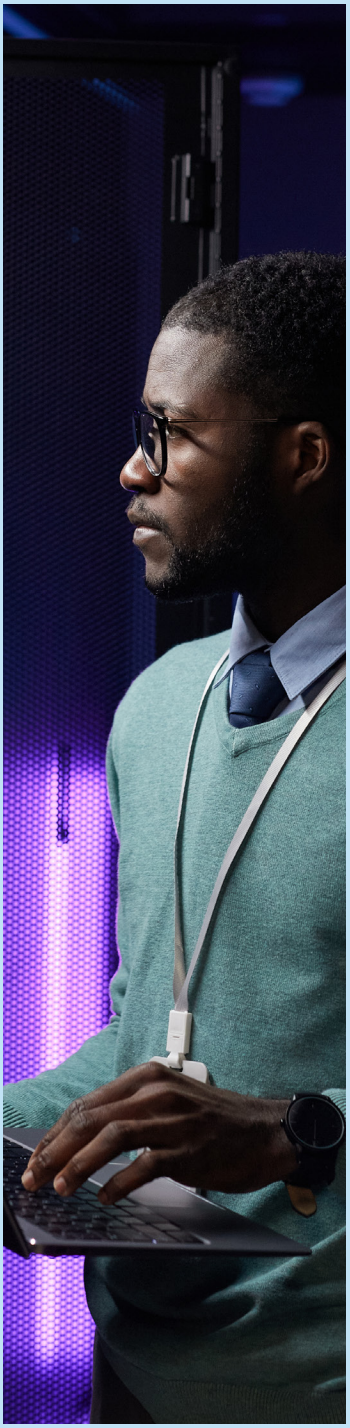
VIEW POINT



OMNICHANNEL FRAUD DETECTION: ENSURING SECURITY ACROSS ALL TOUCHPOINTS

Abstract

In today's interconnected world, businesses must secure a wide range of touchpoints to protect against fraud. Businesses must explore the challenges posed by omnichannel fraud, highlighting the impact of emerging threats such as SIM-swapping, deepfakes, and bots. It delves into the importance of integrated fraud detection systems and fraud risk management strategies, showcasing how AI, machine learning, and behavioural biometrics are key to identifying and mitigating fraud across various sectors. Explore best practices for building a secure omnichannel framework to safeguard customer trust and reduce financial losses.

Infosys®
Navigate your next

Customers today expect a unified experience, whether they're shopping on a website, chatting with a bot, or swiping a card in-store. Businesses have responded by knitting together these touchpoints into a cohesive omnichannel ecosystem. However, the same channels that enhance customer experience also open new doors for fraudsters.

With multiple touchpoints to exploit, cybercriminals can harvest personal data, create fake accounts, hijack legitimate ones, and execute fraudulent transactions. They also manipulate customer service agents through social engineering tactics. If these channels are not properly integrated and secured, fraudsters can easily evade fraud detection systems by switching between platforms.

This PoV explores how businesses can strike the right balance — delivering a smooth customer journey while strengthening fraud risk management and safeguarding accounts from fraud.

The expanding threat landscape

From phishing scams targeting online shoppers to account takeovers via call centres, fraudsters exploit every available touchpoint. Their tactics range from synthetic identity fraud — where fake profiles slip through weak verification processes — to deepfake technology used to impersonate legitimate customers.

The impact of omnichannel fraud is staggering. Beyond financial costs, the erosion of customer trust is even more detrimental.

The cost of fraud poses a significant financial risk to organisations, with businesses losing revenue due to fraudulent activities. Fraud concerns remain high among both consumers and businesses, with a small percentage of all global digital transactions in 2024 suspected to be fraudulent.

Fraudsters take advantage of digital account openings.Account takeovers (ATO) compromise customer trust and finances, with fraudsters exploiting stolen credentials to drain accounts or steal data, a threat that's ballooned with the rise of omnichannel interactions.

As quantum computing advances, real-time deepfake creation could challenge defences, increasing the complexity of cross-channel fraud detection. At the same time, bots are automating fraud at scale, fuelling retail attacks that overwhelm traditional defences across omnichannel platforms.

How fraudsters exploit security gaps across sectors

Fraudsters find weak authentication on mobile apps or unmonitored social media interactions. They often use one channel, say phishing emails, to steal credentials and exploit another, such as mobile banking, to execute fraudulent transactions. Here's how fraud unfolds in different sectors:

Retail and e-commerce

A major tactic is Buy-Online-Pickup-In-Store (BOPIS) fraud. Criminals create fake accounts with stolen identities and credit cards, bypassing shipping verification. They collect items in-store with counterfeit IDs and may cancel orders last minute, exploiting delays in system updates to secure both the product and a refund. Fraudsters also use bot-driven attacks to take over accounts, steal loyalty points, or exploit return policies for financial gain.

Contact centres

Fraudsters use social engineering techniques to trick customer service agents into resetting passwords, changing account details, or bypassing security questions. By posing as legitimate customers, they gain access to bank accounts, shopping profiles, and personal data. In some cases, they even convince agents to disclose sensitive information, which they later use for identity theft or unauthorised purchases.

Banking and financial services

Fraudsters exploit weak authentication processes to gain control over customer accounts. They use stolen credentials, phishing attacks, or deepfake technology to bypass identity verification and authorise fraudulent transactions. Loan fraud is another growing concern, where criminals apply for loans or credit cards using synthetic identities — combining real and fake information to appear legitimate. Once approved, they withdraw funds and disappear before detection.

Telecommunications

SIM-swapping is one of the most common fraud tactics in telecom. Scammers hijack a victim's phone number by convincing a carrier to transfer it to a new SIM card. Once they have control, they intercept One-Time Passcodes (OTPs) and gain unauthorised access to banking, email, and social media accounts. Criminals also create fake accounts with telecom providers to obtain high-end smartphones on instalment plans, disappearing before making payments.

Healthcare and insurance

Medical identity theft is a growing issue, with fraudsters using stolen patient data to receive treatments, prescriptions, or file fake insurance claims. Some criminals create fake clinics to bill insurers for non-existent procedures. Ransomware attacks also target healthcare providers, locking patient records for ransom. From Q3 2023 to Q2 2024, the Federal Trade Commission received over 10,000 reports, with annual losses reaching billions.

Travel and hospitality

Loyalty fraud is a major issue in this sector, with criminals hacking customer accounts to steal points and resell them. Fraudsters also book flights and hotels using stolen credit card information, then cancel and request refunds to different accounts. Chargeback fraud is another concern, where scammers falsely dispute legitimate charges to get their money back while still using the services.

Gaming and digital entertainment

The gaming industry faces rising fraud, including account takeovers, in-game currency theft, and the sale of hacked accounts. Criminals use stolen payment methods to buy virtual goods or sell compromised accounts on the dark web. Bots and automation also play a role in cheating, boosting accounts fraudulently and selling them at a premium. Money laundering through in-game transactions allows criminals to convert illicit funds into digital assets and cash out via marketplaces.

Building a secure omnichannel framework

Ensuring security across all touchpoints requires a proactive and multi-layered approach. Businesses must move beyond traditional fraud detection methods and adopt advanced technologies that analyse customer interactions holistically.

Behavioural biometrics and AI-powered monitoring

Advanced authentication methods, such as behavioural biometrics, enhance security without disrupting user experience. These systems analyse how customers interact with their devices — keystroke patterns, touchscreen behaviour, and mouse movements — to differentiate between legitimate users and fraudsters. Using AI-powered monitoring, businesses can detect anomalies beyond the capacities of traditional security.

Safeguarding payments

As digital payments become the norm, securing transactions across multiple channels is critical. Fraud prevention strategies should include real-time transaction monitoring, tokenisation to protect payment credentials, and Multi-Factor Authentication (MFA) for high-risk transactions. Scammers are increasingly using artificial intelligence to conduct sophisticated frauds, necessitating heavy investments from financial institutions to combat fraud.

Unified fraud detection systems

Fragmented security measures create blind spots that fraudsters exploit. By integrating cross-channel fraud detection — online, mobile, in-store, and call centres — businesses gain a 360-degree view of customer activity. AI-driven systems can analyse data across these touchpoints in real time, identifying suspicious patterns and preventing fraud before it occurs. For example, a global leader in digital payments has established a new initiative aimed at detecting and dismantling online scammers to protect customers, addressing the growing scam ecosystem.

Strengthening identity verification

Fraudsters often exploit weak identity verification protocols to create fake accounts or hijack existing ones. Strengthening verification measures with biometric authentication and risk-based authentication ensures that only legitimate users gain access. These technologies analyse risk factors like device history and geolocation to detect threats. A major e-commerce company launched palm-based payments at a global supermarket chain, enhancing security and convenience.

Breaking down data silos for holistic protection

Data silos hinder fraud detection efforts by preventing teams from identifying patterns across different touchpoints. A unified fraud prevention strategy requires seamless data sharing between departments, allowing cross-channel fraud detection. AI and machine learning models process this integrated data to refine detection strategies and enhance predictive capabilities. New AI tools sold on the dark web allow money launderers to bypass human verification on cryptocurrency exchanges, highlighting the need for integrated and advanced fraud detection systems.

The role of AI and machine learning in omnichannel security

AI and ML play vital roles in enhancing omnichannel fraud detection. These technologies can:

- Analyse large datasets to detect fraud patterns in real time.
- Differentiate between legitimate users and fraudsters using behavioural biometrics.
- Automate risk assessment to apply appropriate security measures based on transaction risk.
- Continuously improve detection models based on emerging fraud trends.

Machine learning models are particularly effective in identifying anomalies, reducing false positives, and predicting fraudulent behaviour before it escalates. As fraud techniques evolve, AI-driven systems adapt, offering businesses a dynamic defence against threats.

Best practices for omnichannel fraud risk management

To ensure security across all touchpoints, businesses should follow these best practices:

- Integrate fraud detection across all channels to ensure visibility into suspicious activities.
- Use behavioural biometrics to identify unusual patterns in user interactions.
- Employ device fingerprinting to detect fraudsters using multiple accounts from the same device.
- Conduct continuous fraud monitoring and analysis to refine detection strategies.
- Foster collaboration between departments to share insights on emerging threats.
- Invest in AI and automation to strengthen fraud detection capabilities.

The future of omnichannel fraud detection

Innovation continues to redefine the battlefield. Blockchain, for instance, is being piloted to create immutable transaction logs, reducing chargeback fraud. Meanwhile, quantum computing promises to supercharge ML models, though it also risks making current encryption obsolete — a double-edged sword.

Another frontier is the metaverse. As virtual reality shopping gains traction, fraud detection systems will need to authenticate digital avatars and monitor in-world transactions. Forward-thinking firms are already experimenting with AI that analyses voice patterns and virtual gestures to verify identities.

The rise of generative AI is projected to greatly increase the risk of fraud. As criminals wield deepfakes, quantum computing, and social engineering with ever-greater finesse, fraud detection systems must evolve, too. A growing number of global enterprises will embrace fully integrated omnichannel solutions driven by AI advancements and increasing regulatory demands. For decision-makers, the time to act is now — before the next big fraud hits.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next