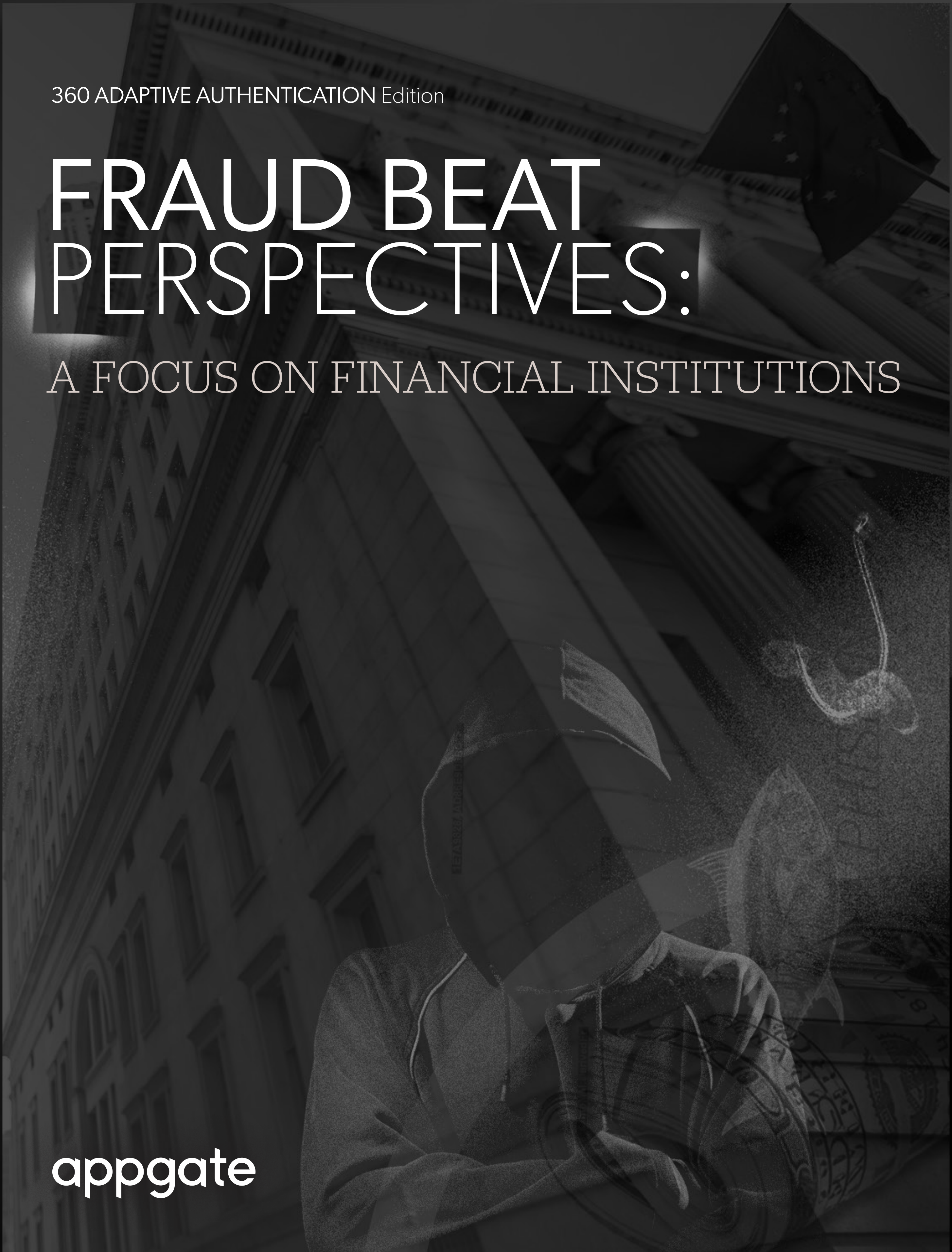
360 ADAPTIVE AUTHENTICATION Edition

FRAUD BEAT PERSPECTIVES:

A FOCUS ON FINANCIAL INSTITUTIONS



appgate

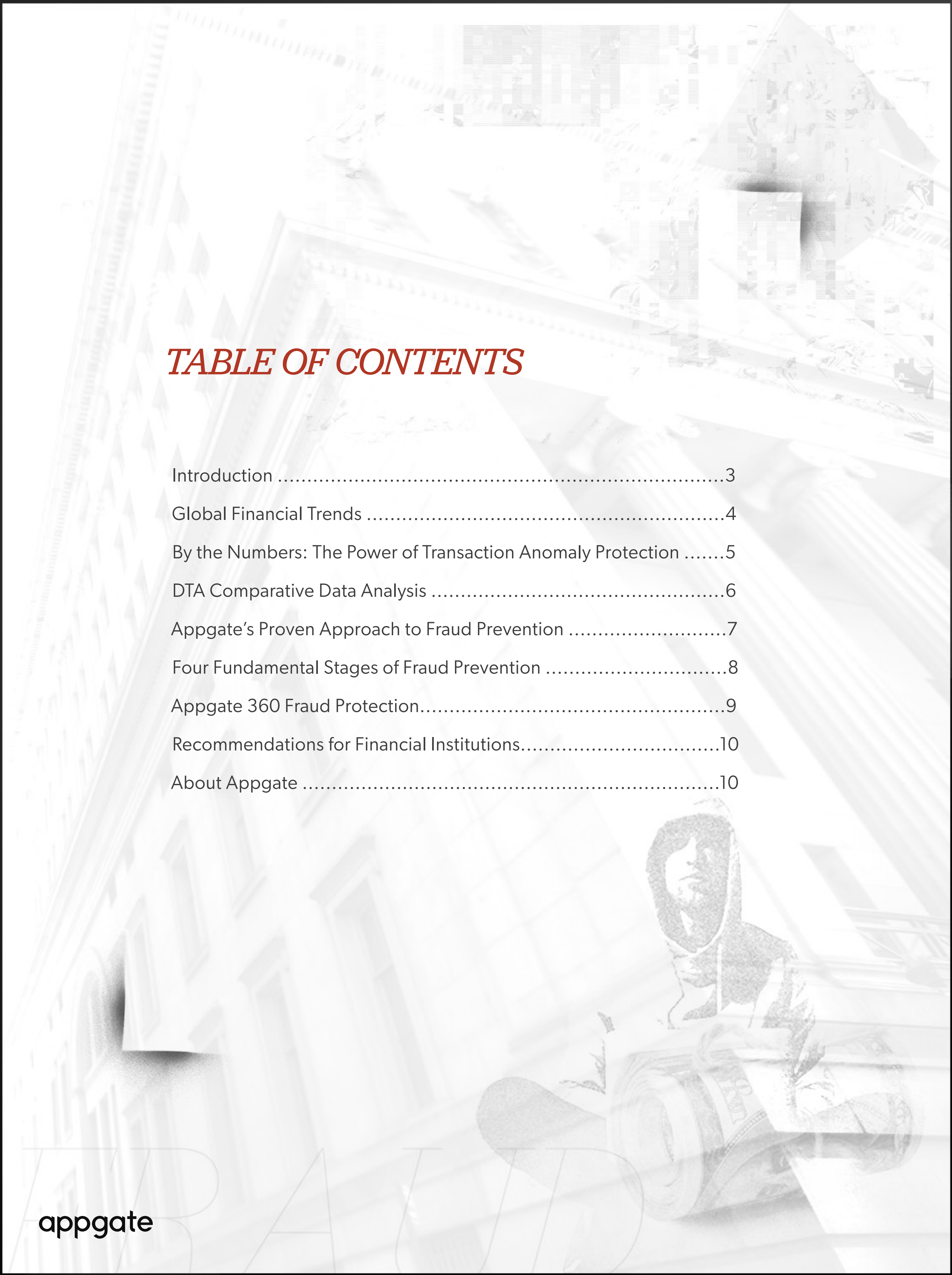


TABLE OF CONTENTS

A quick scan of today's global headlines and industry-related research reports reveals mounting pressures and significant changes faced by financial institutions. These challenges are driven by several key factors:

1 / ***Uncertain macroeconomic outlook*****:** Heightened global economic volatility has increased, with varying growth and inflation expectations across regions, creates an uncertain economic environment ripe for fraud and cyberattacks, as malicious actors seek to exploit regulatory disparities and economic instability.

2 / ***Stricter regulation and government supervision:*** New regulations, such as the Basel III Endgame, impose stricter capital requirements on large and medium-sized banks, including more stringent cybersecurity standards to protect the integrity and security of financial operations.

3 / ***Technological disruption:*** Rapid adoption of AI and machine learning (ML) is transforming the industry, particularly in fraud detection and prevention. These advanced technologies enhance the security of digital transactions by identifying and mitigating threats in real time. However, the increasing sophistication of cyberthreats using the same tech demands continuous innovation in advanced fraud solutions to stay ahead of malicious actors.

4 / ***Systemic risk:*** Increased geopolitical tensions and trade restrictions heighten volatility and systemic risk, with state-sponsored cyberattacks and malicious actors threatening the stability of global financial institutions. Robust cyber defenses are critical to mitigate these risks.

5 / **Increased connectivity and mobility:** Technological innovation and economic interdependencies have increased communication and mobility, as well as the speed of innovation in the financial industry. However, this increased connectivity also facilitates the rapid spread of information and misinformation, which can destabilize banks.

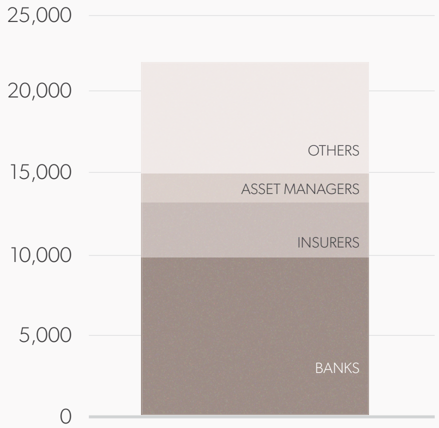
In 2024, the trickle-down effect of these pressures is readily apparent. One of the world's largest banks, JPMorgan Chase, recently reported that it fights approximately 45 billion hacking attempts per day. And incidents like the highly publicized February 2024 Bank of America data breach caused by a compromised third-party vendor, underscores how interconnected IT systems are across the financial industry and the need for comprehensive, multi-layered defenses.

This Fraud Beat Perspectives report focuses on the explosive growth of digital financial transactional channels across payments, collections, investment and savings. It offers data-rich intelligence and actionable guidance that financial institutions can use to supercharge their ability to detect and stop fraudulent transactions before incurring monetary loss and irreparable reputational damage.

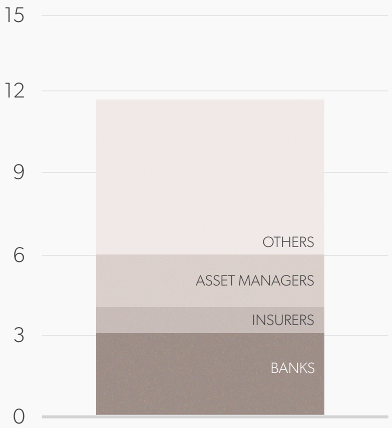
GLOBAL FINANCIAL INSTITUTION **FRAUD TRENDS**

Financial institutions are a favorite target for threat actors seeking to steal funds or data for monetary gain, or nation states focused on more nefarious goals like disrupting global stability. According to the International Monetary Fund's **2024 Global Financial Stability Report (GFSR)**, nearly 20% of reported cyber incidents from 2004 - 2023 impacted this sector, with banks the top target. The GFSR estimates direct losses at nearly $12B during this time, of which $2.5B was recorded from 2020 on, indicating escalation in successful financial institution breaches.

Financial sector cyber incidents
(number, 2004-23)



Financial sector losses
(billions of US dollars, 2004-23)



As the GFSR report highlights, direct financial losses resulting from fraud are substantial and concerning. However, the indirect losses resulting from fraudulent activities, such as damage to reputation or the necessity for security upgrades, can far exceed this direct financial impact. Protecting these institutions is paramount, as incidents within the financial sector can have far-reaching consequences. Cyberattacks can erode confidence in the financial system, disrupt critical services, and trigger a domino effect in other institutions, ultimately threatening global financial and economic stability.

BY THE NUMBERS: THE POWER OF TRANSACTION ANOMALY PROTECTION

Powered by artificial intelligence (AI), the Detection Transaction Anomalies (DTA) solution, a powerful tool in Appgate's 360 Adaptive Authentication multi-layered fraud protection suite, analyzes billions of transactions worldwide to identify and stop malicious attacks. In 2023, DTA analyzed more than 2 billion transactions in North American and LATAM alone, thwarting an estimated $73.5 million in monetary losses due to fraud. This represents a 37% increase in transactions analyzed and a 177% increase in fraud loss prevention compared to 2022.

North America		Latin America	
TOTAL TRANSACTIONS ANALYZED	**612M**	TOTAL TRANSACTIONS ANALYZED	**1.45B**
AVERAGE DAILY TRANSACTIONS	**1.7M**	AVERAGE DAILY TRANSACTIONS	**4.0M**
AVERAGE DAILY ALERTS	**32**	AVERAGE DAILY ALERTS	**45**
ANNUAL LOSSES PREVENTED	**$33M**	ANNUAL LOSSES PREVENTED	**$40M**

In North America, 612 million transactions, equating to a daily average of 1.7 million, were automatically analyzed and suspect transactions were blocked, equaling loss prevention of approximately $33 million. In Latin America, 1.45 billion transactions were analyzed equating to a daily average of 4 million, equaling a loss prevention of approximately $40 million.

The disproportionate volume difference reinforces what we know to be true when it comes to LATAM digital transaction trends:

Financial inclusion efforts: Regional governments and financial institutions have been actively working to increase financial inclusion. Digital financial services, including mobile banking and digital wallets, allow the unbanked population to access financial services and participate in the digital economy.

Innovative fintech solutions: LATAM is a fintech incubator with new financial products and services being introduced that are tailored to the region's needs. These include mobile payment systems, peer-to-peer lending and digital currencies.

Youthful demographics: The LATAM population is relatively young and tech-savvy. Younger consumers are more inclined to adopt digital payment methods and online shopping, contributing to the digital transaction increase.

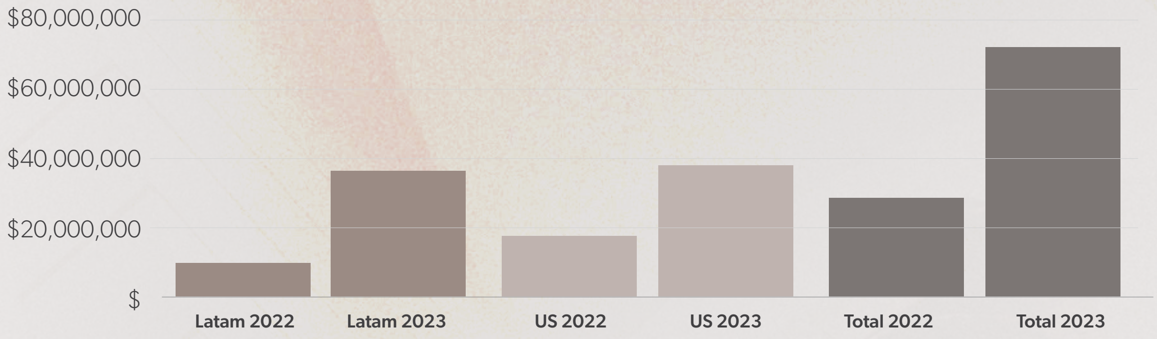
E-commerce growth: The rise of e-commerce platforms in the region drives digital transactions.

In 2023, DTA AI-powered automation capabilities also significantly reduced the number of daily alerts that must be managed in-house fraud prevention teams. The average number of daily alerts was 32 and 45 for North American and LATAM, respectively. This advantage means financial institutions can reduce operational costs by up to 80%, optimize their resources and improve administrative efficiencies. This is especially true when considering that industry estimates suggest that financial services teams can receive anywhere from 100 to 3,000 alerts per day, with some cases involving 10,000 to 15,000 alerts daily.

DTA COMPARATIVE DATA ANALYSIS

Comparing 2023 over 2022, both North America and Latin America experienced a substantial increase in analyzed transactions, reflecting a growing reliance on digital transactions and DTA's major advances in the automatic detection and blocking of fraudulent anomalies across the globe in 2023. Powered by AI and ML, Appgate's DTA solution has significantly improved fraud detection and prevention, leading to a notable increase in the volume of blocked fraud attempts for customers. Let's delve into the data:

Financial losses prevented



The reported sample size is a consistent percentage of Appgate customers, which was maintained at the same level from 2022 to 2023 in order to illustrate a baseline for comparing the evolution of the threat landscape and transactional trends. The data presented underscores the value of Appgate's DTA solution, providing robust fraud detection and prevention that enhances security and operational efficiency. for financial services organizations.

Appgate´s DTA analyzed more than 2 billion transactions and prevented $73.5 million in fraudulent losses.

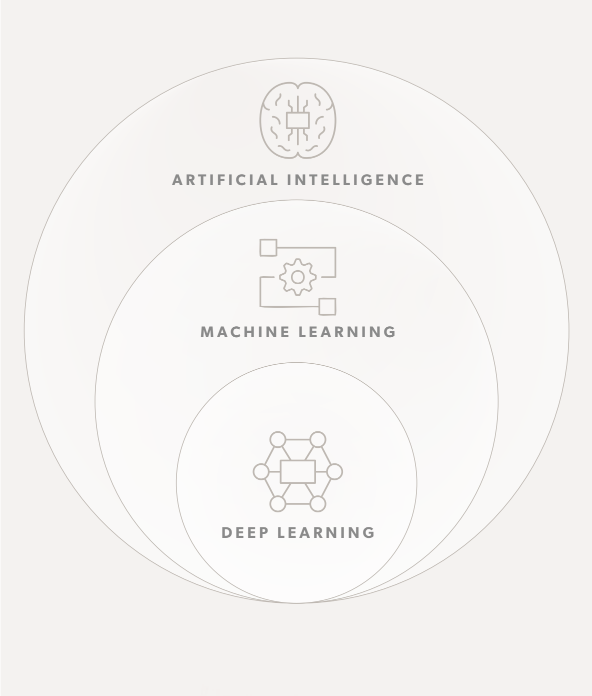
Values representative of local currencies converted into US dollars based on exchange rates at time of report generation.

APPGATE'S PROVEN APPROACH TO TO FRAUD PREVENTION

Appgate's DTA is a fraud prevention solution that helps organizations detect fraudulent activity in their transactions in real time. It leverages interconnected evaluators derived from AI, including ML and its subset deep learning (DL). As IBM defines it, deep learning "is a subset of machine learning, which is a neural network with three or more layers. These neural networks attempt to emulate the behavior of the human brain, and this allows it to "learn" from substantial amounts of data. Although a single-layer neural network can already make rough predictions, additional hidden layers help optimize and refine accuracy."

Deep learning is a driving force in the advancement of AI as it enables the automation of high-volume analytical tasks, leading to more accurate decision-making.

Below are additional data analysis technologies, beyond those previously mentioned, that enable Appgate to generate accurate fraud alerts by identifying anomalies and patterns in customer transactions in real time.



ADDITIONAL EVALUATORS INCLUDE:

- **Institutional rules:** Build restrictions based on custom parameters in real time.
- **Suspicious activity analyzers:** Search over a set of transaction patterns for fraud, attacking the critical path of fraud as soon as it is detected.
- **Real-time analyzers:** Leverage heuristic and anomaly detection to enable real-time monitoring of transactions, reducing friction with customers.
- **Composite evaluations:** Combine different evaluators.

These improvements underscore the value of Appgate's DTA solution, reinforcing its ability to deliver robust fraud detection and prevention that directly contributes to the financial security and operational efficiency of our customers.

FOUR FUNDAMENTAL STAGES OF **FRAUD PREVENTION**

Achieving robust fraud prevention is within reach. While deploying a comprehensive fraud prevention solution as part of a digital transformation initiative, including integrating various software products and organizational areas to mitigate fraud and strengthen financial security can be complex, it doesn't have to be overwhelming. Appgate's experienced team can guide you through best practices, ensuring seamless and efficient implementation.

A comprehensive fraud prevention solution is the result of a well-coordinated system comprised of processes, procedures, interdisciplinary teams, and technology working in harmony.

Appgate's approach to successful fraud prevention solution is built on a foundation of fundamental practices designed to reduce complexity. These practices are distilled into four key phases:

- ***Phase 1:*** Fraud Governance Maturity Assessment
- ***Phase 2:*** Alignment of expectations.
- ***Phase 3:*** Deployment
- ***Phase 4:*** Operation

By approaching fraud prevention as a holistic process and tracking performance through defined key performance indicators (KPIs), organizations can gain a clear roadmap for continuous improvement and strategic evolution. Each cycle through these phases should represent an iterative refinement of the overall fraud prevention strategy.

Appgate's professional services follow these standardized phases, while tailoring the execution to each client's specific requirements. Our collaborative approach fosters a culture of inquiry, critical thinking, and a deep understanding of fraud risks. We strive to create shared value for both Appgate and our customers, ultimately benefiting the end users who rely on our solutions.

Appgate caters to the specific needs of both financial and non-financial institutions:

Financial entities: We've observed significant growth in the adoption of strong governance and fraud prevention strategies within financial institutions. However some organizations may prioritize regulatory compliance over a broader strategy. This can sometimes lead to complex conversations and longer implementation timelines. Appgate's four-phase approach can help streamline this process.

Non-financial entities: For this expanding group, Appgate's DTA often requires more extensive configuration, monitoring, and adjustment throughout the phases. This is due to the wider range of fraud scenarios and limited regulatory precedents compared to financial institutions This trend is evidence that fraud extends beyond the financial sector, with non-financial organizations increasingly recognizing that their services, reputation and customer experience are valuable assets worth protecting.

APPGATE 360 FRAUD PROTECTION

Appgate 360 Fraud Protection, comprising 360 Brand Guardian and 360 Adaptive Authentication, is a comprehensive, multi-layered security platform designed to combat all forms of online fraud. It safeguards every stage of the attack cycle, from initial planning to cashing out. Leveraging an AI-based engine that adapts to user behavior, the solution detects and mitigates threats in real time, neutralizing potential attacks before they cause irreparable damage to the business. While each layer of the Appgate 360 Fraud Protection platform operates independently and effectively, the platform's power is amplified when the layers are integrated as a suite. This integration enables the seamless sharing of fraud intelligence across layers, enhancing the overall effectiveness of the fraud protection system.

About **360 Brand Guardian**

Appgate's 360 Brand Guardian is a comprehensive solution designed to safeguard your digital brand. It is engineered to provide advanced impersonation detection, enabling organizations to identify and mitigate fraudulent activities that introduce significant risk to brand integrity and customer trust. 360 Brand Guardian empowers businesses to proactively eliminate imposters and fake sites aimed at stealing customer credentials:

- **Digital Threat Protection (DTP):** Delivers a comprehensive, multi-channel approach to continuously analyze and monitor web, social media and public data feeds. It enables proactive protection against external threats by discovering and removing them, regardless of user population size. This solution significantly reduces criminal activity and mitigates the risk of future attacks.

- **Digital Risk Protection (DRP):** Uncovers compromised employee credentials, stolen credit cards and exposed source code in public repositories. The solution identifies stolen and exposed data on the Dark Web and Deep Web, allowing for quick action to prevent scams or data leaks within organizational systems.

- **Appgate Email Protection:** Mitigates the risk of phishing, malware and email-borne threats using advanced email protection methods like DMARC, BIMI, SPF and DKIM. The solution effectively detects and neutralizes malicious mails.

About **360 Adaptive Authentication**

Appgate's 360 Adaptive Authentication provides frictionless authentication to safeguard operations and customer experiences without inconveniencing end users—all from a single control point. Through advanced behavioral analytics and risk-based techniques, the solution continuously evaluates user actions, device characteristics and session patterns to deliver dynamic protection for complex fraud. Its comprehensive risk sensors ensure a trusted, secure environment, upholding user confidence and maintaining brand reputation. 360 Adaptive Authentication offers dynamic, customizable, risk- and behavior-based protection that removes user friction and false positive lockouts with:

- **DetectID Authentication (DID):** Provides strong adaptive authentication to secure digital identities with multi-factor authentication (MFA), real-time risk assessment and user-friendly interfaces. The solution intelligently adapts authentication methods as new risks emerge, ensuring secure access across various channels.

- **Risk Sensors:** Analyze user behaviors such as keystroke dynamics and mouse movements to detect and prevent fraud. The solution ensures seamless authentication with continuous monitoring and adaptive learning, integrating across platforms for consistent protection and convenience.

- **Detect Transaction Anomalies (DTA):** Leverages automated learning, prioritizing high-risk alerts to improve efficiency. The solution supports real-time, risk-based authentication and offers omnichannel integration for transaction and login monitoring. Advanced machine learning (ML) and a flexible rules-based system dynamically detects and mitigates both known and emerging fraud threats.

RECOMMENDATIONS FOR FINANCIAL INSTITUTIONS

As the **Faces of Fraud report** revealed, a survey of more than 200 financial institutions highlighted their growing concern about the exponential rise in fraud and the challenges of keeping pace. To adapt to these evolving trends and mitigate fraud risks, financial institutions should:

- **Implement Advanced Cybersecurity Solutions:** Leverage AI and advanced analytics to detect and prevent fraud in real-time, safeguarding customers' sensitive data.
- **Strengthen Oversight and Regulatory Compliance:** Adopt robust cybersecurity solutions to ensure compliance with evolving regulations and security standards.
- **Enhance Resilience Against Cyberattacks:** Develop comprehensive cyber risk management strategies to proactively address emerging threats and maintain business continuity.

By integrating these recommendations, financial institutions can strengthen their market position and bolster customer trust in an increasingly dynamic digital landscape.

For a deeper dive into fraud threats and solutions, explore our **2023 Fraud Beat Annual Report,** - a comprehensive analysis of electronic fraud trends throughout 2023.

Discover how Appgate's **DetectTA Transaction Monitoring** can help your organization identify and mitigate suspicious activity with the power or machine learning and advanced analytics.