Security and Risk Management Leaders' Guide to Online Fraud Detection and Identity Proofing

Published 14 March 2022 - ID G00762737 - 7 min read

By Akif Khan

Knowing whom you're dealing with online and ensuring the integrity of those digital interactions is critical. Security and risk management leaders should use this research to guide their technology and strategy choices related to online fraud detection and identity proofing.

Analysis

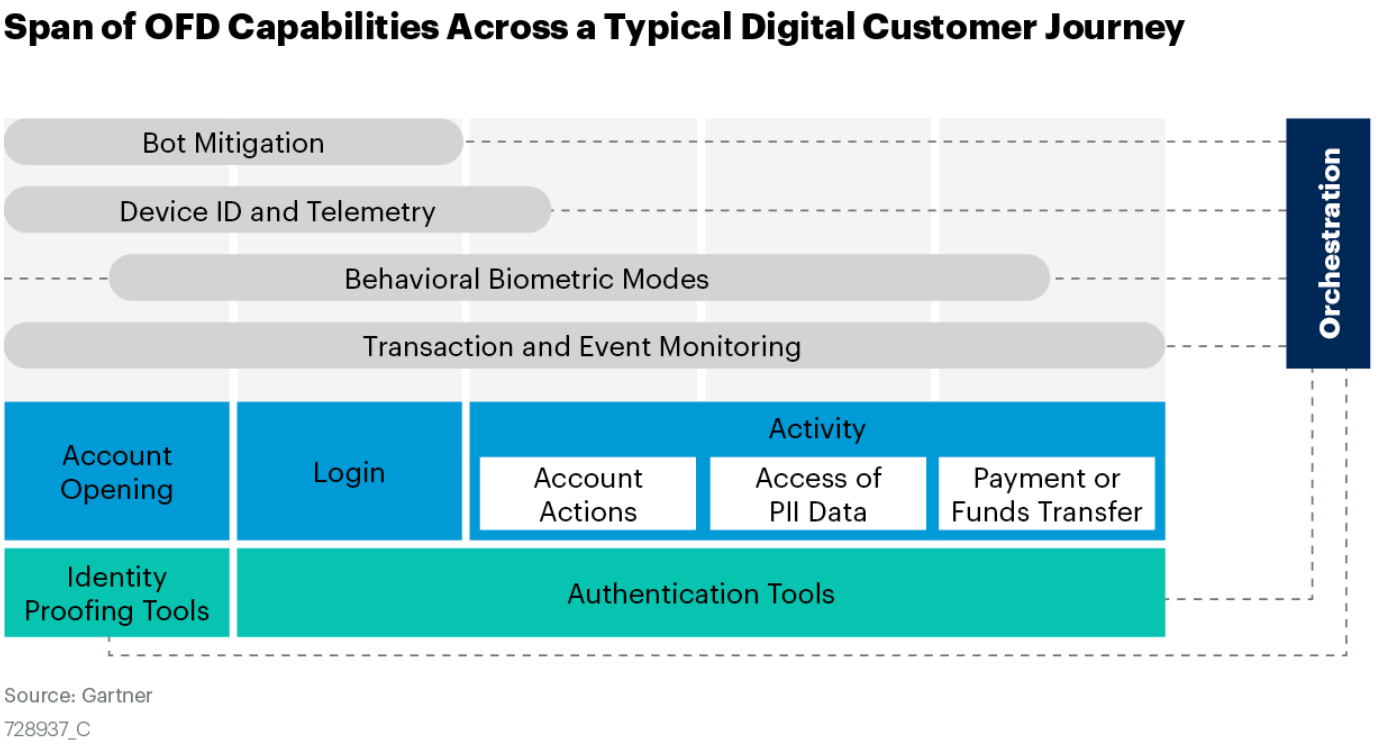
Digital and remote interactions, whether they are in a business-to-consumer (B2C) or a workforce context, present a number of risks to organizations. These risks broadly apply to three key aspects of the user journey:

- **Account opening —** The use of fraudulently obtained identity data to register for services and open accounts. This could include the use of an entire set of stolen identity data, or using snippets of stolen identity data to commit synthetic identity fraud. Examples of abuse include:
  - Subverting the know-your-customer, due-diligence process when opening a bank account
  - Opening multiple digital commerce site accounts to obtain promotional discounts
  - Contractors or gig workers using fraudulent identities to apply for work
- **Account login —** Accessing an account belonging to someone else for illicit gain. Motivations could include simply checking that credentials are valid before testing them elsewhere, and workers providing access to their business accounts to outsource work or carry out account activity.
- **Account or transaction activity —** This is a broad area, in which fraudulent activity could be taking place once logged into an account, or simply as a stand-alone activity, such as a guest check-out scenario in digital commerce. Examples include access to and theft of personally identifiable information (PII), transferring funds, making purchases using stored value or payment instruments,

using fraudulent payment instruments, theft of loyalty points, or gathering information about linked accounts.

The fraudulent activities listed above could be carried out by human users or by automated bots at the point of attack, and the proportions vary across organizations and use cases. Figure 1 shows the convergence between online fraud detection (OFD), identity proofing and authentication capabilities across a digital user journey, and the typical layers needed for an effective OFD strategy.

Figure 1: Span of OFD and Identity Proofing Capabilities Across a Typical Digital User Journey



Managing fraud rates must be balanced against the impact on the user experience (UX) and the cost. Organizations have different tolerances to false positive rates (good users being mistakenly blocked); the rate at which high-risk users are subject to additional authentication measures; and the financial costs (technology, operational and HR) involved in mitigating fraud.

Security and risk management (SRM) leaders responsible for fraud detection and identity proofing should refer to the following research to understand technology and market trends, develop organizational management strategies and/or choose among options to meet technology needs.

Research Highlights

Some recommended content may not be available as part of your current Gartner subscription.

The Online Fraud Detection Market

Detecting fraud in digital channels remains a critical challenge for most organizations, notably those focused on banking and digital commerce. In banking, opportunities present themselves to rationalize the technology stack for fraud prevention, as vendors increasingly evolve from point solutions to platforms. In digital commerce, fraud detection vendors are increasingly differentiating themselves by expanding their applicability to other revenue-affecting use cases, such as policy abuse. As explained in the Market Guide for Online Fraud Detection, the convergence of fraud detection, identity proofing and authentication represents an opportunity for a comprehensive approach to securing digital channels. The orchestration of these complementary activities is a strategic consideration, with many vendors now offering a range of orchestration capabilities.

Creating a Fraud Strategy and Selecting Appropriate Vendors Is Challenging

In a crowded market of vendors with overlapping capabilities, organizations find it challenging to select appropriate vendors. A common failing in many organizations is lack of engagement with all of the appropriate internal stakeholders to create a fraud strategy at the organizational level that aligns with business requirements. (See Figure 2 and How to Create a Payment Fraud Detection Strategy at the Organizational Level.) Such cross-functional alignment lays the groundwork for defining relevant key performance indicators (KPIs). These KPIs can be used to assess the current state, as well as what is required of vendors as part of an RFP. These and other RFP best practices that lead to vendor responses which enable differentiation are described in Best Practices for Better Online Payment Fraud Detection RFPs.

Figure 2: Leadership Is Required to Align Cross-Functional Stakeholders

Leadership is Required to Align Cross-Functional Stakeholders

Source: Gartner
762737_C

Gartner

Best Practices for Vendor Selection in Banking

Unsurprisingly, banks rank among the most targeted of organizations by fraudsters. Transaction monitoring platforms designed to screen high volumes of payment transactions across different banking products and channels represent a strategic investment. With many banks having disparate solutions deployed for different products and event types, resulting in inefficient siloed fraud screening, SRM leaders in banks must focus on consolidating fraud detection across products and channels. The market is also moving toward fewer on-premises deployments and a greater focus on public cloud and vendor-hosted deployments. Creating an RFP that presses vendors to explain the breadth of their capabilities can help differentiate during vendor selection (see Buyer's Guide for Fraud Detection in Banking and Tool: RFP Questionnaire Template for Fraud Detection in Banking).

Fraud Detection and a Good UX Need Not Be Mutually Exclusive

A common casualty of fraud detection is UX. Onerous multifactor authentication (MFA) for all users and false positives resulting in good users unable to access services are all too common. With UX now a critical differentiating battleground in the digital business environment, fraud detection teams are working far more closely with UX teams to ensure needs are balanced. Layered approaches involving bot mitigation, device profiling and behavioral biometric technologies allow UX to be tailored according to risk levels. Dynamic assessment of risk and trust signals and an adaptive approach to authentication enable the selective and intelligent application of friction appropriate for the action that the user is attempting (see Don't Treat Your Customer Like a Criminal).

The Contact Center Remains a Fraud Achilles' Heel for Many Organizations

Although digital channels get the most focus in this era of digital transformation, many organizations still rely on voice channels via their contact centers as part of their omnichannel offerings. Fraud controls in contact centers often consist of little more than knowledge-based verification. Organizations must deploy a layered defense of identity proofing, fraud detection and authentication capabilities, closely coupled with tighter integration into cross-channel fraud detection systems (see Quick Answer: How Do You Reduce Fraud in the Contact Center (Phone) Channel?).

The Evolution of Trust and Safety Teams

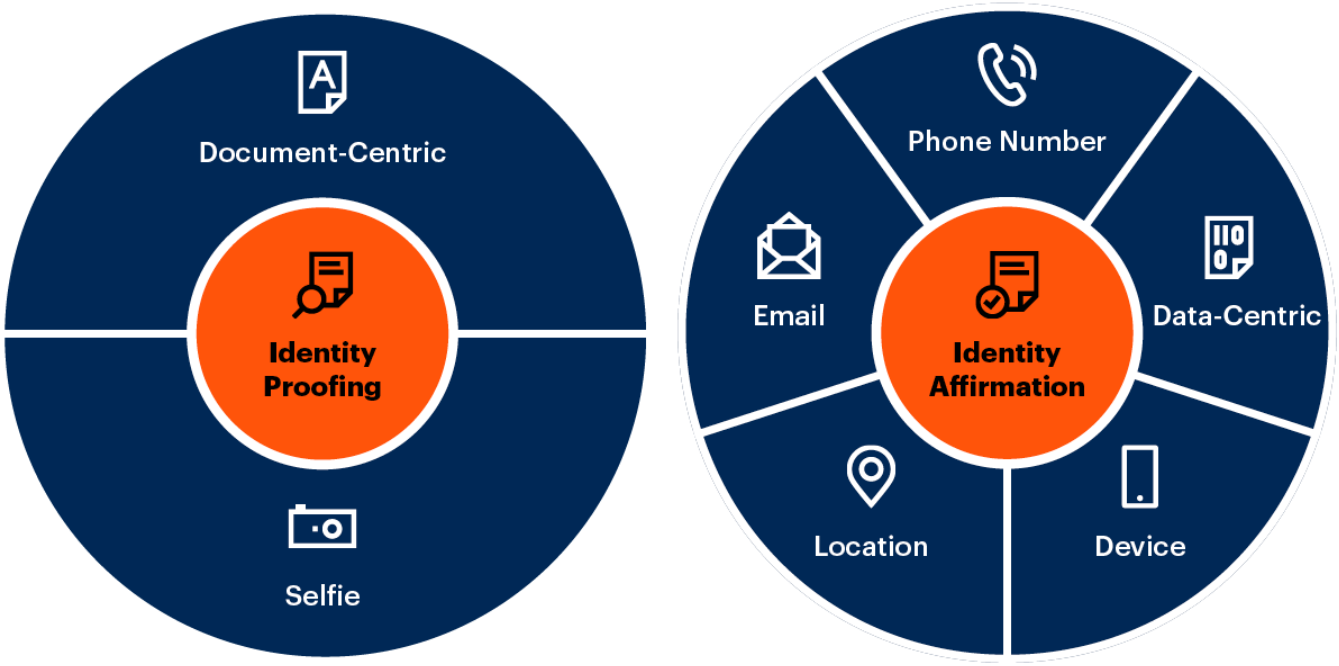
In many organizations, fraud detection is now seen as a component of a broader strategy around trust and safety. More than just rebranding the fraud team, trust and safety teams focus on securing interactions wherever the customer meets the brand (see Create Trust and Safety on the internet). A key tenet of this approach is deep collaboration with the customer experience teams, as well as securing interactions across a range of interfaces, such as email, social media, reviews and comments forums, as well as the supply chain.

The Identity Proofing and Affirmation Market

Identity-first security principles are built on the initial establishment of trust in a real-world identity claim. SRM leaders must balance assurance needs with optimizing UX, while orchestrating multiple tools and carefully selecting vendors from a crowded market (see Market Guide for Identity Proofing and Affirmation). Fraud detection and identity affirmation capabilities are typically deployed alongside identity-proofing processes to mitigate risk (see Figure 3). In many cases, identity proofing is a regulatory requirement that is often used as part of a broader know-your-customer process, such as in financial services. Identity proofing is also used as a fraud mitigation capability, such as when citizens claim benefits from government sites.

Figure 3: Identity-Proofing and Affirmation Capabilities

Identity Proofing and Affirmation Capabilities



Source: Gartner
755371_C

Gartner

Best Practices for Vendor Selection in Identity Proofing

The market of vendors offering identity proofing (aka the “ID plus selfie” process) has become crowded, with both global and regional solutions. Finding differentiation among vendors is challenging. SRM leaders should follow a structured approach to define their business drivers, use cases and roadmaps (see Buyer’s Guide for Identity Proofing). Creation of an RFP that examines the full extent of features and capabilities will ensure investment in a solution that provides value for money and meets strategic requirements (see Tool: RFP Questionnaire Template for Identity Proofing).

CIAM Platforms Should Simplify the Use of Fraud Detection and Identity Proofing

Stand-alone fraud detection and identity proofing solutions that need to be integrated into existing access management systems for account opening and account takeover use cases have been purchased by many organizations. However, as the adoption of customer identity and access management (CIAM) solutions continues across many industries, the opportunity for simplification presents itself. Some CIAM solutions now have fraud detection and identity proofing components as part of their core offering (see Innovation Insight for Customer Identity and Access Management). In some cases, these are native offerings. In others, they are part of a curated “marketplace” of partners

that can be easily enabled. Leveraging such CIAM platforms can greatly reduce the time, cost and complexity of deploying effective fraud detection and identity proofing.