EVENT PROCEEDINGS REPORT

Sponsored by: Callsign

Good is no longer good enough when it comes to fraud identification and detection, especially with customer identity and authentication. Excellence is now table stakes against identity fraud. Digital identity for financial institutions and the challenges and approaches of balancing customer experiences and mitigating fraud are goals for all.

Reinventing Customer Experience with Effective Fraud Control

November 2022

Written by: Ganesh Vasudevan, Research Director; Surya Narayan Saha, Research Manager, Financial Insights

Introduction

This IDC Event Proceedings report captures key takeaways from an exclusive fireside chat between IDC and Callsign on the evolving fraud environment and the need for adaptive fraud control practices. The fireside chat was held during IDC India Virtual Conference, Digital Threshold to Reinvention, on September 6, 2022. Attendees of the event included senior business and IT decision makers from leading financial organizations in India.

In this conversation, Namrata Jolly, general manager Callsign Asia/Pacific (a leading digital identity provider that helps prevent fraud and improve customer experience of the world's largest financial institutions), shared her perspective on fraud control and the need for a holistic customer-centric fraud prevention strategy.

Financial institutions (FIs) in India are increasingly recognizing the need to holistically manage fraud risk. This means having the ability to understand a customer's identity, activity, and behavior across channels and lines of business. The introduction and expansion of real-time payment schemes, such as unified payments interface (UPI), immediate payment service (IMPS), or real-time gross settlement (RTGS), have further accelerated the need for FIs to pursue an enterprise fraud management strategy. In addition, forward-looking FIs view fraud management as an important component of managing customer experience.

AT A GLANCE

ONLINE AND CARD FRAUDS IN INDIA

- 90% increase in card and internet banking–related frauds the first quarter of FY22-FY23
- INR1 million daily average impact of fraud on banks during FY20-FY21
- Time-lag in fraud detection - 93.73% of the frauds in 2021-2022 by value occurred in previous financial years
- 87% increase in phishing incidents during FY20-FY21
- 30% increase in the amount involved in card and internet banking–related frauds during the FY21-FY22

SPEAKERS

- Ganesh Vasudevan, Research Director, IDC Asia/Pacific Financial Insights, as moderator
- Namrata Jolly, General Manager, Callsign Asia/Pacific

How Big of a Problem Is Identity Fraud?

The Reserve Bank of India (RBI) categorizes fraud incidents along the operational areas. Card and internet frauds arising out of identity compromise rank very high in terms of the volume of fraudulent incidents across banks. As per the RBI data, over 60% of the total number of fraud incidents during FY21-FY22 is owing to identity-related exceptions in ATM/debit cards, mobile and electronic banking, and credit cards. The types of identity fraud include application (new account) fraud, account takeover fraud, customer identity theft, and business identity theft, which is usually a business insider theft.

India banks have already recorded more than a 90% increase in card and internet-related frauds during the first quarter of current FY22-FY23 (see Figure 1).

FIGURE 1: ***Online and Card Fraud Incidents***

Number of Frauds Reported by Banks (2019- Q1 FY23)

Number Of Frauds Reported by Banks (2019- Q1 FY23)

Banks	Reported Fraud
2019-20	2,677
2020-21	2,545
2021-22	3.596
Q1 FY 2022-23	6,855

Source: RBI

This exponential increase in fraudulent transactions is a matter of great concern for all the banks, and the regulator (RBI) has made its intent to control fraud quite explicit and clear through various directives. As per the RBI, all regulated entities shall document and implement the configuration aspects for preventive and detective types of controls based on user behavior. It also encourages the adoption of adaptive authentication mechanisms to select the right authentication factors depending on risk assessment and user risk profile and behavior.

Challenge

Creating smooth, frictionless, and engaging digital experiences is a top priority for most FIs. Financial institutions, regardless of size, suffer from a certain amount of bringing nondigital processes online, including the onboarding of new customers, credit account applications, and digital identification. Digital identity and fraud applications are central elements to the customer journey, and thus the need to deliver the customer experiences that consumers expect from FIs. The risk of not fully transforming digital identity and fraud applications to support customer-facing applications is that the goal of creating frictionless customer experiences will not be fully achieved, potentially putting FIs at a competitive disadvantage. The key challenge for FIs is establishing a layered approach of identity management and fraud detection tools to effectively manage fraud across channels and lines of business.

Key Themes and Insights that Emerged during the Fireside Chat

The fireside chat reiterated the understanding that identity is to be centered on a robust and secure verification process with a happy long-term customer experience. Namrata Jolly, general manager Callsign Asia/Pacific, emphasized upon the three key takeaways for FIs in achieving balance between fraud control and customer experience.

» Changes in Regulation

Regulatory bodies across the world are reviewing existing regulations and updating guidelines to help organizations tackle evolving fraud threats and meet changing customer expectations. RBI, through its Master Direction on Digital Payment Security Controls in 2021, reinforced the need for strong customer authentication (SCA) using additional levels of authentication, such as adaptive authentication involving risk assessment, user profiling and other behavioral traits.

The RBI guidelines suggest FIs to validate factors, such as IP location and behavioral biometrics, to help detect suspicious activity from genuine users, as well as adaptive authentication to select the right authentication factors depending on risk assessment and user risk profile and behavior. To achieve this, organizations need to look beyond existing methods, such as SMS one-time passwords (OTPs), to ensure they meet regulations and keep customers happy with frictionless and passive forms of authentication.

» Changes in Fraud Types

Fraud threats are evolving, with phishing and online scams on the rise. The challenge with these threats is that they utilize the very same technologies that are often used to authenticate customers, to manipulate them into handing over access to their accounts or transferring funds. Reliance on methods, such as SMS OTPs and passwords, not only provides a cumbersome experience for customers but is also more susceptible to man-in-the-middle and rogue application malware attacks exposing the risk of account takeover, remote access, and other online scams.

To better tackle such digital threats, a more holistic and layered approach to fraud prevention is needed — one that combines threat intelligence with behavioral biometrics and other data to detect the genuine user as well as signs of fraud.

» Changes in Customer Expectations

Fraud control measures in FIs are conventionally straitjacketed. Everyone goes through almost the same iterations or hoops to prove themselves, which is quite inefficient and cumbersome to the customer experience. This highlights the need for introducing friction by design as an architecture principle for fraud controls. Financial institutions should be able to bring in checks and controls in their online services only as and when it is truly essential.

Part of the reason for unwieldy online authentication is the porting of physical processes to digital channels. Many of the existing identity checks are replications of physical processes, simply digitized. These processes are not refined and redesigned for digital channels, such as again the SMS OTP being used to validate identity. To help improve both digital experiences and reduce fraud, organizations should consider fraud solutions designed for digital and online customer journeys and unobtrusive to the user.

New Digital Identification Technologies

Using new digital identification technologies is the most effective and efficient way for FIs to mitigate fraud. New technologies include behavioral biometrics and dynamic intelligence to help FIs mitigate loss and build a comprehensive enterprise risk program. Callsign's capabilities differentiate itself based on its expertise around the two important elements of digital identification technology — intelligence engine and orchestration layer.

» Intelligence Engine

Using advanced machine learning (ML) techniques, Callsign positively identifies users by their unique characteristics, replicating real-life recognition signals with artificial intelligence (AI) models. Using deep learning (DL) techniques, combining event, threat, and behavioral analytics with multifactor authentication to provide risk intelligence in real time, helps organizations protect themselves against a range of evolving threats. Callsign's device fingerprinting capability uses noncookie-based technology to create a deep, persistent device fingerprint for authentication and fraud detection purposes.

Callsign's unique Muscle Memory Technology – the highest-fidelity form of behavioural biometrics, covers both web and mobile. Passively analysing aspects such as user's typing patterns (such as speed and cadence), the way they hold their device, and the way in which they swipe ensures that the genuine. If there is doubt or signs of malicious intent, the organization can opt to further authenticate the user, or block the transaction. These policy decisions can be built and managed within the orchestration layer.

Callsign's device fingerprinting – By simultaneously checking for signs of fraud or malicious activity (such as malware, remote access sessions and bots) alongside confirmation that the user is who they claim to be and is authorized to access the account (protecting against scams and account takeover activities) organizations able to have a higher degree of protection.

» Orchestration Layer

The second important element of modern identity verification is the orchestration engine. The orchestration layer supports banks in their risk policy management, helping them build seamless customer journeys by uniting systems and technologies to provide a 360-degree view of the customer across web and mobile channels.

Using low- / no-code GUI, policies can be quickly and easily built and edited eliminating the need for costly and time-consuming IT change projects. Whilst new authenticators can be quickly and easily deployed, allowing organizations to test and analyse journeys, ensuring that the balance between security and usability is met.

Callsign's orchestration layer allows organizations to meet the evolving demands of their digital landscape, providing the ability to meet changing regulations while both mitigating risk and improving customer experiences.

Within Callsign's orchestration layer, dynamic interventions can be configured. These interventions use real-time intelligence to provide contextual, personalized, fraud warning messages to consumers. This can protect them against social-engineering scams, in particular ***authorized push payment (APP).***

Conclusion

The key to an effective fraud management capability is being able to layer and integrate intelligent technology solutions across channels and lines of business. Financial institutions' ecosystem of identity and fraud point solutions across lines of business is like a house half built, without any blueprints. Enlisting the services and products of a technology provider with a comprehensive, identity and fraud platform is an important first step. A technology provider with an intelligent platform will be able to connect to existing point solutions in place across channels and complement them to effectively "complete the house."

About the Analyst

Ganesh Vasudevan, Research Director, Financial Insights

Ganesh Vasudevan is the research director for IDC Financial Insights based in IDC's office in Mumbai, India. He is responsible for creating and maintaining research programs, as well as leading custom engagements for financial services institutions in India and across the Asia/Pacific (AP) region. His key research coverage includes retail and commercial banking, branch and alternate channels, payments, and risk management.

Surya Narayan Saha, Research Manager, Financial Insights

Surya Saha is a research manager for IDC Financial Insights and is responsible for research in the banking, financial services, and insurance (BFSI) segment. His research covers insurance, banking, and payments, blockchain technology, digital transformation (DX), and other related emerging technology areas for the financial services industry.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Centre for Consultancy and Research Pvt. Ltd

Unit no.221-223, Vipul Plaza, 2nd Floor, Sector 54, Golf Course Road, Gurgaon Haryana 122002

T +91-1244762300

Twitter @IDC

idc-insights-community.com

www.idc.com