot reverse it due to the character of the payments.

APP fraud schemes include:

- Social engineering
- Romance scams
- Investment scams
- Fake invoice fraud
- Mule account activity
- Property purchase fraud
- Business email compromise

These fraud schemes are difficult to detect because the payment or transaction is enacted by a legitimate user who is logging in from a verified location and device.

Under current legislation, customers have no legal protection against losses. However, under the voluntary Contingent Reimbursement Model Code (CRM Code), which has been in place since May 2019, participating banks will reimburse customers who have been victimized by APP fraud in certain circumstances.

NICE · ACTIMIZE

Only 45%

of reported APP losses are reimbursed or repatriated.[3]

Empowering Customers & Building a Defense Against APP Fraud

NICE · ACTIMIZE

FSOs need to adopt key multilayered defensive tactics that align with the Contingent Reimbursement Model.

- Receiving banks and sending banks must protect both inbound and outbound customers.
- Improve customer messaging and develop educational campaigns to help consumers better protect themselves.
- Issue risk-based warnings within various payment journeys that trigger customers to consider the situation rationally and ask, “does this make sense?”

- Use all available digital tools, including device profiling, malware detection and behavior biometrics, layered with a powerful fraud prevention platform.
- Utilize advanced analytics to build specific models to identify customers at risk of APP fraud and the payments themselves.

FSOs should combine all of these components together with a case management system that helps banks examine the entities involved and identify anomalous behaviors and network lines. This allows them to efficiently identify APP fraud in a way that impacts fraudsters rather than genuine customers.

Holistic Fraud Prevention Starts with IFM-X

As one of the most challenging financial crimes to detect and fight, APP fraud demands a combination of layered, holistic fraud prevention, due diligence and vigilant defensive tactics - all built upon a foundation of AI and advanced analytics.

NICE Actimize's APP Fraud Prevention coverage is powered by IFM-X, the most advanced integrated fraud management platform on the market.

IFM-X

NICE · ACTIMIZE

Out-of-the-box data integration: Simple and quick data integration for faster payments and robust tools to detect, interdict and resolve high-risk events.

APP dedicated analytics: Real-time detection and response for high-value payments and a rich library of predictive features specific to APP fraud. Analyze and evaluate risks of both outgoing and incoming payments.

Web, mobile, offline channel protection: Channel and gateway monitoring to provide hermetic coverage and help FSOs improve the customer experience via payment lifecycle monitoring.

Customer-centric fraud prevention: Monitor monetary and non-monetary events and identify social engineering attacks and mules accounts.

Get a Head Start in Realizing the Benefits of APP Fraud Prevention

Investing in the right systems and developing a proactive approach to APP fraud can offer advantages for FSOs that go far beyond stopping fraud.

FSOs will be better equipped to protect customers from life-changing scams and can reduce their organization's liabilities and fraud losses that impact their bottom line. This creates a hostile environment for fraudsters, further reducing costs on their organization. This also means less management time spent handling the regulatory side of APP fraud.

Most importantly, FSOs can promote customer trust, loyalty and safely facilitate industry innovations.

The APP Fraud Trend Will Continue: Are you Prepared?

The APP fraud trend will likely continue alongside the ongoing popularity of real-time payments. FSOs must revamp their approach to fraud prevention to better protect their organization, customers, reputation and bottom line. With the ability to make real-time, quality decisions backed by autonomous intelligence, FSOs can approach APP fraud in a cost-effective, holistic fashion.

NICE Actimize's **IFM-X** is the first line of defense against APP fraud. This covered, based on expert-driven continuously optimized machine learning analytics, helps ensure FSOs can accurately identify social engineering scams and mule accounts, resolve high-risk events and deliver better customer experiences.

Ready to get started?

Learn more

1 (2021, March 26) APP Fraud continues to rise as criminals target bank customers online. Finextra. https://www.finextra.com/newsarticle/37751/app-fraud-continues-to-rise-as-criminals-target-bank-customers-online

2 Worobec, K. (2021) Fraud – The Facts 2021. UK Finance. https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf

3 Connor, T. (2021, March 30) PSR Consultations: Could the proposed measures to fight fraud have unintended consequences?. Finextra. https://www.finextra.com/the-long-read/172/psr-consultations-could-the-proposed-measures-to-fight-fraud-have-unintended-consequences?utm_medium=longreadflash&utm_source=2021-3-30&member=126912

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.

www.niceactimize.com

NICE ACTIMIZE