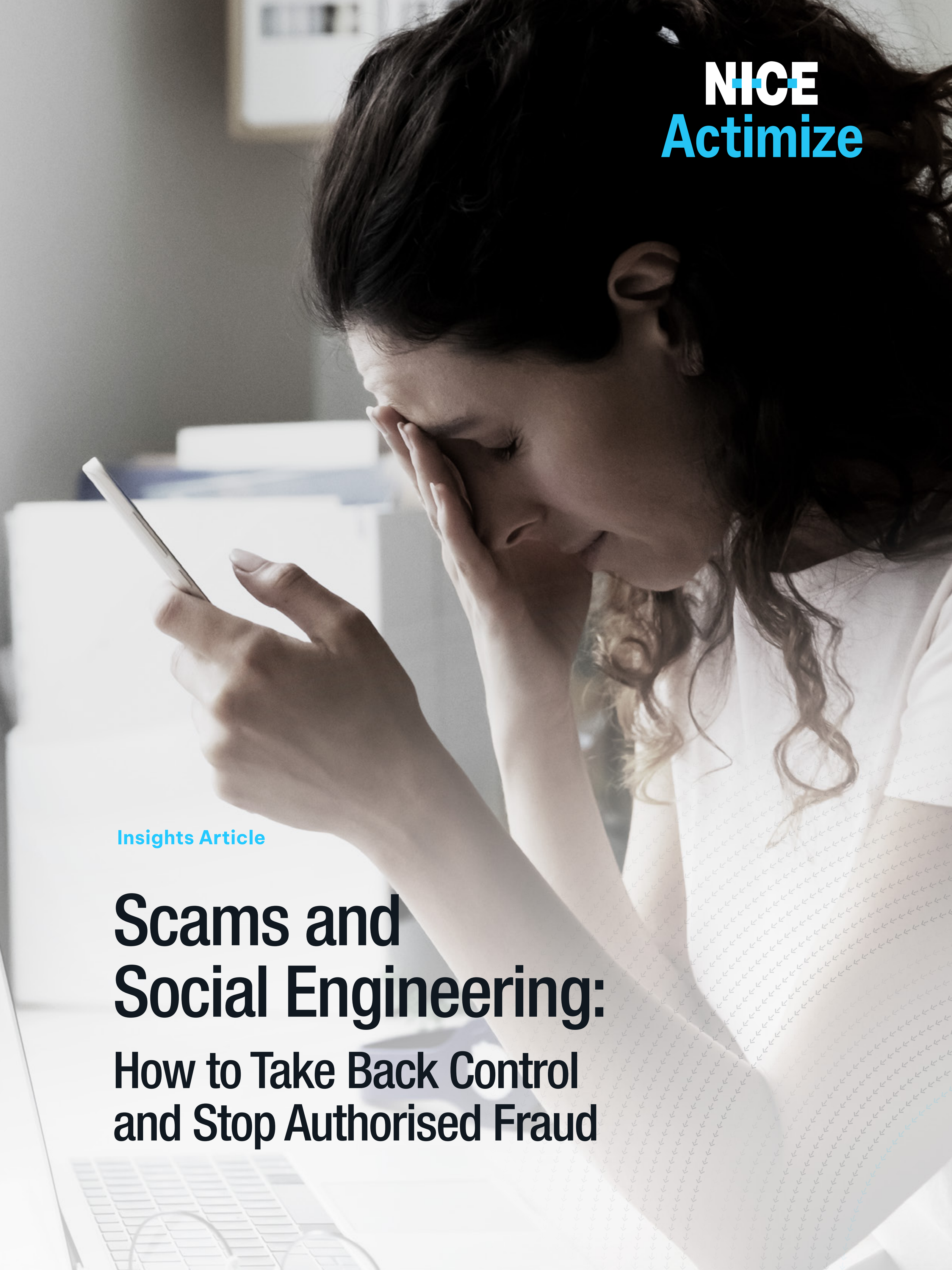

NICE Actimize

Insights Article

Scams and Social Engineering:

How to Take Back Control and Stop Authorised Fraud

Maybe you didn't fall for a financial scam. But we all know someone who did.

Social engineering is a growing global trend: It's an easy way for fraudsters to make money and has high potential for a large profit. As one of the most complex, high-quality fraud typologies, social engineering involves a combination of coordinated attacks that are often difficult to detect or prevent.

Why?

The advances in technology, shifting payments landscape, and market disruption like the pandemic triggered increases in digital activity that heavily influenced social engineering trends. Many fraudsters engaged in identity theft or synthetic identity fraud during the pandemic shifted their focus to social engineering scams.

Other factors include:

- Faster and instant payments, such as peer-to-peer payment (P2P) applications, represent perfect vehicles for fraudsters to get paid. These payments provide immediate cash transfers to anyone, anywhere.
- Mule accounts are easy to set up and maintain, giving fraudsters an easy way to cash out.

Scam tactics evolve so fast that it's straining an FI's ability to fight back, even with cutting-edge fraud prevention tools.

Scams that look legitimate to customers

A scam that typically follows social engineering—authorised fraud or authorised push payment (APP)—is now gaining momentum. It's executed in all kinds of imaginative ways.

At a simple level, a victim is coerced into authorising a transaction that they believe is legitimate, only to realise they transferred funds to an account that's either directly controlled by the fraudster or a mule account. Another way is when customers respond to an ad on a social platform that offers a desired product for a drastically reduced price. They buy it and authorise payment, so the fraudster doesn't even interact with them.

These types of digital attacks are more challenging to manage, as customers truly believe those transactions are authentic. Consequently, they expect fast payment processing and might not even trust their financial institution (FI) when told the transaction is fraudulent.

Balance customer experience with fraud impact

FIs processing these transactions only have a matter of seconds to determine if a particular transaction is fraudulent or not. It's a balancing act: There's pressure to deliver seamless CX while simultaneously mitigating fraud, improving operational efficiency, and complying with regulations.

Regulatory impact on global scale

The sheer prevalence and scale of APP scams are drawing scrutiny at the highest levels. Changing liability laws for scams are pushing responsibility for these attacks towards FIs in Europe and the United States.

DNB Bank, Norway's largest financial services group, reported a 500%+ increase in phishing in 2021 compared to the previous year1. In Europe, apart from the U.K., customers are often still liable for losses associated with these attacks. However, pressure is growing across many markets for FIs to take on more liability.

Attacks in the U.S. sparked federal-level conversations around potential changes in liability laws. In April 2022, U.S. senators sent a letter to a major payments network inquiring about the procedures in place to detect scams, the policies for which scam victims receive refunds, and if Reg E applies to scam victims—including those manipulated into authorising a fraudulent transfer.

With greater adoption of instant payments, proliferation of scams, and government interest in FI fraud prevention processes, it's likely institutions will bear responsibility for losses, particularly in the U.S.

To avoid regulatory fines and loss of revenue from APP scams, FIs need to have the most effective, real-time transaction decisioning tools available, as well as appropriate strategies to communicate with potential victims.

Raise customer awareness

Effective fraud prevention strategies use advanced technology and updated processes, but it starts with educating customers. FIs can warn and train customers to spot fraud. That raises awareness of scams while reducing the likelihood that customers are victimised by fraudsters.

FIs can:

- Explain how they'll communicate when a fraud event occurs, so customers can easily spot requests or instructions that aren't from their FI.
- Employ fraud risk-mindedness to all external communications so customers aren't confused about who is contacting them.
- Eliminate the stigma associated with being defrauded, particularly with sensitive attacks such as romance scams, by:
    - Showing empathy, as these are sophisticated scams designed to prey on emotions and feelings
    - Treating victims with respect to reduce the shame they feel, which also encourages them to reach out immediately when they realise they've been scammed
    - Handling a fraud claim appropriately while protecting the customer's privacy, to strengthen the customer relationship at a time when they might feel exposed or embarrassed

These tips, along with updating technology to better detect a broad range of emerging and existing APP scams, will protect FIs and the customers they serve.

Use advanced authorised fraud risk management

There's no single method to stop authorised fraud, but FIs can fight back with a layered approach to fraud prevention that's supported by advanced analytics and machine learning (ML).

Think of it like a fraud prevention cocktail: a blend of behavioural biometrics and mobile data intelligence mixed with ML and artificial intelligence (AI) models. All these components are brought together with early account monitoring to detect these scams faster. Using smart ML and AI, financial institutions have a comprehensive risk solution that makes it harder for fraudsters to target their organisations and successfully defraud customers.

Authorised fraud risk management that's built on this foundation helps FIs detect these invasive APP scams faster with:

- Proactive customer risk profiling to identify customers who might be more vulnerable to scams and support early intervention strategies.
- Targeted machine learning scam models that are trained and optimised to pinpoint specific scam challenges.
- Earlier mule identification to address the rise in using money mules.

Take Back Control

With NICE Actimize, fraud prevention teams can react to threats in real time using next-generation strategy and decision-making tools. By leveraging collective intelligence across multiple financial institutions (key risk indicators such as region and IP), and a library of 500+ expert features to address a wide spectrum of fraud, FIs have timely information to combat emerging threats.

Learn more 〉

about how to outsmart fraudsters to keep customers safe from increasing authorised fraud such as social engineering scams.

[1] DNB: Annual Fraud Report 2021 (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.

© Copyright 2022 Actimize Inc. All rights reserved.

www.niceactimize.com