TEAM8™

FINTECH REPORT | FEBRUARY 2025

Fraud Exposed

An in-depth look at AI and other disruptive trends and technologies shaping the fraud landscape

AUTHORS

Rakefet Russak Aminoach
Managing Partner, Team8

Ronen Assia
Managing Partner, Team8

Alon Huri
Managing Partner, Team8

Galia Beer-Gabel
Partner, Team8

Hadar Siterman-Norris
Partner, Team8

Yoav Koren
Vice President, Team8

CONTRIBUTORS

Johan Gerber
Executive VP & Head of Security Solutions at Mastercard

Vick Panwar
Principal, Global Banking Strategy & Development at AWS

Laura Spiekerman
President and Co-founder of Alloy

Alex Pillow
Senior Director, Commercial Strategy at Moody's

Ron Shevlin
Managing Director/ Chief Research Officer at Cornerstone Advisors

Noam Izhaki
Co-founder and CEO of Ballerine

Roy Zur
Co-founder and CEO of Charm Security

Liran Amrany
Former JP Morgan Executive, Fintech founder, and Team8 Partner

Team8 is a global Venture-Creation and Venture Capital Fund that creates and invests in companies focusing on Cybersecurity, Data & AI, Fintech, and Digital Health. Team8's signature Venture-Creation model is designed to identify meaningful problems, create theses on potential solutions, and build and invest in innovative companies that tackle these challenges.

Team8 leverages an in-house multi-disciplinary team of more than 80 company-builders, together with a dedicated community of global C-level executives and thought leaders. We partner with world-class founders and work with them to increase their probability of success via a disciplined, repeatable process from inception through product-market fit, growth, and beyond. Team8's unique platform brings together specialized expertise across technology, go-to-market, HR, and strategy.

Team8's fintech practice is led by Managing Partners Rakefet Russak Aminoach (former CEO of Bank Leumi), Ronen Assia (co-founder of eToro), and Alon Huri (co-founder of NEXT Insurance), as well as Partners Galia Beer Gabel (ex-PayPal), and Hadar Siterman-Norris (ex-Mastercard). The leadership team has extensive experience in a range of domains, including banking, insurance, credit, payments, e-Commerce, cross-border trade, capital markets, digital assets, and wealth management.

To learn more about collaborating with Team8 as a fintech founder or early-stage company employee, or to join our growing network of industry partners, please email us at info@team8.vc

Table of **Contents**

Introduction

Fraud is a pervasive and evolving threat that impacts individuals, businesses, and governments worldwide. The financial losses are substantial, but the damage extends beyond monetary loss, affecting trust, reputation, and operational stability. According to some estimates, the cumulative merchant losses to online payment fraud globally between 2023 and 2027 will exceed $343 billion, reflecting both the scale of the problem and the urgent need for effective fraud detection and prevention strategies. To combat fraud, firms are expected to spend over $250 billion by 2031, up from $45 billion today.

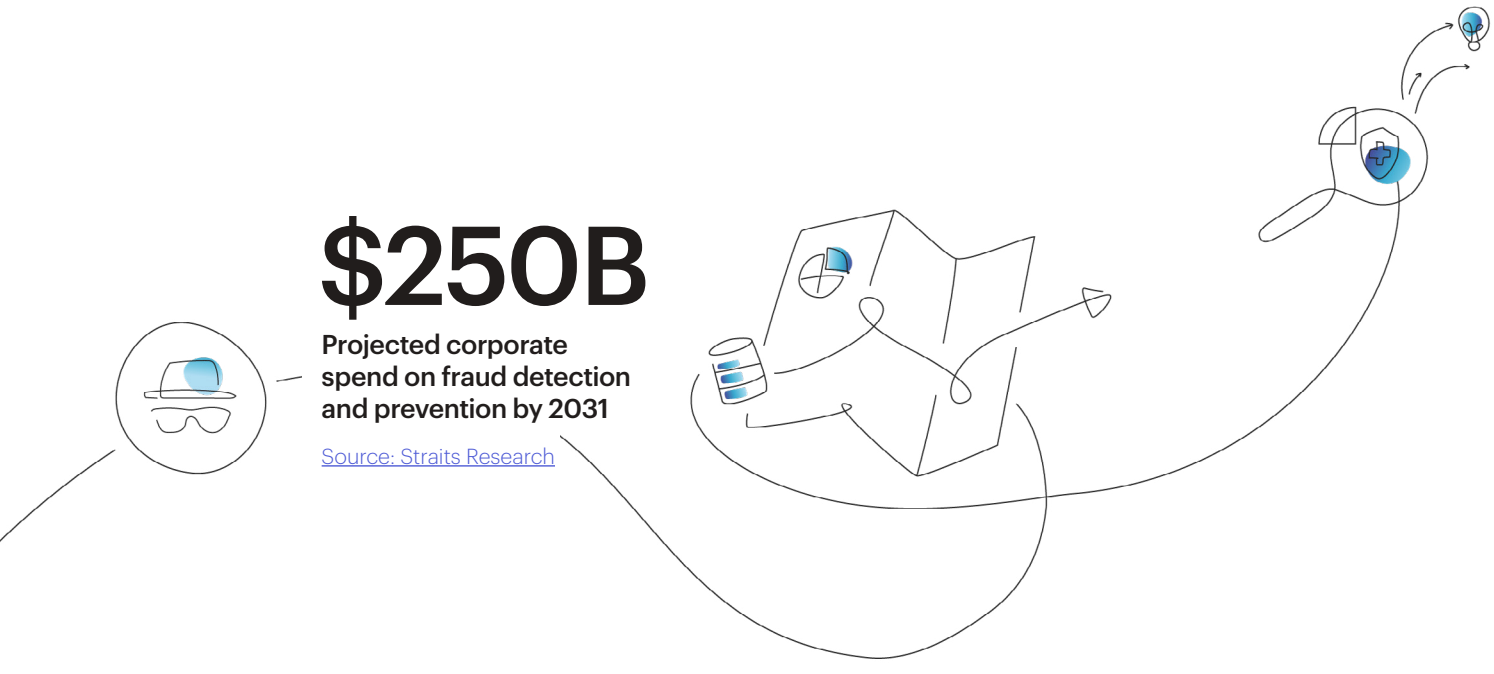
Advanced technologies like artificial intelligence and machine learning are crucial in detecting and preventing fraud. By processing data in real-time, these technologies can identify patterns and anomalies indicative of fraud, such as hidden correlations in transaction data or communication patterns suggesting phishing. In the following pages, we'll explore:

- **The evolution of fraud:** Technological progress and evolving financial systems have caused significant shifts in everything from traditional physical fraud to advanced cybercrime. This section will briefly cover significant milestones and shifts in fraud tactics over the decades.

- **Current trends and challenges:** Generative AI (GenAI) is playing a dual role in both enabling and combating fraud. Unfortunately for financial institutions and technology firms, fraudsters are often the first to leverage new technologies.

- **The future of fraud prevention:** The future of fraud prevention lies in a holistic approach that integrates multiple layers of defense, leveraging technology, enhancing employee training, and fostering collaboration across different sectors and industries.

This report will provide a detailed analysis of the methods used by fraudsters, the role of emerging technologies like GenAI, and the importance of robust regulatory frameworks.



$250B

Projected corporate spend on fraud detection and prevention by 2031

Source: Straits Research

Evolution of fraud

Fraud has existed in various forms since the advent of commerce, adapting quickly with new technological innovations. This section highlights key milestones and shifts in fraud tactics over the decades.

Early Digital Fraud

The transition from physical to digital transactions, and from offline to online communications, both marked a pivotal shift in fraud tactics. In the late 20th century, the advent of digital banking and e-commerce introduced new avenues for fraudsters. Early digital fraud primarily involved card-not-present (CNP) fraud and phishing scams, which became prevalent as online shopping grew. Similarly, the advent of email, SMS, and social media enabled new attack vectors and new forms of social engineering.

CASE STUDY

The eBay Phishing Scam (2003)

In one of the first major phishing scams, fraudsters sent emails purporting to be from eBay, directing users to a fake website to steal their login credentials. This scam affected thousands of users and demonstrated the effectiveness of social engineering tactics in digital fraud. The success of this scam was largely due to the realistic appearance of the fake website and the convincing language used in the emails, which fooled many unsuspecting victims. Impersonation scams remain prevalent today, with fraudsters often sending fake emails from trusted entities like banks, major retailers, and other well-known brands.

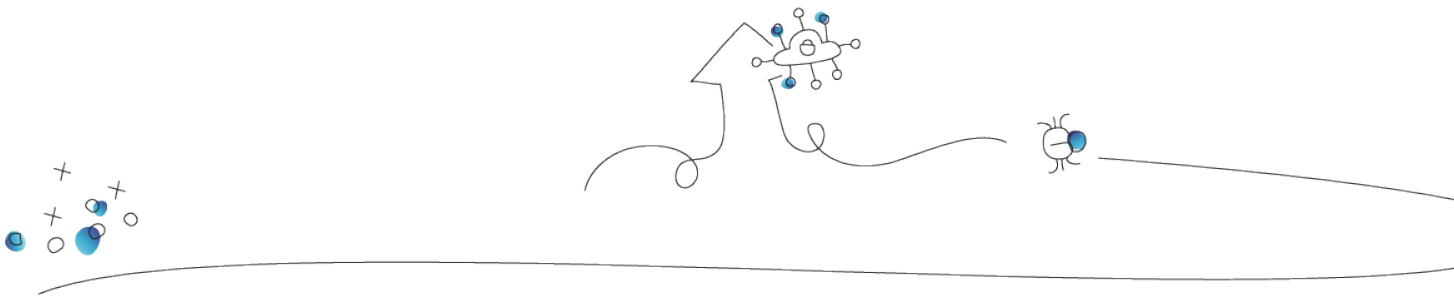
Rise of Sophisticated Cybercrime

The early 2000s saw a surge in sophisticated cybercrime as the internet proliferated. Hackers and organized crime groups began using malware, ransomware, and social engineering techniques to steal sensitive information and commit fraud. Data breaches exposed millions of personal records, making identity theft and financial fraud more common.

CASE STUDY

Target Data Breach (2013)

One of the largest data breaches in history, the Target breach exposed the personal and financial information of 40 million customers. Hackers used malware to infiltrate the retailer's point-of-sale systems, highlighting the vulnerability of even large, well-protected organizations. This breach had significant repercussions, leading to a loss of customer trust, financial penalties, and increased regulatory scrutiny.



The Covid-19 Pandemic

In 2020, the Covid-19 pandemic accelerated the transition of work, commerce, and communications to digital channels, creating new opportunities for fraudsters.

With limited infrastructure in place to defend against online fraud, rates of fraudulent activity skyrocketed.

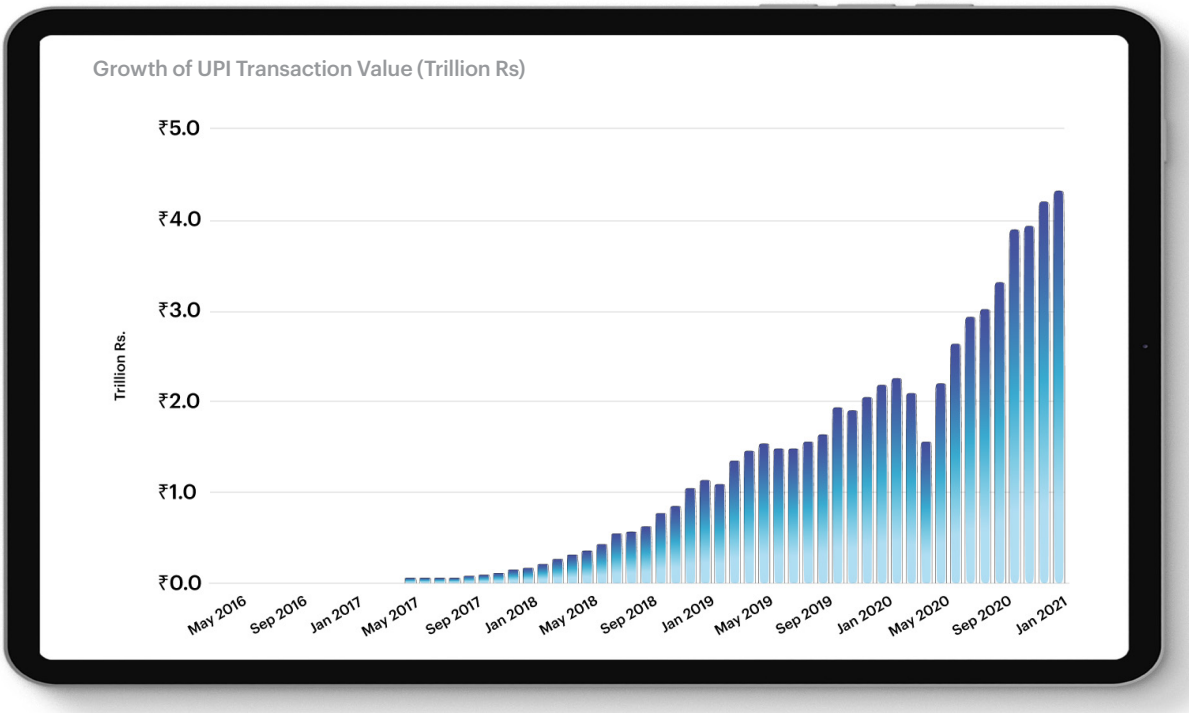
Impact of Faster Payments

Real-time payment systems have revolutionized financial transactions in many countries, offering speed and convenience while also presenting new challenges in fraud prevention. Fraudsters gravitate towards these systems in part because payment approval decisions must be made in near real time, and once processed, the transactions are irreversible - making it easier for them to steal, and keep, other people's money.

United Payments Interface (UPI) is India's Central Bank's instant payment system. UPI has significantly transformed the payment landscape in India, making transactions fast and straightforward. However, its widespread adoption has also made it a lucrative target for fraudsters. According to the BBC, from January 2020 to June 2023, almost half of all financial fraud in India involved the UPI system.

Pix in Brazil has likewise facilitated faster and more convenient transactions, but it has also exposed significant vulnerabilities. According to a 2022 survey by Brazil's banking association, almost one in three Brazilians have fallen victim to financial scams, with many incidents linked to the Pix system. In 2021, the first year after Pix was introduced, reports of social engineering attacks reached a record high, with financial scams causing estimated losses of 2.5 billion reals, 70% of which involved Pix transactions.

Even in the US where faster payment systems like Zelle, RTP, and FedNow haven't gained as much traction as similar solutions in India and Brazil, fraud targeting real-time payments is rapidly increasing.



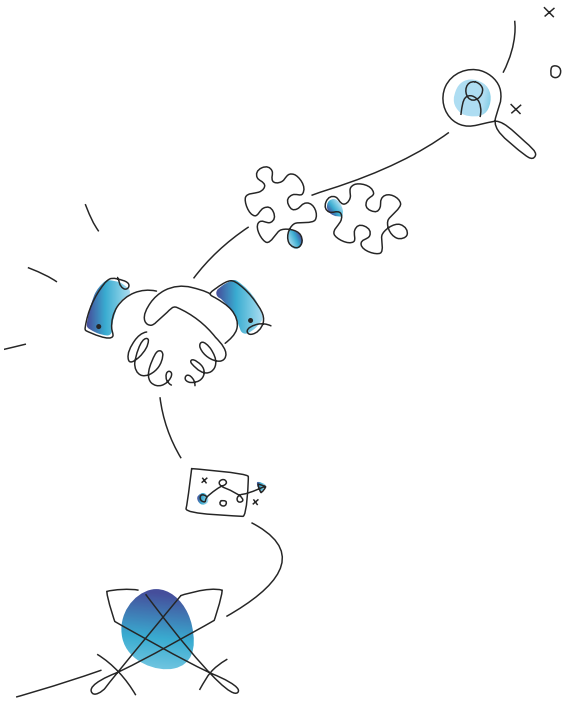
Source: Fintechna

Regulatory Evolution

As emerging threats of fraud have continuously evolved, so too has the regulatory landscape to address them. These key regulatory changes include data protection regulations, such as the EU's GDPR and California's CCPA, strengthened anti-money laundering (AML) regulations, and U.S. consumer protections such as Reg E and Reg Z which aim to protect consumers and limit their liability for fraudulent transactions.

While regulations like the GDPR and the CCPA prioritized data protection, and reforms such as the AML Act enforced stricter compliance, new AI-driven fraud threats require even more adaptive strategies. Organizations seeking to combat this increasingly complex threat landscape need to utilize AI-based solutions to stay ahead of bad actors. In parallel, industry trends are highlighting the growing importance of collaboration between institutions to strengthen defenses against fraud. By combining AI-driven solutions, such as Ballerine's, with cross-industry cooperation, organizations can better navigate this evolving landscape and take a proactive stance in fraud prevention.

Noam Izhaki
Co-founder and CEO, Ballerine



CASE STUDY

Anti-Money Laundering Act

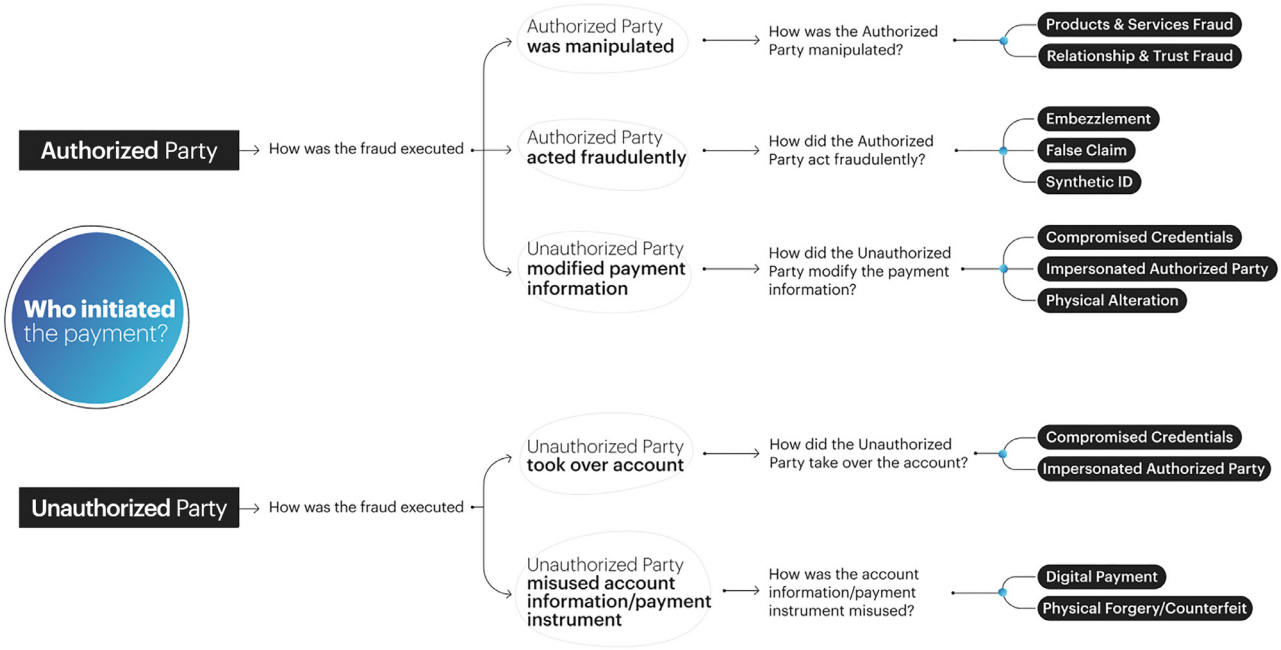
The AML Act of 2020 introduced comprehensive reforms to strengthen anti-money laundering regulations in the United States. The act requires financial institutions to implement robust AML programs, including customer due diligence and transaction monitoring, to prevent financial crimes. This regulatory change aimed to close loopholes that allowed illicit activities to go undetected and emphasized the importance of vigilance in financial transactions. Notably, the act mandated the establishment of a beneficial ownership registry to increase transparency and combat shell companies used for money laundering. Financial institutions have since enhanced their compliance frameworks, incorporating advanced analytics and AI-driven monitoring systems to detect and report suspicious activities more effectively.

Not all shell companies are set up by organized crime groups, however almost all organized crime groups use shell companies. Businesses need to look for indicators of shell companies in their third party onboarding and monitoring if they want to identify potential fraudulent networks. The alternative is to wait for a transaction monitoring tool to alert, which invites additional costs and pressure to the anti-fraud effort as teams scramble to block fraud whilst not allowing false positives to harm conversion. Whilst current methods will remain part of the mitigation, shifting more of the burden to the onboarding phase and focusing on prevention will be crucial for organizations seeking to reduce the impact of fraud on their bottom line.

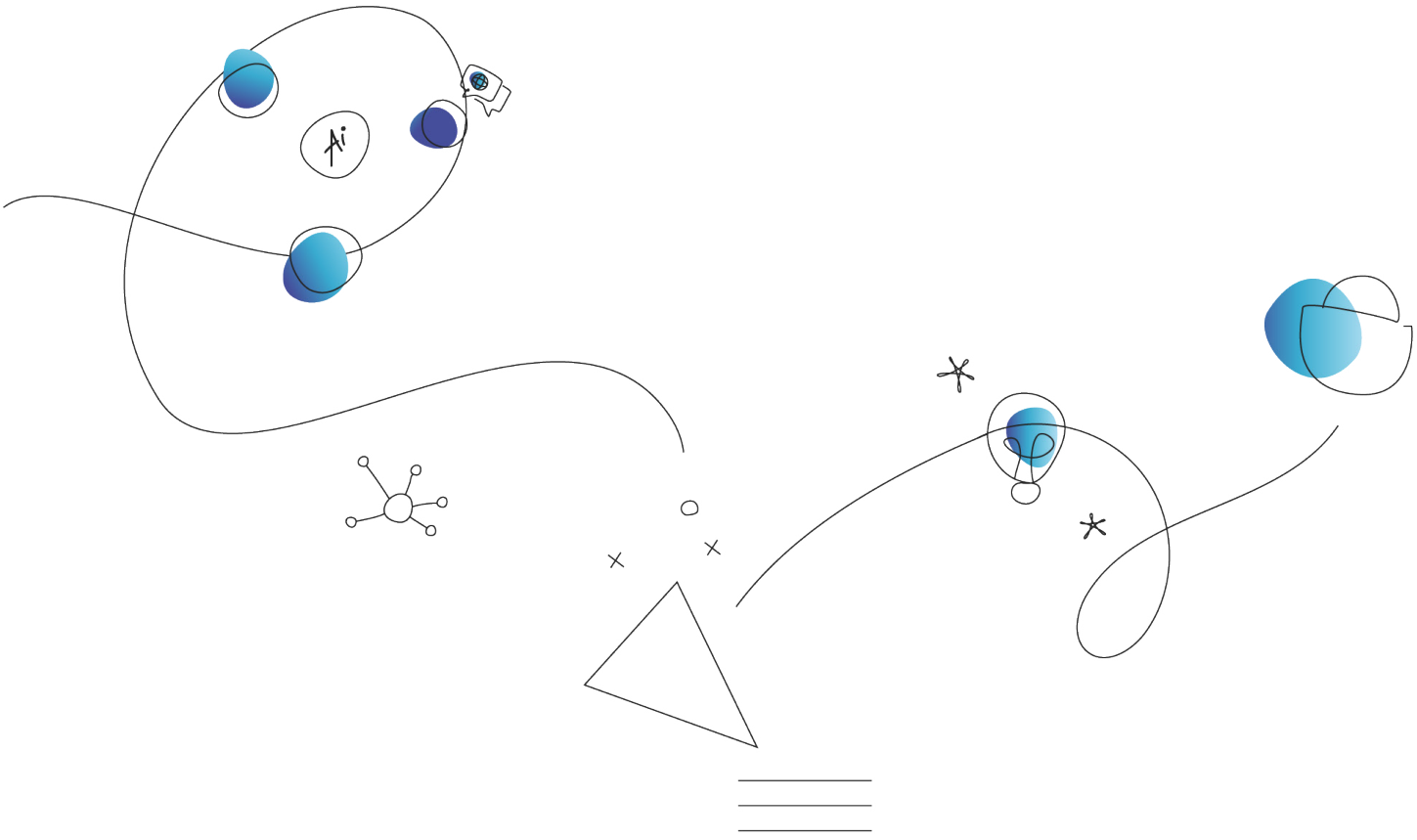
Alex Pillow
Senior Director,
Commercial Strategy, Moody's

Today, fraud takes on many different forms, depending on who was manipulated and how, and who authorized the transaction.

Fraud Classifier



Source: Federal Reserve



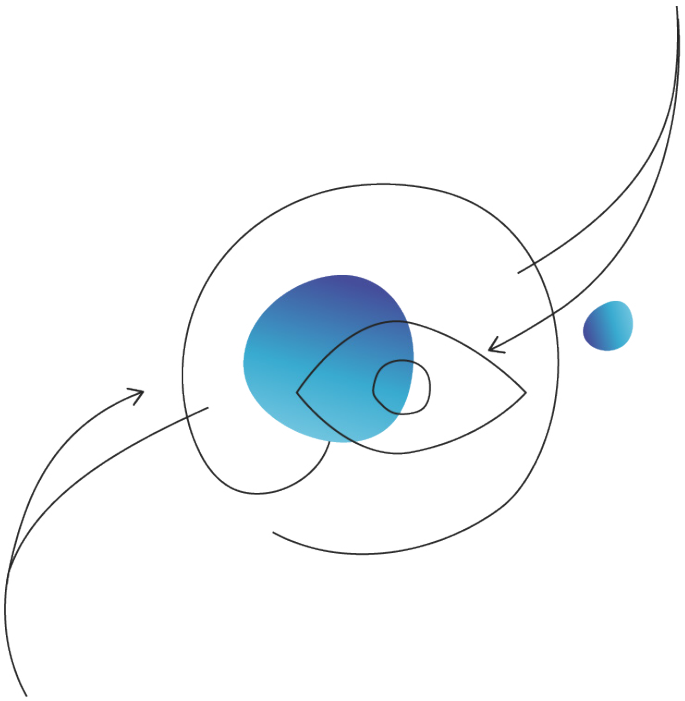
Current **Trends and Challenges**

Fraud is undergoing massive disruption and advancements thanks to new technologies like Generative AI (GenAI). This section covers the key trends in fraud today.

Understanding the Fraudster's Perspective

At Team8, our cyber fund focuses on understanding the "attackers' perspective" to develop innovative cybersecurity solutions. Fraudsters, like cyber criminals, continually evolve their techniques to bypass new defenses. Financial institutions must routinely adapt their strategies to keep pace with these ever-changing tactics. A thorough analysis of the tools, evolving strategies, and the psychological and social factors driving fraud is essential for building a proactive defense, anticipating threats, and effectively addressing emerging challenges.

Fraudsters employ a range of tools and techniques to deceive individuals and organizations. In fact, a whole business of fraud tools - "Fraud as a Service" - has emerged to serve fraudsters and increase their effectiveness.



Fraudsters toolbox
Ranked by level of complexity (low to high)

01. DATABASES

Detailed databases of stolen personal information, financial details, and security data.

02. MASS SPAM

Automatically sending large volumes of unsolicited messages to social engineer victims into sharing information or downloading malware.

03. VULNERABLE TARGETS

Targeted list of vulnerabilities and exploits for specific retail and payments sites.

04. PERSONALIZED ATTACK CONTENT

GenAI allows messages to be more personalized, giving them more legitimacy and increasing the likelihood of individuals falling victim to these fraud attempts.

05. WEBSITE IMPERSONATION

Creation of fake websites that mimic legitimate ones to trick users into entering personal information and/or passwords.

06. SOCIAL ENGINEERING BOTS

Bots that can intercept one-time passwords and automate collection and use of stolen identity information.

07. AML ORCHESTRATION

Automated systems and structuring of transactions to avoid detection and bypass AML checks.

08.FRAUD ORCHESTRATION

Fraud platforms that coordinate efforts across various tools and potentially various fraudsters to automate end-to-end fraud execution and maximize impact of fraud efforts.

Phishing and Social Engineering

Phishing involves fraudsters sending deceptive messages that appear to be from legitimate sources, tricking individuals into providing sensitive information, such as login credentials or financial data. These messages often mimic the branding, language, and formatting of trusted organizations to lower the target's guard.

Phishing tactics include:

- **Spear Phishing:** Targeted attacks using personal information
- **Clone Phishing:** Copying legitimate emails and altering them with malicious content
- **Whaling:** Targeting high-profile individuals like executives
- **Vishing:** Voice-based phishing attacks using personal information
- **Smishing:** SMS-based phishing attacks

Social engineering manipulates human behavior, exploiting trust and emotions to gain unauthorized access to systems or data.

Techniques include:

- **Pretexting:** Creating fabricated scenarios to obtain confidential information For example, an attacker might pose as an IT technician to gain a user's credentials and access to secure systems.
- **Baiting:** Offering enticing lures to trap victims,
- **Quid Pro Quo:** Promising a benefit in exchange for information

Malware and Ransomware

Fraudsters frequently use malware and ransomware in sophisticated ways to achieve various goals:

- **Banking trojans:** Malware designed to steal banking credentials
- **Cryptocurrency mining:** Malware covertly uses victims' resources
- **Identity theft and credential harvesting:** Spyware and keyloggers steal personal information
- **Corporate espionage and data breaches:** Advanced Persistent Threats (APTs) target corporate networks
- **Ransomware attacks:** Targeting critical infrastructure to increase the likelihood of ransom payment

Other tactics include compromising email accounts to initiate fraudulent wire transfers and mimicking legitimate software to trick victims into paying for unnecessary services. After stealing data using malware, fraudsters often sell it on dark web marketplaces. This data can range from personal identification information and login credentials to corporate secrets.

Business Email Compromise (BEC)

BEC scams involve compromising legitimate business email accounts to conduct unauthorized fund transfers. This method often targets employees responsible for financial transactions, exploiting their trust and authority. According to the Internet Crime Complaint Center (IC3), BEC scams have led to significant financial losses, with fraudulent transfers often sent to accounts in various countries.

The Role of GenAI

GenAI is playing a dual role in both enabling and combating fraud. Financial institutions and technology firms must continuously innovate to stay ahead of fraudsters, who are often first to leverage new technologies.

Benefits of GenAI in Fraud Detection

GenAI enhances fraud detection by enabling real-time analysis and pattern recognition. AI algorithms can process and analyze data faster and more accurately than traditional methods, identifying suspicious activities as they occur. This capability is crucial for financial institutions that handle millions of transactions daily, allowing them to quickly flag and investigate potential fraud.

Experian's 2024 Future of Fraud Forecast highlights the necessity for businesses to implement multilayered fraud prevention solutions that "fight AI with AI" to safeguard customers against increasingly sophisticated threats.

AI-driven models help in:

- **Real-time Monitoring:** AI can analyze vast amounts of transaction data in real time, identifying patterns and anomalies that indicate potential fraud.
- **Pattern Recognition:** Machine learning algorithms can learn from historical fraud data to recognize new patterns of fraudulent behavior, enabling proactive prevention.
- **Automated Alerts:** AI systems can automatically flag suspicious transactions, reducing the time required for human intervention and increasing the chances of stopping fraud before it escalates.
- **Enhanced Decision-Making**: GenAI enables analysts to respond to complex cases more quickly and accurately by providing immediate access to relevant data and insights. By synthesizing large volumes of information from various sources, GenAI can simulate potential scenarios and outcomes based on historical data and current trends, helping analysts understand the broader context and implications of suspicious activities.

Risks of GenAI

Fraudsters can exploit the same technology to create sophisticated scams, leveraging various methods to deceive their targets. They might use deepfakes, which are highly realistic videos and audio recordings, for impersonation purposes. Another tactic involves creating AI-generated phishing emails that closely mimic legitimate communications, making them harder to distinguish from genuine messages. Additionally, fraudsters can use AI to automate the creation of fraudulent content at a much larger scale, enabling them to scam a wider audience. These advanced techniques require a minimal investment of time and money, and demonstrate how technology can be weaponized to enhance the scale and effectiveness of fraudulent activities.

Challenges in Keeping Up with Technological Advancements

The rapid pace of technological advancement presents a constant challenge for fraud prevention efforts. Organizations must continually update their systems, integrating new solutions and tools to enhance detection and prevention capabilities and stay ahead of fraudsters. Effective fraud prevention requires a collaborative approach among financial institutions, technology firms, and specialized vendors.

CASE STUDY

The Arup Deepfake Fraud Incident (2024)

In early 2024, UK engineering group Arup fell victim to a sophisticated deepfake scam, resulting in a loss of HK$200 million ($25 million). Fraudsters used AI-generated video to impersonate the company's CFO during a video conference, convincing an employee to make a total of 15 transfers to five Hong Kong bank accounts. The employee only discovered it was a scam after following up with the group's headquarters. This incident, one of the world's biggest known deepfake scams, highlights the growing threat of AI-generated content in corporate fraud and the need for enhanced verification processes in financial transactions.

While fraud prevention efforts often involve enhanced authentication and monitoring systems, financial institution CEOs must: 1) Ensure that fraud prevention measures don't compromise the customer experience. Frictionless solutions like biometric authentication or behavioral analytics can provide strong security without burdening customers with unnecessary steps. 2) Advocate for ongoing staff training to help employees recognize phishing attempts, social engineering schemes, and other fraud tactics. Even the most advanced systems can be undermined by human error. A well-informed workforce is an essential line of defense against fraud.

Ron Shevlin
Chief Research Officer,
Cornerstone Advisors

The Future of Fraud Prevention

The future of fraud prevention hinges on a number of factors. We believe that the integrated use of AI and machine learning in fraud detection will continue to grow, becoming more sophisticated and enabling organizations to identify patterns and predict fraudulent activities with greater accuracy. In parallel, regulatory bodies will intensify their efforts to combat fraud, introducing stricter regulations and compliance requirements that will likely influence the direction of innovation in the space.

To maximize success, the industry will need to adopt a holistic approach to fraud prevention, and a multi-layered defense strategy that incorporates technology, policy, and human factors.

Cyber criminals are increasingly using AI to accelerate and scale their ability to steal personal data and turn it into targeted scam attacks against consumers. To counter this, key innovators in the digital ecosystem need visibility 'upstream' where the cyber risk exists, to enable them to innovate 'downstream' and prevent the fraud from taking place.

Only by working globally, across multiple industries and sectors, can we address all points of risk: at the breach layer (data compromise), the identity layer (ensuring you know your customer is who they say they are, authentication and ID verification) or at the transaction layer (risk scoring, rules, monitoring, decisioning). At Mastercard, we see this form of collaboration as central to protecting our interconnected world from cyber criminals and fraudsters.

Johan Gerber
Executive Vice President, Head of Security Solutions at Mastercard

The Convergence of Cybersecurity and Fraud Prevention

The financial sector is witnessing a major transformation in its approach to security with the emergence of cyber-fraud fusion centers. This innovative strategy represents a holistic approach to combating the increasingly intertwined threats of cybercrime and financial fraud. By breaking down traditional silos between cybersecurity and fraud prevention teams, organizations are creating a joint effort against sophisticated adversaries.

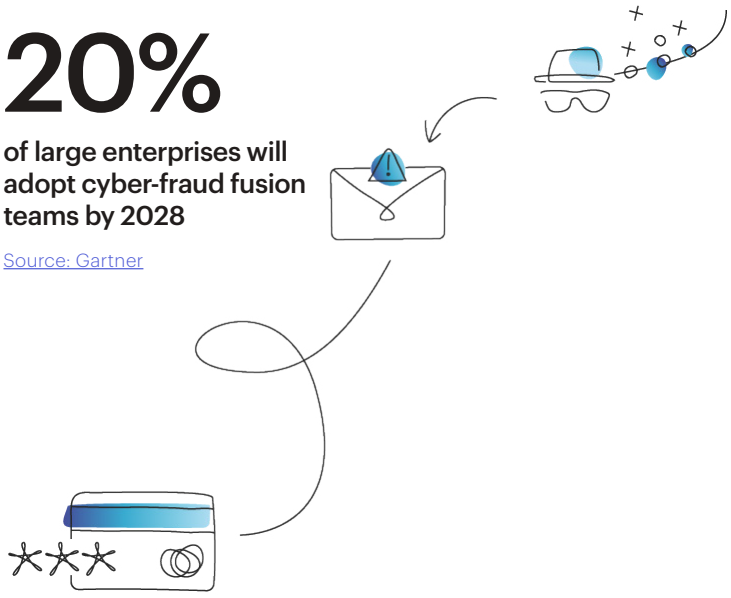
Industry leaders like Capital One, Citibank, and Mastercard are at the forefront of this trend. Their success is driving wider adoption, with projections from Gartner indicating that by 2028, 20% of large enterprises will have shifted to cyber-fraud fusion teams, a significant increase from less than 5% today. This integration allows for more rapid threat detection and response, as risk indicators can be identified further upstream in the attack chain.

The cyber-fraud fusion approach leverages shared information, tools, and expertise to develop comprehensive strategies that account for the full spectrum of cyber and fraud risks. By doing so, it enables organizations to stay ahead of evolving threats and respond more effectively to the complex, multi-faceted attacks that characterize the modern threat landscape.

20%

of large enterprises will adopt cyber-fraud fusion teams by 2028

Source: Gartner



The New Frontline in Fraud Detection

AI and machine learning are playing an increasingly critical role in combating sophisticated fraud. These technologies have the potential to not just enhance existing fraud prevention capabilities, but also to fundamentally reshape our approach to fraud detection. While AI can be harnessed by fraudulent actors to create more sophisticated scams, it can also be leveraged to better protect against fraud, creating a dynamic interplay between attack and defense in the digital realm.

AI-driven models can process vast amounts of data at unprecedented speeds, allowing for instantaneous analysis of transactions and user behaviors. Unlike traditional rule-based systems, AI and ML models can detect subtle patterns and anomalies that would otherwise be imperceptible to human analysts or conventional algorithms.

The dual nature of AI in fraud – as both a potential threat and a powerful defense tool – underscores the importance of staying at the forefront of technological advancements. However, it's crucial to recognize that these technologies are not infallible. AI and ML models also have limitations, including hallucinations and false positives, which can have outsized consequences for financial institutions and others dealing with customers' money. Balancing the power of AI with an understanding of its limitations is key to effectively leveraging these tools in the fight against financial crime.

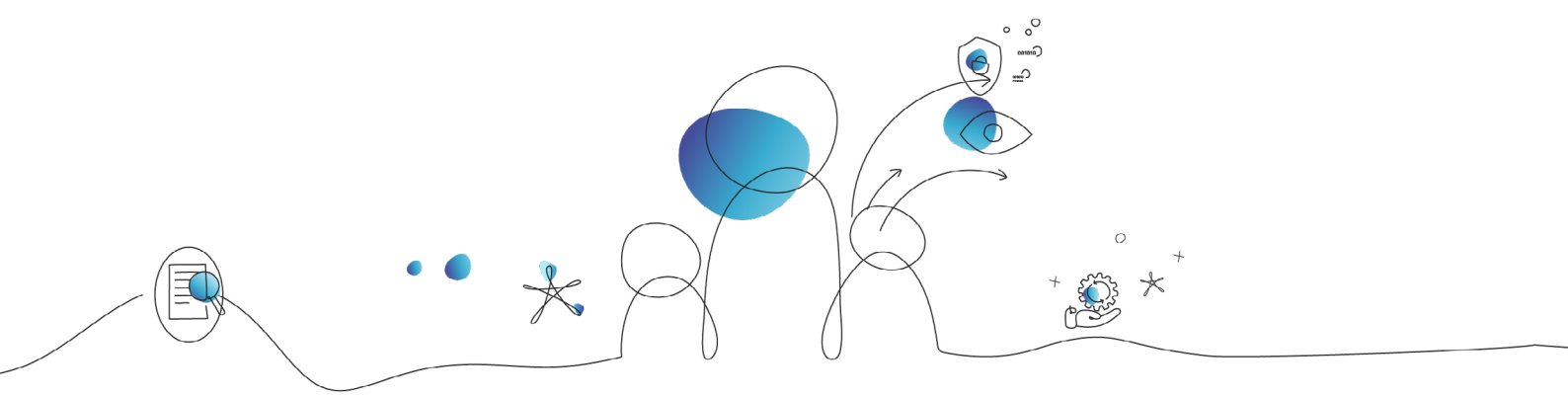
For instance, an AI system might identify a fraudulent transaction not just based on its monetary value or location, but by correlating it with hundreds of other data points, including the user's typical behavior patterns, device information, and even contextual data like current events or social media trends.

Machine learning algorithms are taking this a step further by continuously evolving their fraud detection capabilities. By ingesting historical fraud data, these algorithms can recognize emerging patterns of fraudulent behavior, effectively staying one step ahead of criminals. This adaptive learning is crucial in an environment where fraud tactics are constantly changing. An ML system might notice a new trend in how fraudsters are structuring their transactions to avoid detection, and automatically adjust its parameters to flag these new patterns, all with minimal human intervention.

GenAI is proving to be a game-changer in improving the overall effectiveness of fraud prevention platforms. By analyzing vast datasets of fraudulent and legitimate transactions, it can suggest new rules and optimize existing ones, significantly enhancing the accuracy of fraud detection systems. Moreover, GenAI is being leveraged to provide clear, human-readable explanations for AI-driven decisions. This explainability is crucial not only for regulatory compliance but also for building trust in AI systems among both internal teams and customers.

Looking ahead, the integration of AI and ML in fraud detection is likely to become even more sophisticated. We can expect to see more use of federated learning, where AI models can be trained across multiple institutions without sharing sensitive data, enhancing collective fraud detection capabilities while maintaining privacy. Additionally, the use of AI in creating dynamic user risk profiles that adjust in real-time based on behavior will become more prevalent, allowing for more nuanced and less intrusive fraud prevention measures.

As we move forward, the key to successful fraud prevention will lie not just in the power of AI and ML technologies themselves, but in how effectively they can be integrated into holistic fraud prevention strategies that also account for human expertise, regulatory requirements, and evolving criminal tactics.



The Human Element

As fraud technology advances, the human element of fraud has come into greater focus. Humans can be both another line of defense, but also an attack vector for fraudsters to exploit.

The Next Frontier in Behavioral Analysis

As we look to the future of fraud prevention, the role of behavioral biometrics and analytics is poised to become increasingly central. We predict that these technologies will evolve to create an even more nuanced understanding of user behavior, forming a critical component of multi-layered defense strategies.

Advanced AI algorithms will likely enhance behavioral biometrics, allowing for real-time adaptation to subtle changes in user patterns. This could lead to seamless, continuous authentication that goes beyond the login process, providing security throughout the entire user session without compromising user experience.

We anticipate that behavioral analytics will expand to incorporate a wider range of data points, potentially including cross-platform behavior analysis. This holistic view of user activity could significantly improve the accuracy of fraud detection, particularly in identifying sophisticated account takeover attempts.

Passwordless Technology

The move towards passwordless authentication is shifting the security paradigm from "what you know" to "who you are" or "what you have". While this addresses many traditional vulnerabilities, it also brings the human element of security into sharper focus.

The response to these evolving threats is twofold:

1. **Enhanced biometric security:** Developing more sophisticated liveness detection to combat deepfakes
2. **Comprehensive employee training:** Equipping staff and customers with the skills to recognize and resist advanced social engineering attempts..

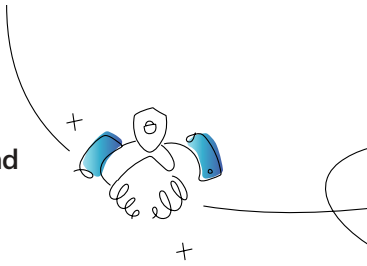
Scams and Authorized Push Payment Fraud

As technology in fraud prevention has advanced, fraudsters are increasingly targeting humans, often the weakest link in the security chain. Authorized Push Payment (APP) fraud, where victims are tricked into willingly transferring money to fraudsters, has become a significant threat, especially as real-time payments have become more popular. APP is just one method through which scams are executed, and if we look at the total damage of scams and social engineering globally, a recent report by GASA identifies losses of approximately $1.03 trillion USD.

$1.03T

Estimated value of financial losses incurred from scams and social engineering globally

Source: GASA



Top five most common fraud types in the US and UK

Source: Alloy 2024 State of Fraud

In this context, fraudsters will typically employ social engineering tactics to manipulate victims into voluntarily transferring funds, often by impersonating trusted entities like banks, government agencies, or known businesses.

Regulatory approaches to APP fraud prevention vary significantly across countries, directly influencing the pace and nature of innovation in the financial sector. In the UK, new regulations introduced in October 2024 require payment services providers to reimburse customers for APP scams. The refund scheme also introduces shared responsibility, with sending and receiving banks splitting liability for non-card payment scams up to £85,000 per claim. This shift in liability creates a strong financial incentive for UK banks to invest in cutting-edge fraud prevention technologies and strategies. The potential for significant reimbursement costs motivate these institutions to accelerate innovation, developing more sophisticated detection systems and user-centric security features.

In the US, liability for APP fraud still primarily rests with the victims. However, increasing regulatory scrutiny and the potential for future liability shifts are beginning to change this dynamic. As US financial institutions anticipate regulatory changes, they are beginning to prioritize new fraud prevention strategies and solutions.

A paradigm shift is essential in how we address APP fraud, scams, and other human-centric threats. The focus must extend beyond traditional fraud detection to proactively protect the human factor, the most targeted and vulnerable link in the chain. Organizations need to embrace a new standard of customer security, combining cutting-edge technology and psychology to empower and protect their customers. By creating a customer security framework of prevention, detection, intervention, and remediation, financial institutions can significantly reduce fraud losses, and enhance customer trust while positioning themselves as leaders in security and customer experience.

Roy Zur
Co-founder and CEO, Charm Security

Charm

Beyond regulatory pressures, customer expectations around trust and security are also pushing US banks to innovate. As fraudsters grow more sophisticated, the reputational risks and potential loss of customer confidence have become significant motivators. Forward-thinking financial institutions are now proactively exploring innovative fraud protection and remediation solutions to not only stay ahead of fraudsters but also meet evolving customer demands and regulatory pressure.

This contrast in regulatory frameworks offers a compelling case study in how liability can drive innovation. For instance, following changes in UK liability rules, banks like Monzo have introduced innovative, user-centric security features. One such feature is Trusted Contacts, which requires approval from a pre-designated secondary contact for large transfers or new recipients. This exemplifies a shift towards user-empowered security that balances convenience with robust fraud prevention. Should similar liability be imposed on US financial institutions, we would likely witness a rapid surge in the development of comparable innovative features aimed at mitigating APP fraud risks, fundamentally changing the landscape of fraud prevention.

The Evolution of Identity Verification

As digital fraud becomes more sophisticated, identity verification methods must evolve. The future lies in dynamic, multi-layered approaches that balance security with user convenience. This evolution aims to create a more robust, flexible, and inclusive identity ecosystem in the digital age.

Combatting Deepfakes

As the battle against increasingly sophisticated deepfakes intensifies, we anticipate a revolution in identity verification crucial for maintaining trust in digital interactions. Liveness detection mechanisms will likely become the cornerstone of robust identity verification processes, evolving to counter the rapid advancements in deepfake technology.

We predict a convergence of active and passive liveness detection techniques, creating a seamless and highly secure verification process. Future systems may employ AI-driven, dynamic challenges that adapt in real-time to potential threats, while simultaneously analyzing subtle biometric markers invisible to the human eye.

Enhancing Authenticity

The adoption of Near Field Communication (NFC) for document verification is expected to gain traction, offering enhanced authentication accuracy. Already common in various applications, NFC is increasingly being used for secure identity document verification, with 140 states and non-state entities offering NFC-enabled biometric documents. This technology is attractive as a form of document verification because it is extremely secure and entails only minimal friction. We foresee a transitional period where NFC verification coexists with advanced optical document analysis, gradually becoming the gold standard as technology and policy align.

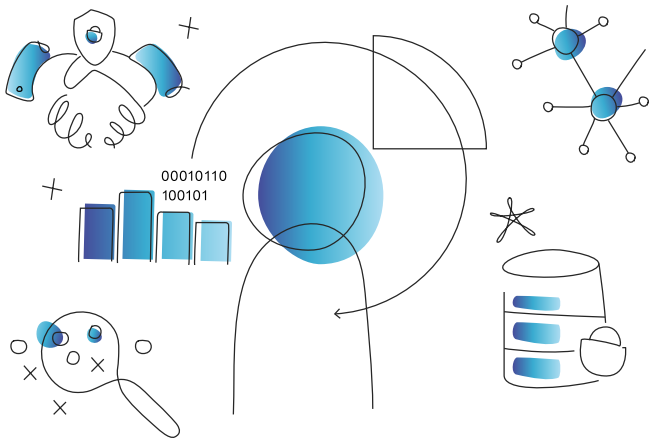
Building a Proactive Fraud Prevention Strategy

We also anticipate a shift towards more proactive and intelligence-driven strategies. The emergence of "fraud intelligence" as a distinct category of threat detection services marks a significant evolution in the field. This approach combines cybersecurity techniques with forensic analysis of online fraud data, creating a more comprehensive view of the threat landscape.

A key development in this area is the cyber-fraud kill chain, which adapts common cybersecurity methodologies to map out the tools, tactics, and procedures (TTPs) used by fraudsters. This framework allows organizations to interrupt fraud at multiple stages, moving beyond reactive measures to anticipate and neutralize threats before they fully materialize.

While technological advancements are crucial, the human element remains vital, especially in relation to scams and APP. We predict an increased focus on educational interventions as part of a holistic fraud prevention strategy. These programs have shown promising results in reducing susceptibility to fraudulent schemes, although specific efficacy rates may vary depending on the context and implementation.

As fraud tactics continue to evolve, this multifaceted approach – combining advanced threat intelligence, strategic frameworks, and human education – will be essential in building robust, adaptive fraud prevention strategies.



The Consolidation of Fraud Prevention Solutions

The consolidation and integration of diverse fraud detection capabilities into comprehensive platforms is also a trend to watch for the future of fraud prevention. This shift is driven by the increasing complexity of fraud threats and the need for more holistic, efficient solutions.

We anticipate vendors will continue to expand their offerings, combining multiple online fraud detection capabilities into unified solutions. This trend is already visible in the market, with individual features like device intelligence and behavioral biometrics becoming standard components of broader platforms. Leading payment gateway vendors are expected to offer increasingly sophisticated native fraud detection solutions, though these may not match dedicated vendors for complex use cases.

Preventing fraud before money is stolen requires a holistic approach to identity risk management. That means financial institutions need to implement controls to verify customer behavior both at onboarding and throughout the customer lifecycle. By looking at potential and current customer identities from many different angles, FIs can ensure they can continue to grow without being held back by the threat of fraud.

Laura Spiekerman
President and Co-founder,
Alloy

ALLOY

The future points towards integrated platforms capable of orchestrating multiple fraud prevention capabilities. These systems will likely create dynamic user journeys that balance security with user experience, adapting in real time to minimize risk without introducing unnecessary friction. This evolution promises more effective fraud prevention while potentially simplifying the technology stack for many organizations.

Preparing for the Future: Recommendations for Stakeholders

As we stand on the cusp of a new era in fraud prevention, stakeholders across the financial ecosystem must adapt their strategies to meet evolving challenges. Our research points to several key areas where focused efforts can yield significant results in safeguarding against sophisticated fraud threats.

Reframing the Narrative: From Isolated Incidents to a Continuous Narrative

Traditional approaches to fraud prevention often categorize incidents into buckets such as Account Takeover (ATO) or ACH fraud. However, this classification system fails to capture the complex, evolving nature of modern fraud schemes. To effectively combat fraud in the future, we need to shift our perspective and view fraud as a series of interconnected events - a story with multiple chapters, rather than isolated incidents.

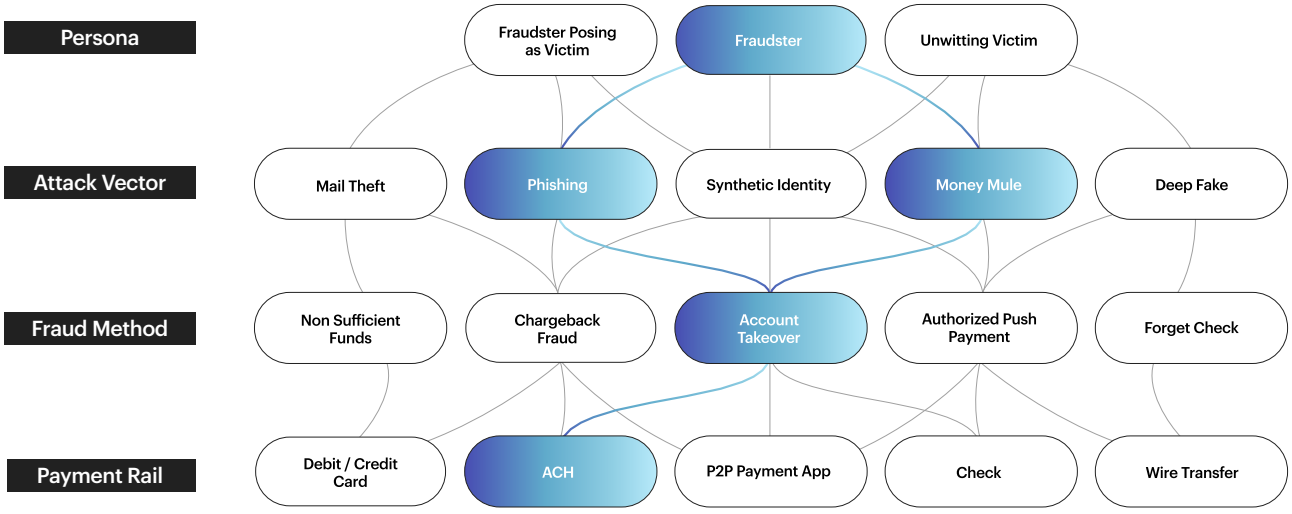
Fraud Typologies as Narratives

Each fraud attempt is a narrative that unfolds over time, often involving multiple touchpoints, technologies, and human manipulation. For example, what might initially appear as a simple ATO could be part of a larger, more sophisticated scheme:

1. **Recon:** The fraudster gathers information about the target through social media or data breaches.
2. **Initial Access:** Using the gathered information, they attempt to gain access to the account through phishing or credential stuffing.
3. **Escalation:** Once inside, they may change account details or add new beneficiaries.
4. **Exploitation:** The compromised account is used to initiate fraudulent transactions or as a stepping stone to attack related accounts.
5. **Cover-up:** Attempts are made to hide the fraudulent activity, potentially by deleting transaction records or communications.
6. **Fund retrieval:** The fraudster uses a series of mule accounts and transfers to access the funds while making it harder for the victim's bank to trace the money movement.

By viewing fraud through this narrative lens, we can better understand the interconnected nature of different fraud types and develop more comprehensive prevention strategies.

All fraud types are multidimensional



Implications for Fraud Prevention

This narrative-based approach to fraud typologies has several implications for the future of fraud prevention:

1. **Comprehensive Monitoring:** Instead of focusing on individual transaction points, fraud prevention systems need to monitor user journeys across multiple channels and over extended periods.
2. **Pattern Recognition:** AI and machine learning models should be trained to recognize not just individual red flags, but sequences of events that could indicate a developing fraud narrative.
3. **Cross-functional Collaboration:** As fraud narratives often span multiple departments (e.g., from customer service to transactions to security), organizations need to break down silos and foster cross-functional collaboration in fraud prevention.
4. **Predictive Analysis:** Understanding fraud as a narrative allows for better predictive capabilities. By recognizing the early chapters of a fraud story, organizations can intervene before the scheme reaches its climax.
5. **Adaptive Defense:** As fraudsters adapt their narratives, fraud prevention strategies must be flexible enough to recognize and respond to new plot twists in the fraud story.

By adopting a narrative-based approach to fraud, organizations can develop more nuanced, effective, and adaptable fraud prevention strategies for the future.

Financial Institutions: Spearheading the AI-Driven Defense

Financial institutions are at the forefront of the battle against fraud, and their approach needs to be both innovative and comprehensive. They must adopt a proactive stance that moves beyond reactive measures, anticipating and neutralizing threats before they fully materialize.

Complementing this strategic shift is the adoption of advanced machine learning models. Financial institutions should implement both supervised ML for known fraud patterns and unsupervised ML for anomalies and new tactics. The integration of graph analytics for real-time analysis is particularly promising, as it can uncover complex fraud patterns and relationships that might otherwise go unnoticed.

However, with great power comes great responsibility. As these AI models become more sophisticated, there's an increasing need for robust governance frameworks. Institutions should develop sandboxes for testing new models, ensure the ability to revert to older versions if needed, and implement bias auditing through performance reporting across different demographic groups.

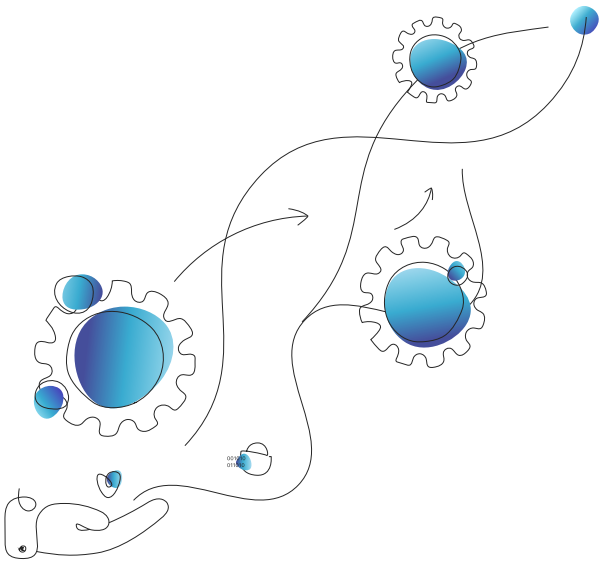
Regulators: Striking the Balance

Regulatory bodies play a crucial role in shaping the future of fraud prevention, primarily by protecting customers from fraud. However, their mandates can also have unintended consequences, like strict data collection and storage requirements that may increase the risk of exposing PII and sensitive financial information in data breaches. They walk a tightrope between fostering innovation and ensuring consumer protection.

As noted in our discussion about the UK's refund scheme for scams earlier in this chapter, rules and regulations have a unique ability to incentivize innovation by assigning liability to the party most able to address each type of risk in the fraud chain. Rules-driven innovation doesn't necessarily need to come from regulators. For example, in card payments, the networks assign liability across issuers and merchants in a way that encourages each party to adopt new technologies to combat fraud.

Regulators should also mandate improved security measures. Drawing lessons from Brazil's response to Pix-related fraud, considerations should include requiring financial institutions to implement daily transfer limits and caps on nighttime transactions. Furthermore, the creation of shared databases for tracking fake accounts across institutions could significantly hamper fraudsters' ability to operate.

As AI becomes increasingly central to fraud prevention, regulators must also establish robust AI governance frameworks. This includes developing guidelines for bias auditing in AI models and requiring explainability in AI-driven fraud prevention systems. The ability to provide clear insights into ML model outputs isn't just a technical necessity—it's a matter of maintaining trust and accountability in our financial systems.



Technology Providers: Empowering Through Innovation

For technology providers, the focus should be on developing comprehensive fraud intelligence platforms that combine threat intelligence, digital risk protection services, and fraud operations. These platforms should implement behavioral analytics across the entire user journey, a crucial step in preventing business logic abuse.

A particularly pressing area for innovation is in combating deepfake attacks in identity verification processes. Advanced liveness detection techniques, combining both active methods (requiring user actions) and passive methods (analyzing micromovements, 3D depth, and metadata elements), will be crucial in this fight.

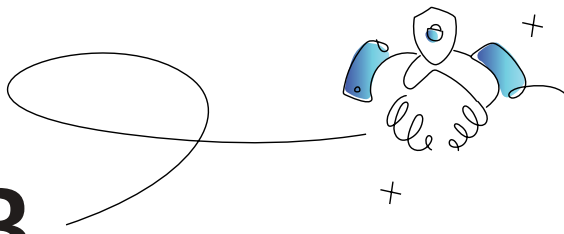
Although AI is used in fraud prevention today, AI-powered deep fakes present an escalating threat as fraudsters leverage this technology to mass-produce hyper-realistic synthetic content that compromises customer accounts and data. In response, financial institutions are building robust fraud defense mechanisms built on multi-modal generative AI frameworks to simultaneously analyze diverse data streams, including voice, biometric, video feeds, textual information and user behavior patterns. Using these services and models allows AWS customers to conduct real-time analysis across various channels, detecting subtle inconsistencies in facial expressions, voice characteristics, keystroke patterns, and transaction behaviors to identify and thwart sophisticated deep-fake threats as they occur.

Vick Panwar
Principal, Global Banking
Strategy & Development, AWS

Moreover, providers shouldn't neglect the often-overlooked area of post-payment fraud. With losses amounting to approximately $23 billion in 2022, there's a clear need for solutions that can evaluate post-payment user activity, including return history and other metadata.

Investment Trends

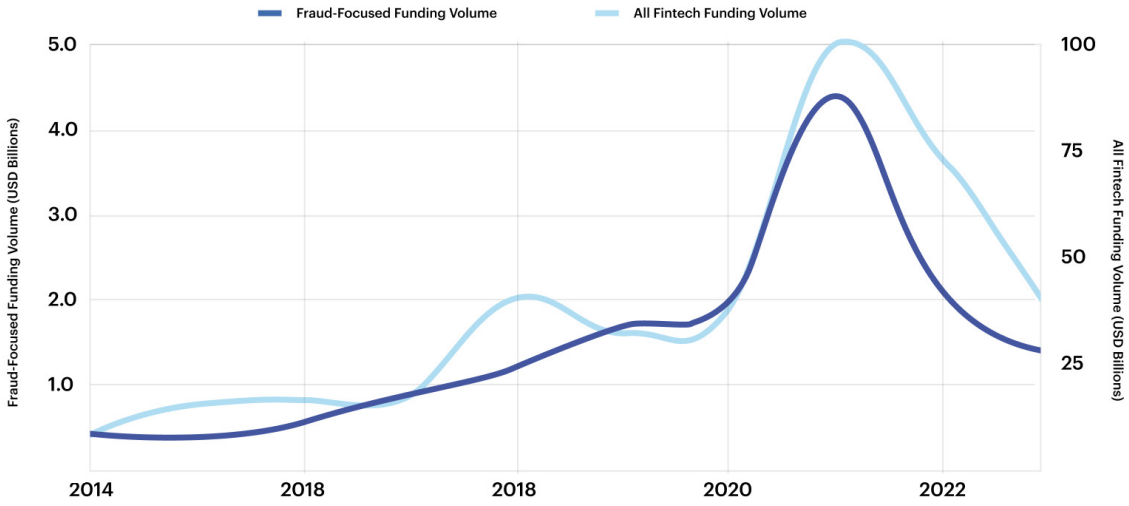
Fraud is one piece of a larger puzzle that includes compliance and risk management solutions. These areas are deeply intertwined, with the lines between preventing fraud, managing risk, and ensuring regulatory compliance often blurred. In this section, we will examine investment trends in the fraud ecosystem, recognizing that advancements in fraud prevention are inseparable from the technologies and frameworks driving risk management and compliance initiatives. Addressing the entire category provides a more holistic view of the market dynamics and innovation shaping the future of fraud mitigation.



$15B

has been invested in fraud-focused companies across 1,000 deals over the past decade

Funding Trends (2014–2023): Fraud-Focused Fintechs Mirror Funding Patterns Across All Fintech Verticals



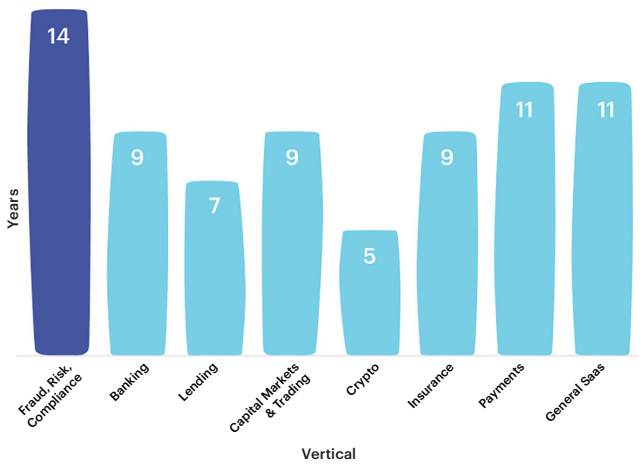
Source: Team8

Recent Investment and M&A Activity

Over the last decade (through H1 2024), fraud, risk management, and compliance companies raised over $15 billion across 1,000 deals analyzed by Team8. Reflecting broader fintech investment trends, nearly two-thirds of this funding occurred between 2020 and 2023, with a peak of $4.4 billion in 2021. Notably, in 2023 fraud companies demonstrated a higher success rate in progressing from Seed to Series A compared to the fintech average, 37% versus 31%.

When it comes to acquisitions, the vast majority of acquirers of fraud companies are strategic buyers, 70% vs. 49% across fintech generally. Active buyers in the space have included IBM, Moody's, Thomson Reuters, and others. The median time to exit for fraud companies is roughly 12 years, indicating that these strategic acquirers prefer mature companies rather than snapping up young companies.

Median Exit Time for Fintech Verticals (2013 - 2023)
Fraud, Risk & Compliance Startups take the Longest to Exit Due to a Preference for Mature Acquisition



Source: Team8

Looking Forward

For investors looking to make an impact in this space, several areas show particular promise. Cyber-fraud fusion technologies, expected to reach early majority adoption by 2028, represent a significant opportunity. Companies developing advanced behavioral analytics for continuous authentication are also worth watching, especially as we move toward a passwordless future.

Integrated fraud prevention platforms that can orchestrate multiple capabilities are another area ripe for investment. Look for startups building comprehensive ecosystems that incorporate fraud intelligence, combining cybersecurity and online fraud forensic data signals.

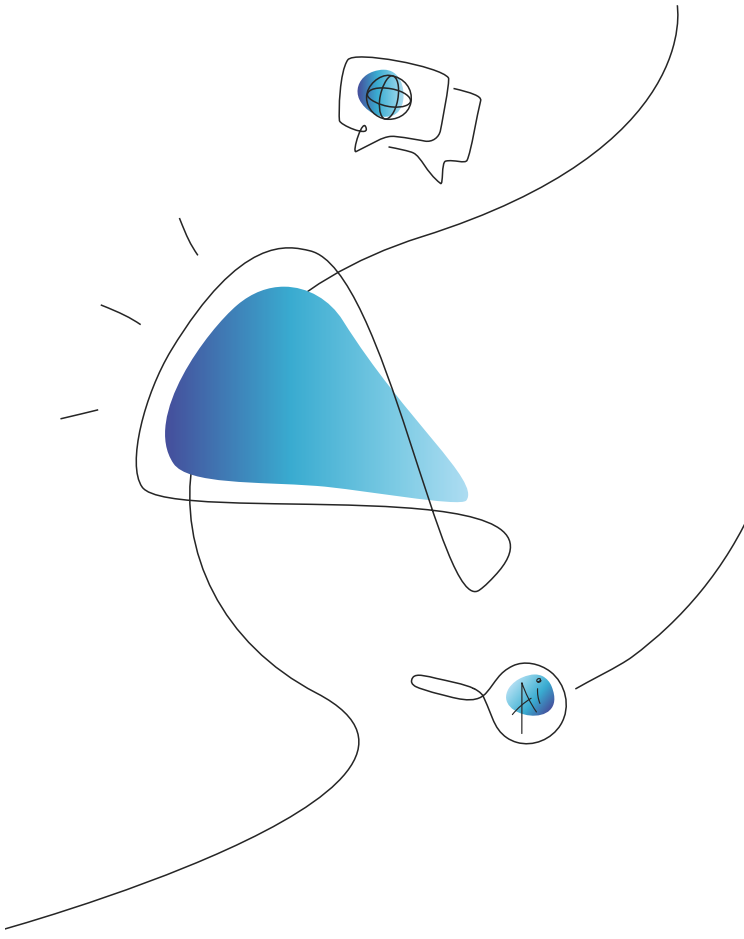
Lastly, the rise of GenAI presents exciting possibilities. Companies developing GenAI applications for upskilling platform administrators, providing explainability for decisions, and guiding new rule creation are at the cutting edge of fraud prevention technology.

In the coming years, we anticipate a significant shift in the fraud prevention investment landscape:

1. We expect to see increased investment in firms leveraging GenAI for fraud detection, particularly those offering explainable AI solutions.
2. Consolidation will accelerate, with larger tech firms acquiring AI-driven fraud prevention startups to enhance their offerings.
3. Venture capital will flow heavily into companies developing integrated platforms that combine multiple fraud prevention capabilities.
4. Startups that adopt the 'attacker's perspective' and integrate psychological insights with AI and traditional cyber defenses are well-positioned to gain significant traction, particularly in combating fraud that exploits human vulnerabilities.
5. Cross-industry partnerships and investments will rise, as sectors beyond finance recognize the need for advanced fraud prevention technologies.

These trends will likely reshape the competitive landscape, driving innovation and potentially leading to the emergence of new market leaders in fraud prevention.

Collaboration between key stakeholders will be key. By working together and implementing these recommendations, we can build a more resilient financial ecosystem—one that can withstand the sophisticated threats of today while being flexible enough to adapt to the challenges of tomorrow. The future of fraud prevention lies in a holistic approach that integrates multiple layers of defense, leveraging technology, enhancing employee training, and fostering collaboration.

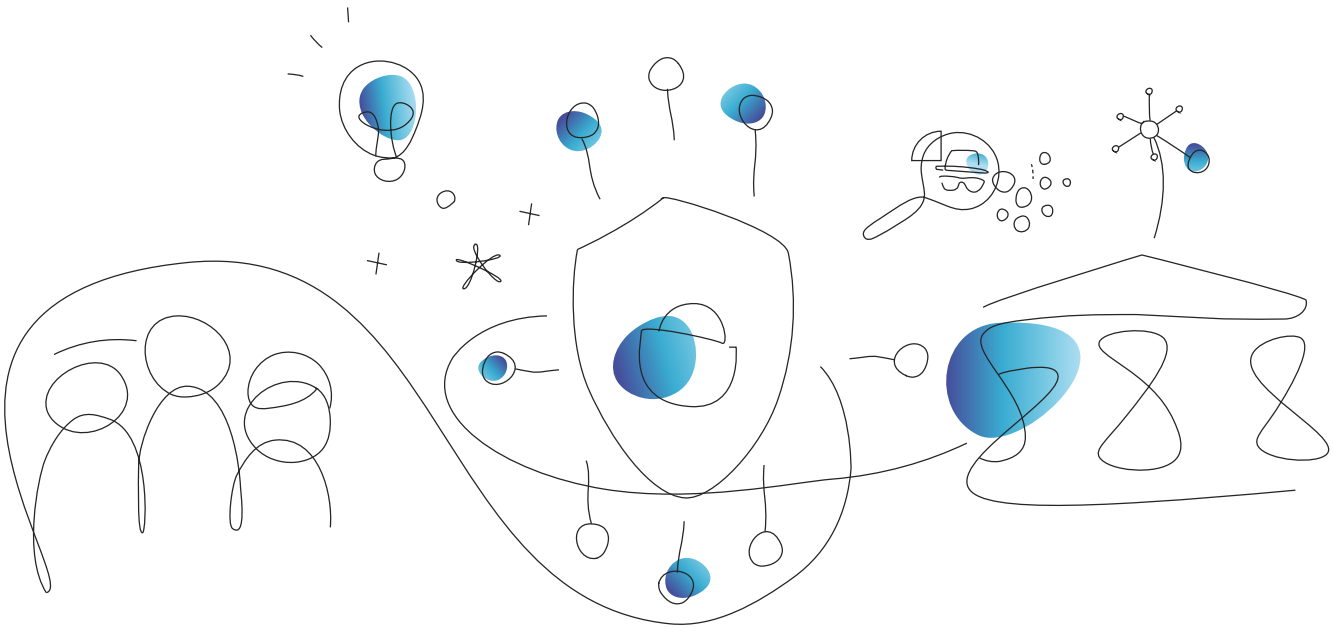


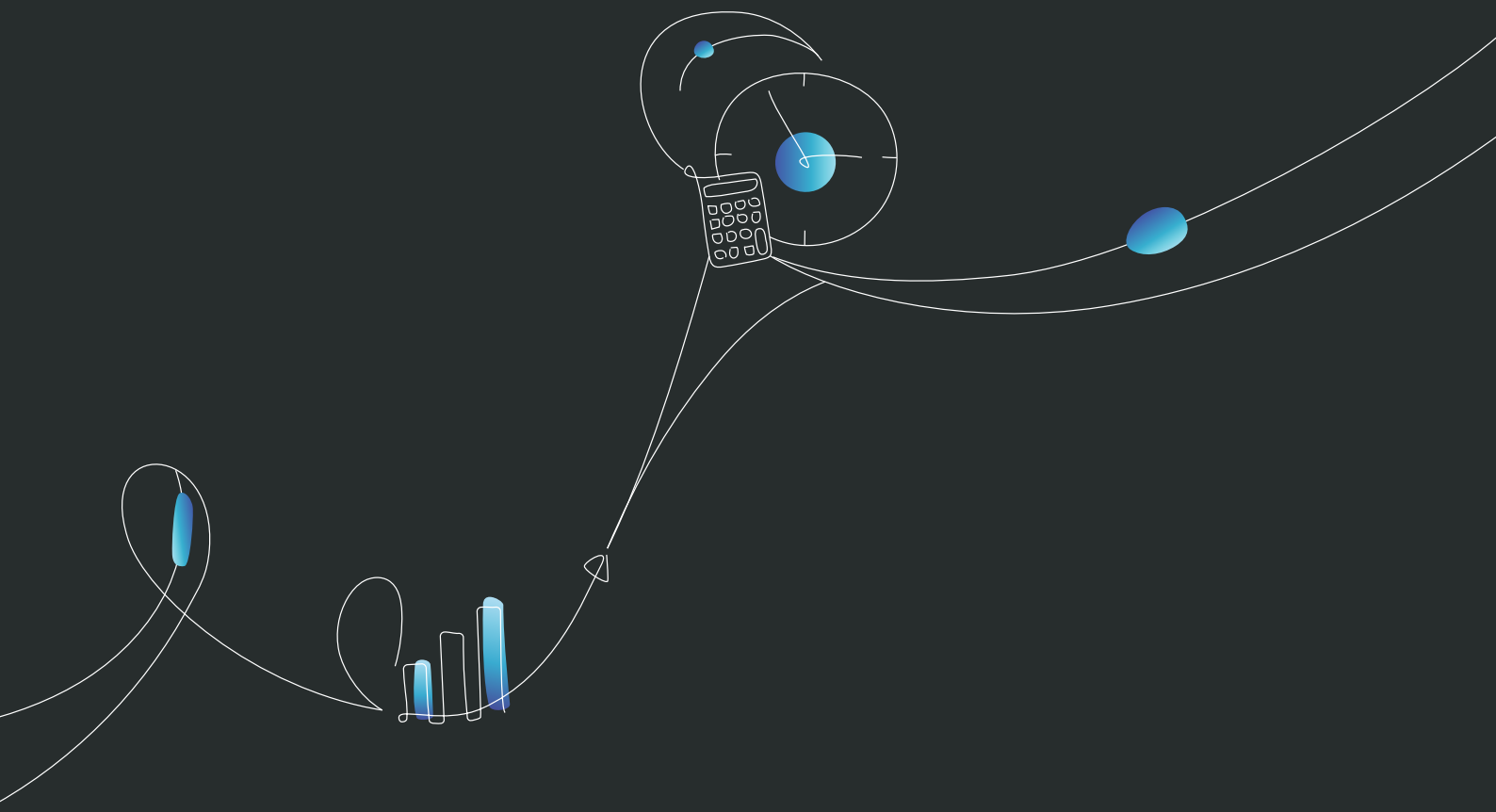
Conclusion

As fraud evolves in step with rapid technological advancements, the future of fraud prevention demands a proactive, multi-layered approach. Financial institutions, regulatory bodies, technology providers, and industry leaders must stay agile, leveraging advanced tools like artificial intelligence, machine learning, and behavioral analytics to detect and prevent fraudulent activity in real time. These technologies are only as effective as the strategies and collaboration behind them, underscoring the need for cross-sector innovation.

AI is transforming fraud detection, but fraudsters are also adopting advanced technologies. Success hinges on organizations integrating cutting-edge tech with human expertise and operational agility.

Writing this report has sharpened our focus on key areas where the next major opportunities will emerge in the fraud prevention landscape. At Team8, we believe that with the convergence of new technologies like GenAI, real-time payment systems, and future regulatory changes, the conditions are ripe for innovation. We hope this research provides value to all of our readers — whether it sparks the inspiration for a new venture, fuels your next investment decision, or simply serves as thought-provoking material for your next strategic meeting. As always, we'd love to hear your feedback and welcome any thoughts or insights you might want to share.





For more information
Contact us at: info@team8.vc | www.team8.vc

TEAM8™