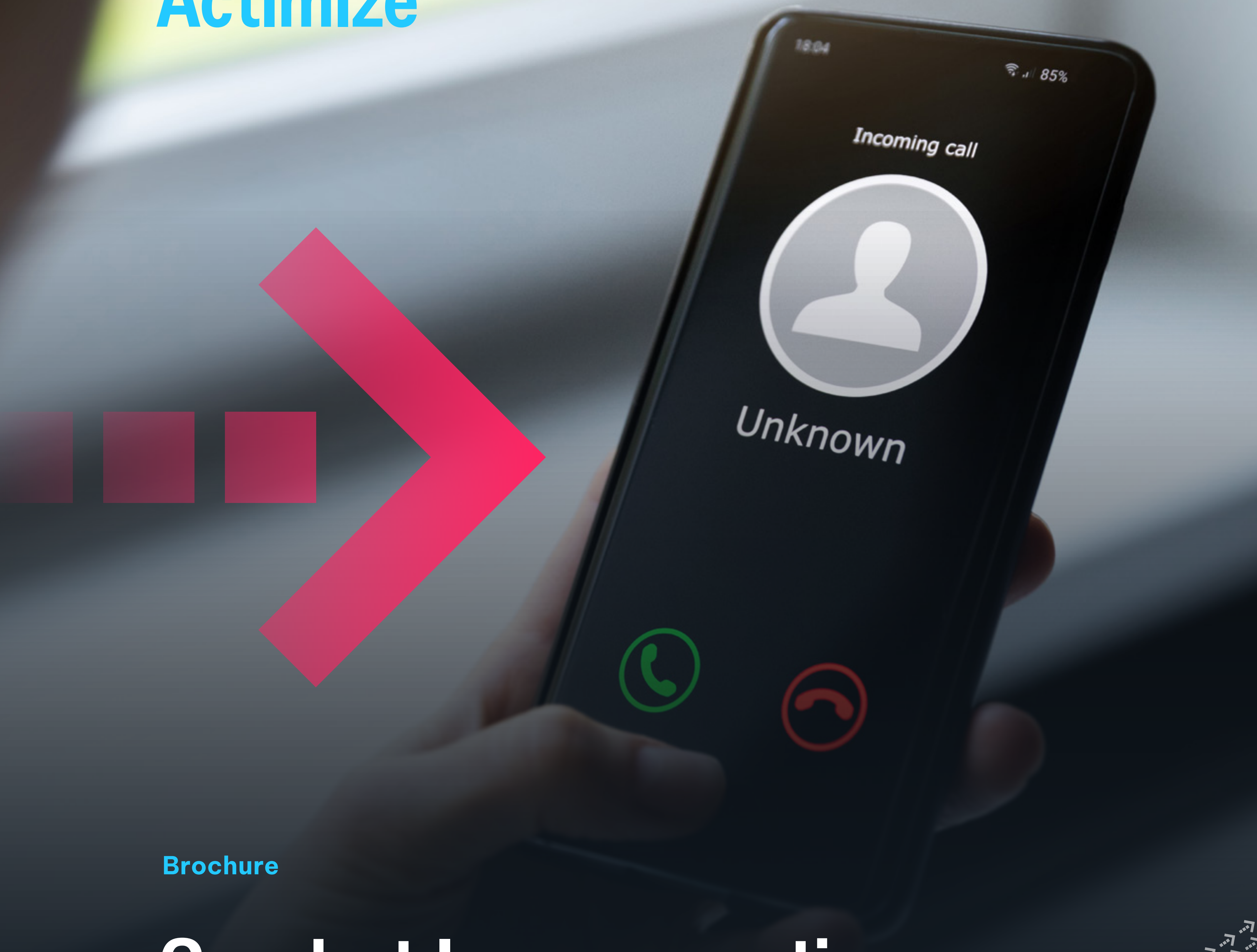
NICE Actimize



Brochure

Combat Impersonation and Common Scams

The Social Engineering Tactic That Leverages Good Customer Relationships

Social engineering is a complex, high-quality fraud tactic where victims are manipulated into authorizing transactions on a fraudster's behalf. It's a core technique used in impersonation scams: Fraudsters pose as legitimate persons and entities to convince customers to do business with them.

And it's working. The Federal Trade Commission (FTC) received more than 2.5 million reports of impersonation scams from consumers nationwide from the beginning of 2017 through the middle of 2022, and those consumers reported losing more than $2 billion to these scams.[1]

The Human Toll of Impersonation Scams

At a simple level, authorized fraud is when a victim is coerced into authorizing a transaction that they believe is legitimate, only to realize they transferred funds to an account that's either directly controlled by a fraudster or mule account.

While it's generally accepted that financial insecurity is a key factor in falling for impersonation scams, it would be short-sighted to assume that savvy customers won't fall for them. These scams can impact all ages, education levels, and wealth, but some demographics are more vulnerable than others, e.g. senior citizens. By establishing authority and creating a sense of urgency, the scammers are able to coerce a victim into conducting an action, usually a fraudulently induced payment or providing personally identifying information.

Some of the most common types of scams include:

- Impersonation scams – The scammer pretends to be the customer's bank, a government agency, or law enforcement. One of the most common scams involves a "police officer" and "grandchild" calling a grandparent to wire bail money into a scammer's account.
- Investment scams – These involve false investments where the scammer takes off with the money; crypto investment scams are a major problem.
- Romance scams – The scammer takes on the persona of a romantic partner to coerce the victim into providing funds for them through various means.
- Purchase scams – Fake products and/or services are listed for sale where the victim makes a payment for something that never arrives.
- Advance Fee scam – The most prominent example of this is the Nigerian Prince (419 scam) email chain that invites victims to send a small amount of money in exchange for receiving a larger amount in return, but other examples include the beneficiary fund scam where scammers request help to get money from a bank in another country, lottery scams that claim the victim won money in an overseas lottery, career opportunity scams that entice victims to attend a consultation at the cost of an upfront fee, and other investment scams.
- Safe Account scam – This can be an offshoot of impersonation scams where the scammer convinces the victim their money is not currently safe but will be safe if moved into the scammer's account.

→ Learn More

In an instant payments landscape, impersonation scams are even more challenging to catch. Not only are real customers authorizing these payments—cash transfers happened immediately. Even with cutting-edge fraud prevention tools, financial institutions (FIs) are struggling to combat these sophisticated scams. The sheer prevalence and scale of these authorized push payment (APP) scams are drawing scrutiny at the highest levels.

Global and Regulatory Impact

Changing liability laws for scams are pushing responsibility for these attacks toward FIs in Europe and the United States.

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 Regulation E applies to scam victims—including those manipulated into authorizing a fraudulent transfer.[2]

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, especially impersonation scams that are so hard to detect given their level of sophistication, FIs need to have the most effective, real-time transaction decisioning tools available, as well as appropriate strategies to communicate with potential victims.

Bank Impersonation Scams

The growing trend of bank impersonation scams in particular is alarming because fraudsters perfected their outreach tactics. Clues like misspellings and amateur design that imply fraud are nonexistent.

Fraudsters phish confidential information by employing website links that successfully mirror the bank's communications or other forms of phishing, such as:

- Smishing—fraudsters send text messages via spoofed numbers
- Vishing—scammers use phone calls to trick victims into revealing sensitive information that can be used to gain account access

These techniques are often used together, and they're highly effective at convincing victims that their bank is legitimately contacting them. In these types of attacks, customers truly believe the transactions they're authorizing are authentic. Consequently, they expect fast payment processing and might not even trust their FI when told the transaction is fraudulent. As friction in the process can lead to customer attrition, FIs are also under pressure to deliver seamless customer experiences while simultaneously mitigating fraud, improving operational efficiency, and complying with regulations.

How can financial institutions combat impersonation scams, retain customer trust, and maintain compliance? With a three-pronged strategy: safeguarding against these kinds of attacks with education, updating their fraud prevention strategies, and adopting technology powered by AI/ML for scale and speed.

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 impersonation fraud. That raises awareness of scams while reducing the likelihood that customers are victimized by fraudsters.

To raise awareness, 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 realize 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

→ Learn More

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.

Advanced Authorized Fraud Risk Management

There's no single method to stop authorized 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 behavioral 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, FIs have a comprehensive risk solution that makes it harder for fraudsters to target their organizations and successfully defraud customers.

Authorized 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 optimized to pinpoint specific scam challenges
- Earlier mule identification to address the rise in using money mules

Take Back Control from Scammers

With NICE Actimize, fraud prevention teams can react to threats in real time using next-generation tech 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 such as impersonation scams.

For more information on NICE Actimize solutions that combat authorized fraud, click here

[1] FTC: FTC Proposes New Rule to Combat Government and Business Impersonation Scams (2022)
[2] U.S. Senate: Oversight Letter (2022)

→ Learn More

NICE Actimize

Know more. Risk less.

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.

niceactimize.com