VISA

Visa Consulting & Analytics (VCA)

How to guard against fraudulent use of data

Today, a reality facing stakeholders in the payment ecosystem is the potential impact of fraudulent use of compromised data. For financial institutions, this is primarily the result of external cyber-attacks on third-party organizations, such as vendors, merchants, payment processors and even government databases. Whenever consumer data, including but not limited to payment credentials, are compromised, there is a high risk that this data could be leveraged by unscrupulous threat actors to perpetrate fraud. Financial institutions are highly exposed to this growing area of risk, where such external data compromise events occur outside their own protection measures and controls.

In this paper, we share insights into how financial institutions can guard against fraud arising from such external data compromise events. In summary, we discuss the threat landscape; we investigate the main ways that threat actors seek to exploit compromised data; and we suggest best practices to assist financial institutions in containing risks, operationalizing their preparedness, and improving their resilience against such fraud.

Assessing the threat landscape

Over recent years, data compromise events have become an all too frequent phenomenon. Data compromise events that occur outside a financial institution's organization may include vendor data, merchant data, payment processor data, and even government data. In the final months of 2022, for example, we observed several high-profile data compromise events across the globe – targeting a large telecom operator, a low-cost airline, a credit bureau, a government portal, and more. Many, many more.[1]

In most instances, the main risk arising from cybercrime involving compromised data is the risk of payment-related fraud. The potential impact of such fraud is not limited to monetary loss. It can also lead to significant business and operational disruption and have a direct impact on an organization's customers. At Visa Consulting & Analytics (VCA), we work with clients to assess the risks they face and implement measures to protect against or mitigate such fraud, and some of our key insights are shared in this paper.

The prevalence and potential consequences of data compromise events cannot be overstated.

$10.5tn

Cybercrime is expected to cost companies worldwide upwards of $10.5 trillion annually by 2025.[2]

422m

Over 422 million individuals fell victim to data compromise events globally in 2022.[3]

1. Apple.com, "The Rising Threat to Consumer Data in the Cloud", December 2022, https://www.apple.com/newsroom/pdfs/The-Rising-Threat-to-Consumer-Data-in-the-Cloud.pdf
2. Security Boulevard.com, "The Top Data Breaches of 2022 so far", November 2022, https://securityboulevard.com/2022/11/the-top-data-breaches-of-2022-so-far/
3. Identity Theft Resource Center, 2022 Data Breach Report, January 2023, https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final.pdf

Appreciating the inherent risk factors and market threat drivers

Today's payment ecosystem is intricate and complex. Hence, it is important for financial institutions to recognize the inherent risk factors which cause vulnerabilities, make it possible for threat actors to propagate malicious attacks, and increase the likelihood of external data compromises leading to fraud. In devising any defense against fraud, it is also important for financial institutions to understand the dominant threat drivers that significantly increase the risk of fraud arising from external data compromise events.

Understanding and isolating these factors and drivers helps financial institutions to formulate a response that is more methodical, rigorous, and holistic.

Ecosystem risk factors

Key factors/contributors that elevate risk and fuel the rise in external data compromise events across the globe:

The proliferation of data - the abundance and extent of data being collected by businesses worldwide is a lucrative target for threat actors

The shift to digitization - the rapid migration to digital channels, buoyed by the pandemic, aggravates the risk of data theft and fraud, compounded by weak layers of digital authentication

The lack of investment - a lack of investment by third party organizations in cybersecurity infrastructure and capabilities and the scarcity of expert security professionals[4]

The sophistication of attack modes - the evolution of fraud attacks which are increasingly well-orchestrated and automated, often leveraging sophisticated malwares and bots

Insider threats - employees with access to sensitive data may pose a threat if, intentionally or unintentionally, they cause data leakage

Market threat drivers

Industry-specific nuances that increase the risk of fraud arising from external data compromise events and amplify the resulting effect:

Organized criminal syndicates – cybercriminals adept at harvesting personal information and sensitive data on an industrial scale are becoming more sophisticated and organized, and may operate internationally

Physical mail theft – notwithstanding the increase in sophisticated attacks, the theft of physical mail is a common method of harvesting and misusing personal information

Social engineering - an effective technique for targeting vulnerable individuals and manipulating them into sharing confidential data and personal information

SIM swaps and/or porting - a methodology for compromising and taking over mobile numbers, which is often associated with the broader financial crime modus operandi

Weak authentication – institutions that have not implemented robust protocols (such as biometrics or multi-factor authentication) are often targeted as this creates opportunities for account takeovers (e.g., at call centers, or via online or mobile banking channels)

In today's environment, the challenge for financial institutions in tackling the occurrence of fraud is heightened by the abundance of faster payment mechanisms across the globe.[5] This is another reason why it is important for financial institutions to be prepared in guarding against fraud.

4. Jisc.com, "Lack of investment in cyber security is a false economy', August 2022: https://www.jisc.ac.uk/blog/lack-of-investment-in-cyber-security-is-a-false-economy-24-aug-2022
5. Faster payment solutions include Australia's NPP (New Payment Platform) system, India's RTGS (Real Time Gross Settlement) system, and Singapore's FAST (Fast and Secure Transfers) system.

Understanding the modus operandi

To frame the most effective response in guarding against the related risks, it is useful to consider the ways in which cyber criminals seek to exploit compromised data for monetary gain.

The top three modes of exploiting compromised data

TYPOLOGY	Identity Theft	Account Takeover	Fraudulent Use of Accounts
MODE	**Fraudulent applications to avail credit facilities**	**Fraudulent fund transfers**	**Fraudulent e-commence transactions**
MODUS OPERANDI	Using compromised personal information from a data compromise event, threat actors pose as a bona fide individual. They then approach a financial institution and apply for unsecured credit products such as credit cards, personal loans and, increasingly, buy now pay later services.	Threat actors misuse compromised personal information and account credentials obtained via a data compromise event (e.g., financial information, address, phone numbers, etc.) and often supplement them with data obtained via social engineering techniques. They then get access to and take over an existing account.	Compromised card credentials are obtained via a data compromise event and are used to perpetrate fraudulent transactions. This is not limited to enumeration attacks (which are precursors to card-not-present fraud) and card-not-present fraud.

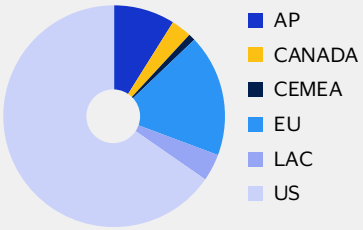
Visa insights

Overview of trends – investigations of cases where payment data was potentially at risk of being compromised

Distribution of cases by region

(October 2021 - September 2022)

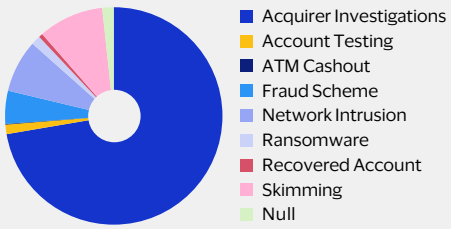
Visa's Global Risk Investigations team observed a 9.2% increase in the number of recorded investigations over the period October 2021 to September 2022 compared to the previous year, with the U.S. region having the largest share of cases at 66%.



Distribution of cases by category

(October 2021 - September 2022)

Our data reveals a 278% increase in the share of skimming investigations over the period of October 2021 to September 2022 compared to the previous year. Meanwhile, fraud scheme investigations increased by 326%. Acquirer investigations, primarily comprising of smaller merchant compromises, constituted the largest proportion of cases at more than 72%.



Best practices - protection measures and responses

VCA works with clients globally to advise on protecting their operations from fraudulent use of compromised data.

Our recommended measures and responses include a combination of tactical and strategic actions to detect anomalous behavior, isolate instances of potential fraud or attacks, and establish a layered defense approach across the lifecycle.

TYPOLOGY	Identity Theft	Account Takeover	Fraudulent Use of Accounts
TACTICAL ACTIONS	• 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)	• Monitor unusual login attempts and successful logins on banking portals • Investigate login concentrations (e.g., IP address, geolocation, device, etc.) for potential linkages • Monitor spikes in overall and account-level volumes at call centers • Identify unusual changes to personal information, and validate such changes with clients using the original data	• Monitor for suspicious activity, particularly in relation to cross-border activities and crypto purchases • Monitor for unexpected changes in transaction patterns, velocity, amounts, merchant types, and merchant countries • Implement robust compromised card lifecycle management processes
STRATEGIC ACTIONS	• Deploy a cutting-edge fraud detection platform for new acquisitions • Augment capabilities leveraging integrated case management, machine learning-based fraud risk scoring, and link analysis • Implement advanced list management capabilities equipped with pioneering phonetic match algorithms (e.g., Soundex)	• Deploy robust authentication controls and protocols at call centers • Leverage advanced authentication capabilities (e.g., voice biometrics, multi-factor authentication, device binding, etc.) • Augment fraud risk mitigation by leveraging behavioral biometrics and investing in malware detection capabilities	• Utilize best-in-class technology and platforms augmented with predictive capabilities • Deploy automated alert disposition capabilities to validate suspicious activity with customers • Deploy fraud risk strategies to monitor portfolio level activity (i.e., extend approach beyond PAN-level activity)

In addition, client awareness sessions focusing on various social engineering techniques and scams, reinforced with education on how to protect personal data, are one of the critical success factors which bolster a client's defenses against fraud.

In all instances, speed is key. This is a dynamic environment in which cyber criminals continually probe for weaknesses in institutions, and these weaknesses can be exploited with devastating speed and severity.

Assessing your level of preparedness

When assessing your readiness to protect your business from fraud, it is important to review your options, and prepare for your response.

1. Readiness

Strategy and framework
Strong fraud risk framework and combative strategies

Fraud risk scoring
Best-in-class risk models and scoring algorithms

List management
Integrated enterprise-level watchlist management

Robust response plan
Comprehensive threat response plan and well-rehearsed execution model

2. Review

Prevention and detection
Robust fraud risk mitigation infrastructure and strategies

Strong authentication
Layered omni-channel authentication capabilities

Fraud intelligence
Germane and actionable cross-spectrum fraud intelligence

Investigation protocols
Robust analysis and investigative procedures

3. Response

Coordinated execution
Seamless, well-orchestrated cross-functional execution

Contact strategies
Established omni-channel client communication and contact strategies

Awareness and education
Thematic and targeted client awareness campaigns

Recovery and deterrence
Efficient recovery strategies, and industry deterrence liaison

Visa's contribution to trust and security

Visa plays a pivotal role in working to strengthen security controls across the payment ecosystem. Over the years, Visa's security roadmap, which involves collaboration with clients, industry partners, and regulatory bodies, has driven significant improvements in the security posture of the wider payment ecosystem.

Historically, roadmaps have included initiatives such as EMV[6] adoption, PCI DSS adoption, PIN mandates, 3D-Secure adoption, and consumer awareness campaigns. Such initiatives are guided by the four pillars of payment security.

Visa's Risk Security Pillars

Devalue Data

Render data useless for criminals, reducing incentive for payment breaches

CREDENTIAL ON FILE TOKENIZATION, EMV CHIP

Empower Consumers

Engage cardholders as an underutilized resource in fighting fraud

TRANSACTION CONTROLS, CONSUMER AWARENESS

Protect Data

Safeguard payment data

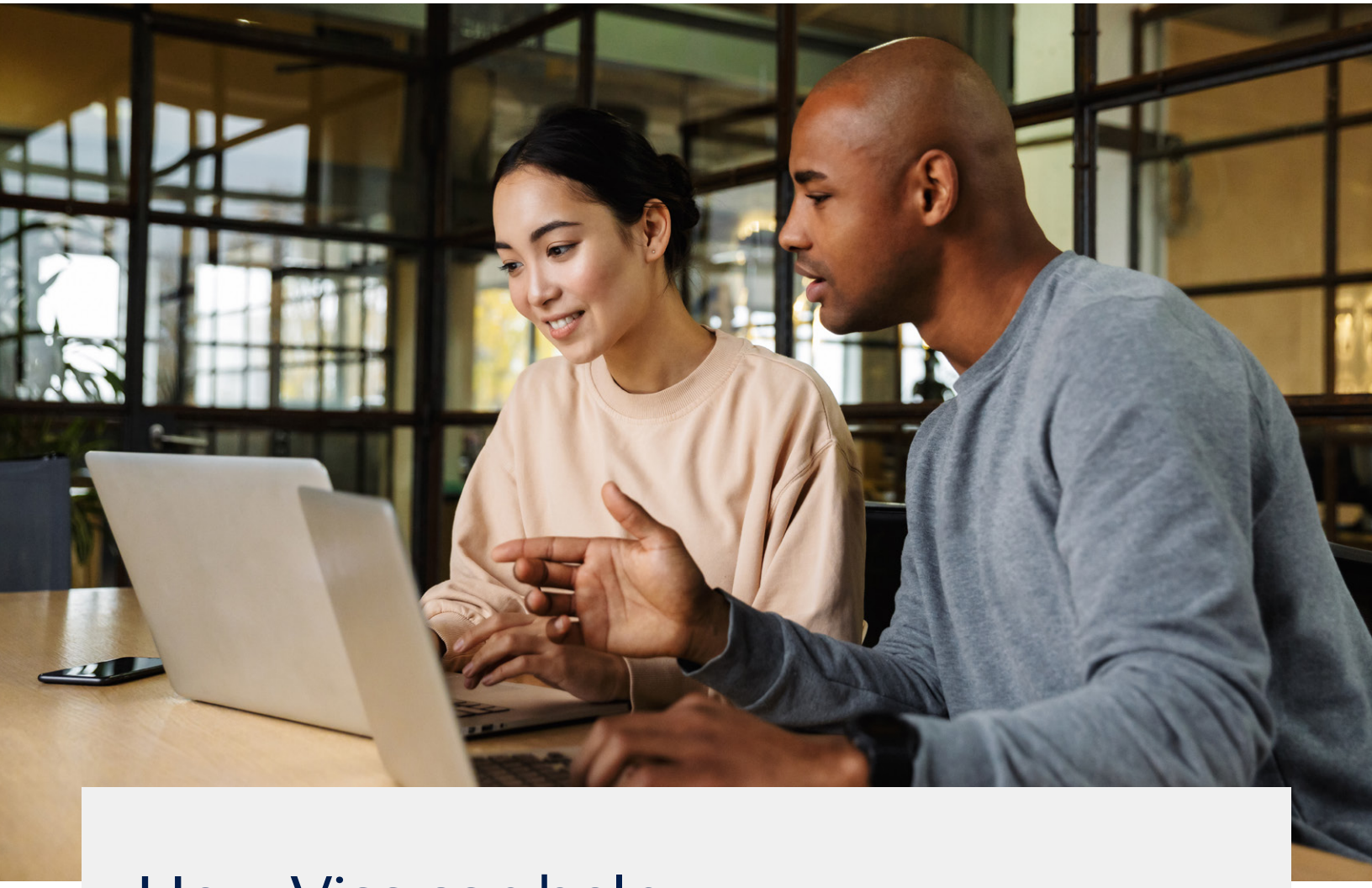
PCI DSS, THIRD PARTY REGISTRATION

Harness Data

Identify fraud before it occurs and increase confidence in approving good transactions

EMV® 3DS[6], RISK SCORING FRAUD DETECTION

6. EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC



How Visa can help

In the face of the threats of fraud arising from external data compromise events, VCA is ideally positioned to work with clients to assess the ways that the risk factors and threat drivers impact their own institution, their level of preparedness, the strategies that ought to be deployed, and how best to implement them. VCA's capabilities include performing comprehensive diagnostics on a client's current control environment and assessing whether response plans are commensurate to the current threat landscape. This enables clients to augment their fraud risk management strategy and provides a framework to optimize security and enhance risk mitigation measures.

In addition to our advisory services, VCA provides a set of data-enabled risk solutions. These solutions draw on a defense-in-depth model, spanning the payment lifecycle, to complement a client's existing risk mitigation capabilities. This enables proactive risk management to be augmented via the use of advanced analytics and machine learning-enabled fraud intelligence.

Visa's proprietary risk solutions utilize global artificial intelligence and machine-learning technologies to detect new and emerging fraud attempts. Clients can set up network-level rules to efficiently manage as the first line of defense against attacks involving data compromise events or enumeration activity. These tools continue to operate effectively, even when a client's host systems are down.

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.

For more information, please contact your Visa Account Executive, email Visa Consulting & Analytics at VCA@Visa.com or visit us at Visa.com/VCA

Follow VCA on

