VISA

Visa Consulting & Analytics (VCA)

Fight fraud with leading-edge strategies to stay ahead of complex threats

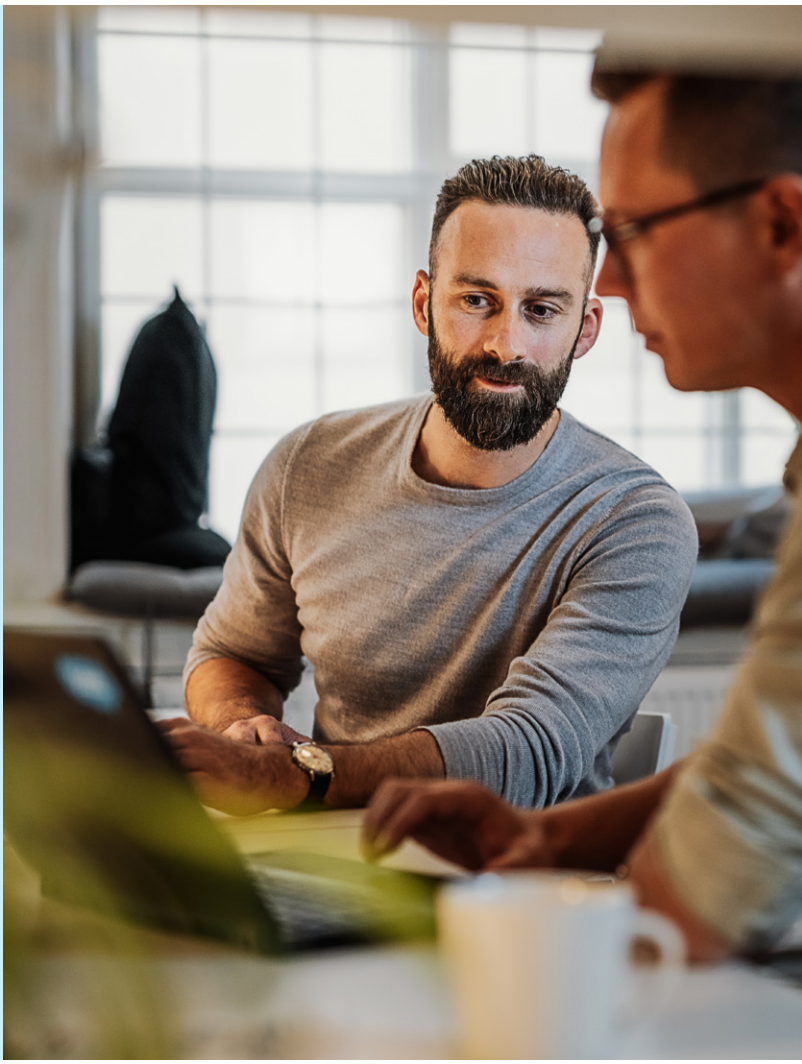
A guide for financial institutions combatting online fraud

Security protocols around online digital-payments infrastructure continue to advance and strengthen. As a result of more sophisticated guardrails, financial cybercriminals are shifting their efforts towards a slightly more penetrable landscape: application fraud and identity theft. Compared to transactional fraud, online application- and identity-related fraud can pose greater risk to financial institutions (FIs) and to their customers.

In this deep-dive into the next key influencer in payments this year, Visa payments advisors share their expert insights on the rapidly evolving online-fraud landscape, overview various risk typologies, and outline tactical risk-mitigation considerations for FIs.

Due to several factors—like market maturity, different levels of model availability globally, and minimal recourse to recoveries—application fraud and identity theft are on the rise. Application fraud involves the use of stolen credentials or false information by "threat actors" to apply for or enroll in financial services.

Threat actors typically approach FIs applying for credit, which contributes to an increase in identity theft events, because obtaining credit allows them to access funds and valuable resources under false identities. This exploitation of credit systems enables fraudsters to make unauthorized purchases, withdraw cash, or commit other financial crimes before the fraud is detected. Manifesting itself in the form of either first-party or third-party fraud, the threat from application fraud is expected to grow rapidly, particularly as the payments-industry continues implementing and embracing digital-acquisition models.



Surveying cybercriminal tactics: application fraud, identity theft, and online data scams

Cybercriminals are dominating the threat landscape for application fraud and identity theft using sophisticated tactics such as stealing personal information through various online scams, creating fake identities, and exploiting artificial intelligence to manipulate data. Online marketplaces on illegal websites play an increasingly significant role, as cybercriminals buy and sell consumer data. The availability of this stolen information makes it easier for attackers to create convincing false identities and commit fraud across various platforms.

	North America & Latin America	Asia Pacific	Europe and CEMEA
Average Fraud Rate	6.2%	6.8%	3.4%
Most fraudulent document type	Driving License	Indian Tax ID	National ID Card

244%

Year-over-year increase in digital document forgeries

40%

Deepfakes used for biometric fraud in 2024

Source: Entrust Cybersecurity Institute, 2025 Identity Fraud Report: https://www.entrust.com/resources/reports/identity-fraud-report

Why the surge in application fraud and identity theft is a growing concern for FIs

Three main implications for FIs

Increased identity theft fraud

External data breaches and compromise events are leading to a rise in identity theft fraud, often orchestrated by organized crime syndicates. This results in more fraudulent applications being submitted to FIs.

Higher credit losses due to undetected application fraud

Many FIs are struggling to detect a substantial amount of application fraud. This undetected fraud is often absorbed and obscured as credit losses, impacting risk management efforts.

Digital lending due diligence challenges

The rapid growth of digital lending has made it difficult for FIs to perform robust due diligence. This challenge hampers their ability to implement effective straight-through processing, making it easier for fraudulent applications to slip through the cracks.

The advent and widespread adoption of digital banking further exacerbate these risks. While digital banking platforms provide convenience and accessibility to legitimate users, they also make it easier for fraudsters to engage in identity theft, application fraud, and exploit weaknesses through online scams. This amplifies the challenges faced by financial institutions in detecting and preventing fraudulent activities. The nature of digital transactions and the vast amount of personal information accessible online often make it easier for fraudsters to commit cybercrimes with greater impact and anonymity.

The taxonomy and modus operandi (MO) of application fraud

Application fraud is a pervasive global issue affecting FIs as they expand their digital offerings and outreach. Fraudsters swiftly adapt to preventative measures, employing various malicious techniques to perpetrate application fraud. Understanding the taxonomy of application fraud is critical to effectively identify, mitigate, and prevent financial losses.

Three main types of application fraud

First-party fraud

Individuals or entities misrepresent their personal information as part of an application or transaction request with the intent of committing fraud.

The typical MO includes:

- Fraudulent financials
- False information
- Collateral fraud
- Employment fraud

Third-party fraud

A third party takes a victim's identity and/or details without their knowledge, or creates a new identity using stolen credentials, with the purpose of perpetrating fraud.

The typical MO includes:

- Stolen identity
- Synthetic identity
- Mixed identity
- Fake/set up companies

Collusion fraud

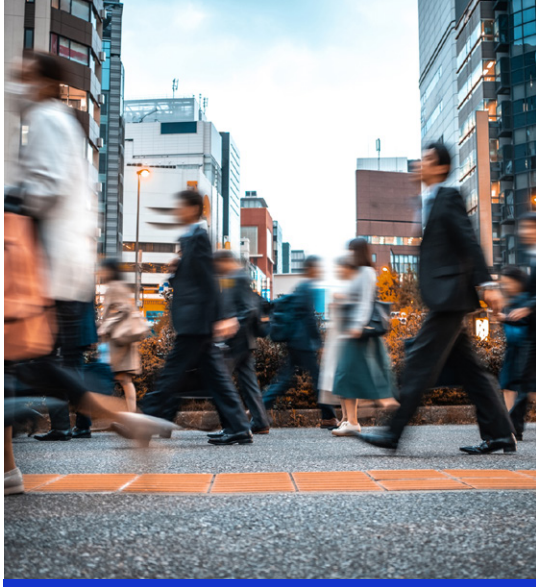
Individuals allow their identities or accounts to be used for fraud, acting in collusion with criminal syndicates or employees of FIs (e.g., sales agents).

The typical MO includes:

- Employee collusion
- Syndicate fraud
- Complicit money mule

Each of these three fraud types can be highly diverse in terms of MO and techniques. So, they present very distinct risks and impacts for FIs institutions across different geographies. Let's consider each of them individually:

	First-party fraud	Third-party fraud	Collusion fraud
Common variations and techniques	**Income inflation and asset misrepresentation:** misstating income or assets to qualify for higher credit limits or loans **Bust-out fraud:** establishing creditworthiness over time before maxing out credit limits and defaulting **Address manipulation:** providing incorrect addresses to evade detection or facilitate subsequent fraud **Mule accounts:** opening accounts using legitimate credentials but intending to launder illicit funds	**Identity theft:** using stolen credentials (e.g., social security numbers, passports, national IDs) to open fraudulent accounts **Synthetic identity fraud:** creating fake identities by combining real and fabricated data elements to bypass risk controls **Deepfake and AI-powered attacks:** using generative AI to spoof biometric authentication and impersonate real individuals **Cross-border fraud:** using stolen identities from one region to apply for credit in another country with weaker identity verification controls	**Straw borrowers:** applying for financial products on behalf of another individual to circumvent creditworthiness checks **Friendly fraud:** legitimate account holders falsely claim fraud or identity theft to dispute transactions and avoid repayment **Mule accounts and money laundering**: individuals allow their accounts to be used to receive and move illicit funds **Collusion with organized crime:** in some regions, second-party fraud is coordinated by fraud rings that manipulate account holders to facilitate schemes
Risks and impact across geographies	**Developed markets:** fraudsters exploit gaps in credit history data, misrepresenting financial history to access credit **Emerging markets:** with alternative data used for underwriting (e.g., mobile payments, digital lending, etc.), fraudsters fabricate digital identities to manipulate lending models **Regions with strong privacy regulations:** in regions like Europe, institutions may struggle to verify financial claims due to limited data-sharing capabilities	**North America:** synthetic identity fraud continues to be a major issue due to reliance on static data like social security numbers **Europe and Asia:** identity theft-related fraud is prevalent due to extensive digital banking ecosystems and government ID integrations **Africa and Latin America:** alternative credit data (e.g., telecom data, digital wallets) is exploited for fraud as financial systems expand **International money movement:** stolen and synthetic identities are used to open accounts for illicit fund transfers	**Regions with low levels of financial literacy:** individuals may unknowingly have their accounts used for money laundering activities without realizing the consequences. These accounts are often referred to as "mule accounts" **High-risk jurisdictions:** areas with high corruption rates or limited enforcement see straw borrower schemes used for credit fraud and tax evasion **Digital-first economies:** fraudulent activities are increasing due to the ease of online disputes and the misuse of refund mechanisms in e-commerce and digital lending



Key challenges for FIs

Owing to its inherent nature, application fraud poses several distinct challenges to FIs when compared to transactional fraud. Some of them include:

One-shot prevention opportunity

Unlike transactional fraud, application fraud must be detected at the initial application stage, offering only one chance for prevention

Limited off-the-shelf risk models

Institutions often lack ready-to-use models for detecting application fraud, necessitating custom solutions

Higher ticket size losses

Application fraud often involves larger financial losses compared to transactional fraud

Lack of sophisticated platforms

Many institutions lack advanced tools for detecting and analyzing application fraud

Minimal recourse to recoveries

Recovering funds lost to application fraud is challenging, emphasizing the need for prevention

Sub-optimal list management

Effective fraud prevention requires well-maintained lists of known fraudsters, which many FIs struggle to manage

Lack of subject matter expertise

Specialized knowledge is needed to combat application fraud, which many FIs may lack

Risk/loss quantification limitations

Assessing the risk and potential losses from application fraud accurately is difficult, complicating resource allocation and prevention efforts

Due to the inherent limitations in terms of expertise, risk scores, platforms, list management and the potential difficulty in recovering funds, combating application fraud requires more intricate layers of controls than is the case with transactional fraud.

How FIs can strengthen defenses against application fraud

As fraud evolves with advancements in AI, digital identity solutions, and financial technology, each of the three fraud types outlined above presents distinct challenges requiring tailored strategies for effective prevention and risk mitigation. FIs are advised to implement multi-layered defenses, fraud intelligence sharing, real-time monitoring, and other measures to prevent financial losses.

Examples of effective mitigation and control layers

Pre-acquisition controls

Multi-layered identity verification

- Verify customer identity using government-issued ID documents
- Utilize digital ID proofing, biometric authentication, and behavioral analytics
- Combine biometrics, device intelligence, and machine learning (ML) driven risk scoring

Income validation

- Authenticate submitted income documents for legitimacy from independent sources

Intelligence repository

- Cross-reference applicant information with known fraud databases and participate in industry-wide fraud prevention networks
- Strengthen fraud intelligence sharing between financial institutions

Advanced credit modeling and real-time monitoring

- Use AI and ML to detect patterns indicative of fraudulent applications

Innovative technologies

- Analyze device information during the application process to identify suspicious devices or those associated with known fraudsters
- Identify high-risk patterns such as location inconsistencies
- Utilize ML to detect anomalies in application data and behavior

Post-acquisition monitoring

Transaction monitoring and early-warning indicators

- Monitor transactions in real-time for suspicious patterns or behaviors. Use AI/ML algorithms to detect anomalies
- Identify irregular repayment patterns, address inconsistencies, and synthetic identity traits
- Review First Payment Default (FPD) cases to determine instances of customer not found/contactable

Behavioral analysis and device intelligence

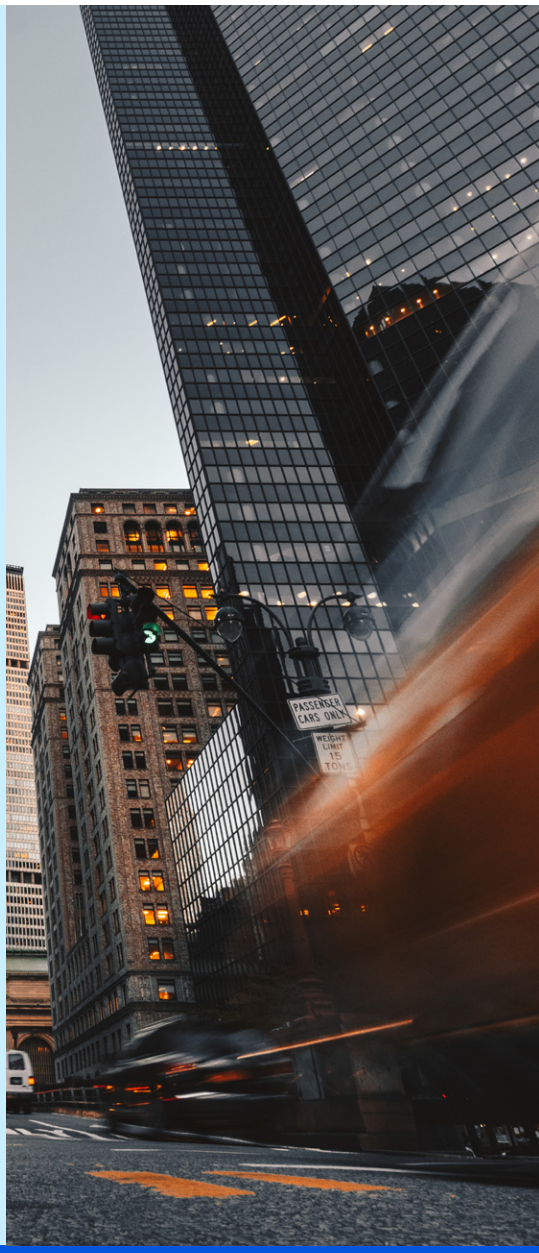
- Analyze customer behavior patterns over time, high-risk patterns, sudden changes in spending habits or account usage

Account activity reviews

- Periodically review account activities, especially for high-risk accounts
- Set triggers for manual reviews based on certain criteria

Continuous risk assessment

- Regularly update risk models based on new fraud trends and pattern; adjust parameters based on evolving threats
- Conduct customer awareness programs to highlight the risks and consequences of facilitating fraud



Understanding and learning from global best practices

At Visa Consulting & Analytics (VCA), we work with clients globally to help protect their portfolios from application fraud and identity theft. Typically, our recommended measures include a combination of tactical and strategic actions to identify unusual activities and pinpoint potential fraud, establishing a layered defense approach across the acquisition lifecycle.

Tactical Controls

- Intensify new client onboarding due diligence protocols
- Augment fraud prevention controls focused on digital channels
- Perform robust identity checks using advanced digital solutions
- Augment detection capabilities (e.g., with facial biometrics, liveliness checks, and independent database validations)

Strategic Controls

- Deploy a cutting-edge acquisition fraud detection platform
- Augment capabilities utilizing integrated case management, ML-based fraud risk scoring, and link analysis
- Implement advanced list management capabilities equipped with pioneering phonetic match algorithms

In all instances, speed is key. In a dynamic situation where fraudsters continuously probe for vulnerabilities in institutions, potential risks can quickly escalate with severe consequences.

How Visa can help

In the face of sophisticated application fraud risks, Visa has enhanced its capabilities by integrating Featurespace's advanced AI into its fraud prevention and risk-scoring offerings. This enhancement provides real-time detection of sophisticated fraud attacks, ensuring businesses stay safe without adding friction to the user experience.

Furthermore, VCA is ideally positioned to work with clients to assess risk vectors, potential impact, level of preparedness, and risk mitigation infrastructure, along with deployable strategies and the best methods for implementation. VCA's capabilities encompass performing comprehensive diagnostics of the client's current control environment, tailored to the threat landscape. This approach allows VCA to enhance its application fraud risk management strategy and framework to deliver optimal performance and future-proof risk mitigation.

Beyond advisory services, VCA provides risk solutions using a defense-in-depth model in the acquisition domain. These solutions complement the client's existing risk-mitigation capabilities, offering proactive risk management augmented with advanced prevention and detection strategies.

About Visa Consulting & Analytics

We are a global team of hundreds of payments consultants, data scientists and economists across six continents.

- Our consultants are experts in strategy, product, portfolio management, risk, digital and more with decades of experience in the payments industry.
- Our data scientists are experts in statistics, advanced analytics and machine learning with exclusive access to insights from VisaNet, one of the largest payment networks in the world.
- Our economists understand economic conditions impacting consumer spending and provide unique and timely insights into global spending trends.

The combination of our deep payments consulting expertise, our economic intelligence and our breadth of data allows us to identify actionable insights and recommendations that drive better business decisions.

To get started, reach out to your Account Executive directly. Learn more about the team, resources, and our data-backed insights on Visa.com/VCA, and follow the team on LinkedIn.

Forward-looking statements. This content may contain forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. Forward-looking statements generally are identified by words such as "believes," "estimates," "expects," "intends," "may," "projects," "could," "should," "will," "continue" and other similar expressions. All statements other than statements of historical fact could be forward-looking statements, which speak only as of the date they are made, are not guarantees of future performance and are subject to certain risks, uncertainties and other factors, many of which are beyond our control and are difficult to predict.

Third-party logos. All brand names, logos and/or trademarks are the property of their respective owners, are used for identification purposes only, and do not necessarily imply product endorsement or affiliation with Visa.

As-Is Disclaimer. Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The Information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required.