ThreatMark

→ BEHAVIORAL INTELLIGENCE PLATFORM

DISRUPTING SCAMS & SOCIAL ENGINEERING FRAUD.

Modern scam techniques have evolved.

Scams now target those most vulnerable; the customer. Fraudsters commonly avoid direct interaction with banking platforms, manipulating the victims into conducting the transaction instead. Traditional fraud detection methods are therefore ineffective as the legitimate user is logging into their own account from their own device and location, with appropriate credentials to carry out the transaction.

Instant Payment Scams

Instant payment scams exploit the speed of electronic transactions, tricking victims into making immediate payments under false pretenses. Common tactics include fake invoices, lottery winnings, or urgent requests for help. Once the payment is made, it's often irreversible, causing financial losses and highlighting the need for caution in online transactions.

Investment Scams

Investment scams lure individuals with false promises of high returns or exclusive opportunities. Perpetrators may use fake investment platforms, Ponzi schemes, or pressure tactics to persuade victims to invest. Once funds are transferred, scammers disappear, leaving victims with significant financial losses.

Peer-to-Peer Fraud

Peer-to-peer (P2P) fraud involves deceptive practices within direct transactions between individuals. Scammers exploit platforms facilitating peer-to-peer interactions, such as online marketplaces or payment apps. They may use fake profiles, misrepresent items, or employ various schemes to defraud unsuspecting users, often resulting in financial losses.

Purchase Scams

Purchase scams deceive buyers through fake online listings, often on e-commerce platforms. Scammers offer goods or services at attractive prices, enticing victims to make payments but the purchased items never arrive or are vastly different from descriptions. This emphasizes the importance of verifying sellers and using secure payment methods when making purchases.

Authorized Push Payment Scams

Authorized Push Payment (APP) scams are a sophisticated fraud involving perpetrators tricking individuals into willingly transferring funds to an account controlled by money mules. Perpetrators disguise themselves through convincing stories, exploiting trust to manipulate victims into authorizing payments.

Romance Scams

Romance scams involve fraudsters building fake romantic relationships online. The fraudster creates a fictitious personas to emotionally connect with target, gaining trust over time. They then exploit this trust to request money, often citing emergencies or personal crises. Victims, emotionally invested, suffer significant financial losses and emotional turmoil before realizing.

MITIGATING SCAMS IN REAL TIME.

ThreatMark's unique **Fraud Disruption Solution** refocuses fraud professionals on identifying fraudulent users against legitimate customers, interrupting fraud operations across all stages of the attack.

Scams and social engineering fraud present significant challenges for banks due to their reliance on manipulating the customer rather than breaching the system directly. These schemes exploit human psychology, tricking individuals into voluntarily surrendering sensitive information or making unauthorized transactions. As a result, traditional security measures that monitor for external threats are often bypassed, making detection and prevention particularly difficult.

70%
Better detection rate
(than traditional FDS)

90%
Fewer false positives
(than traditional FDS)

90%
Decrease in cost for authentication
(ets. SMS cost saving)

2
Weeks to implement
(cloud option)

Improved detection & scoring methods
(when integrating with existing systems)

ThreatMark's Behavioral Intelligence Platform is the world's first full-stack fraud prevention platform built on behavior intelligence. Combining transaction risk analysis, threat detection, and user behavior profiling capabilities in one integrated platform, ThreatMark monitors signals including:

Instant Payment Risk Scoring
In vishing attacks, scammers use various tactics to avoid being caught including using high-priority transactions. Carefully examining the priority attribute of a payment is a method of preventing fraudulent transactions.

Active Phone Call
Scammers use coercion to manipulate victims acting against their best interest, often talking the victim through the money movement process. Monitoring for active phone calls during a banking session can be a signal of a scam in progress.

Abnormal Payment
Fraudulent payments can be identified by analyzing payment amount, time, day and month of transfer, and beneficiary. Examining payment context with other risk indicators can detect abnormal payments and disrupt fraud attacks.

Remote Access Tools (RAT) In Use
When scammers convince unsuspecting victims to install a RAT, they hijack legitimate banking sessions. The moment the scammer starts the tool, mouse movements, keystrokes, and other behavioral patterns indicate a RAT is in use.

Payment Tampering
Payment tampering fraud happens when someone intervenes with the payment process to divert funds, alter payment information, or manipulate transaction data. Discrepancies between payment details can reveal tampering.

Mobile Biometry Anomaly
Mobile behavioral biometry is used for continuous user verification. Observing each user's unique patterns of they how use a device during previous sessions, matches can be made in real-time to confirm if a user is legitmate.