Visa Consulting & Analytics

COUNTERING EMERGING CYBER THREATS

How businesses can anticipate and address emerging threats from cybercriminals

VISA

everywhere you want to be

Cybercrime has evolved from loosely organized groups targeting individuals to criminal activity that involves highly skilled, well resourced networks of threat actors targeting technology assets of larger corporations and their interconnected infrastructure to access data for malicious reasons.

Today, these organized groups identify vulnerabilities in the ecosystem and seek to take advantage of them at an industrial scale. Cybercriminals are innovative, agile, and quick to adopt or target new technologies. When they spot an opportunity, they scale attacks quickly to maximize their success.

Recent months have been an ideal environment for these cybercriminals. With a surge in digital payments and emerging API-led open banking use cases, their potential attack surface has expanded considerably.

In this paper, Visa outlines the emerging cyber threats and how businesses can address them. With targeted focus, organizations can anticipate threats, address vulnerabilities, and implement the safeguards.

Defining cybercrime in the payment space

Cybercrime is criminal activity where computers or the Internet are the source, target, or place of a crime.

In a payments context, it covers any fraudulent activity that involves the targeting of digitally enabled payment systems and companies that operate in the payments ecosystem.

Cybercrime also includes, but is not limited to, the theft of payment credentials that are stored on or processed by computers and networks; the use of compromised payment credentials to conduct digital payments, such as e-commerce payments; and the use of digital payment systems to monetize other forms of fraud, such as ransom attacks or the theft of government disbursements.

Acknowledging the changing landscape

The past 18 months have proven to be a fertile ground for cybercriminals due to a major shift in consumer behaviors towards digital commerce and companies facing challenges to serve the surge in consumer expectations.

This has led to a rise in cyber fraud incidents, including data breaches, ransomware attacks and phishing scams. Although they are not all payments specific, many have a payments related dimension (either because payment businesses may be the target for similar attacks, or because the cybercriminals intend to use payment systems to monetize their profits).

A larger number of consumers and businesses to target

New consumer behaviors boosted digital payments, with total global e-commerce purchase volumes rising by an estimated US $26.7 trillion during 2020 alone.[1] The rise in consumers transacting online could make them more susceptible to phishing attacks.

A wave of disruption

The world had to adapt quickly with the sudden introduction of work from home, and the implementation of new retail models like Buy Online, Pick Up in Store (BOPIS). Any break from routine tends to favor cybercriminals because they can hide among the behavioral shifts, take advantage that banks and processors are shifting gears and target both merchants and consumers.

A delay in resolving legacy issues

Over several years, the payment sector has been subject to a wave of mergers and acquisitions, which often necessitates the adoption of new technology infrastructure, the integration of different IT operations and the alignment of risk management teams. Any delays in organizations adopting an integrated approach to their technology and cybersecurity management could lead to opportunities for cybercriminals to exploit.

These risks are not theoretical. In the U.S., for example, complaints of suspected internet fraud surged by 61 percent in 2020 alone, according to the FBI's Internet Crime Report. Those fraud events, ranging from personal and corporate data breaches to payment card fraud, phishing and identity theft, cost victims more than US $4.2 billion.[2]

1. UN News, Global e-commerce jumps to $26.7 trillion, fuelled by COVID-19, https://news.un.org/en/story/2021/05/1091182
2. US Federal Bureau of Investigation, 2020 Internet Crime Report, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Five leading cybercrime trends

In recent months, the following cyber fraud trends have captured the attention of payments businesses:

TREND #1

Enumeration attacks (attacks using trial-and-error to guess login info)

Cybercriminals have been using the global surge in e-commerce volumes as cover for their account testing exercises.

Through enumeration attacks, which involve the scalable and programmatic automated testing of common payment fields via e-commerce transactions, their aim is to effectively guess the full payment account number, CVV2 and/or expiration date.

To camouflage their activities, cybercriminals often created COVID-related merchant names and targeted donation related merchants. In some sophisticated attacks, they have directed automated enumeration attempts via globally located e-commerce merchants. Where they have been successful in guessing legitimate account details, an emerging trend has been to use them to purchase cryptocurrencies.

The best solution is for issuers to:

- Step up account monitoring activities (including monitoring API functionality and behavior for bot or scripting attacks)
- Look out for unusually high growth in transaction counts
- Pay attention to declines for invalid account numbers
- Identify flurries of regular authorization requests from the same source (e.g., one every few seconds)
- Implement security safeguards such as IP Allowlist, which indicates what IP addresses can access your account, reCAPTCHA, which enables web hosts to distinguish between human and automated access to websites and device fingerprinting, a process used to identify a device based on its unique configuration

If an attack is suspected, it is important to act fast and investigate. It also pays to look out for authorization requests using sequential account numbers and provide extra protection to any similar numbers, perhaps by applying highly targeted transaction-level blocks.

TREND #2

Rapid emergence of Click and Collect or BOPIS

Among the most significant trends during the past year was the rapid emergence of Click and Collect or BOPIS.

This new model met the needs of merchants and consumers alike but, unfortunately, cybercriminals were quick to spot the security vulnerabilities, then scale up to perpetrate high volumes of fraud.

Typically, cybercriminals use compromised account credentials to conduct fraudulent online purchases or to intercept details of legitimate purchases. They then go to the store to pick up the goods, pretending to be customers.

In this instance, the best solution is for process improvements on the merchant side – for example, by encouraging and enabling customers to protect their online accounts and applying some additional checks at the time of pickup, such as order number verification and ID verification.

TREND #3

Payment-related ransomware

Ransomware attacks have been making headlines for several months. Typically, a cybercriminal will use malware to encrypt data on a company's business critical technology and then demand a ransom payment before agreeing to reinstate the service.

While ransomware is a risk faced by any type of business, cybercriminals are increasingly directing their attacks at the payment ecosystem and evolving their approach accordingly. For example, in addition to or instead of disabling core systems, the perpetrator may also steal payment account data. And, unless ransom demands are met, cybercriminals may threaten to publish this data online or sell it to the highest bidder.

To prevent such attacks, companies should focus on employee education and trainings related to security best practices such as reporting suspicious emails and/or links. Companies should also apply a rigorous approach to cybersecurity, reducing their attack surface, applying robust data security protections and complying with industry standards.

Additionally, companies should implement a defense-in-depth approach that includes detective and preventive controls to prevent threat actors from gaining access to the network and deploying ransomware. If the preventative controls fail to stop the attackers from encrypting the data, the company should have strong backup and recovery capabilities.

TREND #4

Targeting government disbursements

Many governments introduced financial assistance schemes for both employers and citizens over the course of the past year and have been supporting the recovery with stimulus payments.

The rapid rise of these programs creates high risk of fraud and, often, digital payment systems are involved. In the U.S., for example, cybercriminals have used stolen identity credentials to apply for unemployment insurance and then loaded the funds onto prepaid or virtual payment accounts. These are then monetized through the purchase of gift cards, cryptocurrency or electronics or by making person-to-person funds transfers.

In this instance, partnerships between government, law enforcement and the payment industry are the best defense. In addition, issuers can apply additional checks and controls to minimize the risks – such as enhanced identity verification at the account opening/account loading phase and monitoring for suspicious monetization techniques once funds have been disbursed.

TREND #5

POS malware and e-skimming

Payments continues to operate in an ecosystem that relies on the use of account details (full payment account number, the CVV2 and the expiration date).

This data is constantly under intense scrutiny from cybercriminals, who are probing for new ways to obtain fresh details, and an emerging threat is the rise of e-skimming or digital skimming.

Attacks involve the injection of malicious code into a merchant's e-commerce systems to harvest payment card details as they are being entered into the checkout pages. If these attacks are successful, cybercriminals can often maintain access to the compromised servers and move around within the merchant's wider network.

To guard against such attacks, the responsibility is generally on merchants and their vendors to ensure that the latest cyber controls are effectively deployed. For example, good governance will ensure that software is regularly updated and patched, robust firewalls are in place, access to administrative portals is effectively controlled and systems are regularly scanned for vulnerabilities or malware. Also, techniques such as tokenization are increasingly used to desensitize account data.

These five types of cyber fraud are a main concern in the current environment. However, as payments evolve, so too will the techniques of the cybercriminals, and new types of fraud will likely emerge such as cryptocurrency, P2P-related activity and supply chain compromised attacks.

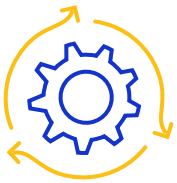
Three categories of threat

In evaluating the risk from cyber fraud, it can be useful to look at the issue through three lenses, which can help to reveal the related vulnerabilities and point towards the most effective solutions.

People-related

This is the BIG one. Almost every successful attack can be traced back to a failure to follow protocols – like someone clicking on a dubious email link, failing to follow password guidance or, in some instances, collusion with cybercriminals (insider threat). This also goes beyond employees and applies to vendors and third parties too, since they often have access to an organization's systems.

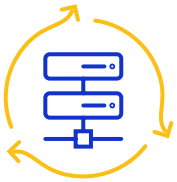
The human dimension is regarded as the weakest link, which requires constant attention – including the effective screening of new hires, training and messaging for all employees, and education and messaging for customers. Some organizations also employ "simulated threat" exercises to identify where gaps in training, process, or technology would strengthen defenses.



Process-related

The rise in curbside pick-up fraud is a good demonstration of the need for risk analysis and robust processes (in this case, enhanced ID verifications), and the consequences if these are overlooked. But globally uniform and unchanging processes can also become a vulnerability (with cybercriminals on the lookout for consistent processes, as well as consistent process anomalies). In addition, sometimes organizations have processes, but don't have a consistent policy around it such as patch management or network security issues.

The situation calls for several protections, such as source code analysis and validation, disciplined incident response services, behavioral analysis, impossible login analysis and system account health – with regular reviews and updates of all processes.



Technology-related

Wherever monetary value is transferred, or payment credentials are collected, processed, stored or transmitted, there will always be risks. And, as more payments are now digital, the enabling technology is under constant scrutiny – this is the reality of operating in the payment sector.

These days, every payment business needs to be a technology business, and any risk management team needs to have deep technology expertise. Organizations should prioritize safeguards including up-to-date threat intelligence, network segmentation and analysis, close monitoring and protection of endpoints, tokenization and biometric authentication.

Two responses for organizations to consider

1

Partner your cybersecurity and payment fraud organizations

Visa has observed that all high-performing risk teams have a shared characteristic – they all take a holistic view of cybercrime, financial fraud and payment risk.

They recognize that their adversaries have a sophisticated knowledge of the payment ecosystem and a bank's role within it. They take the view that cybercriminals understand the type of banking processes, controls and vulnerabilities that stem from siloed organizations and governance. They also understand that the biggest threats tend to reside at the intersections, as do the most effective solutions.

They have structured their teams and processes accordingly. They combine risk management expertise (traditionally associated with fraud management teams) with technology expertise (traditionally associated with cybersecurity teams). Going beyond collaboration, they achieve true co-located and active collaboration.

2

Create a cybersecurity strategy framework - design, define, diagnose, defend - to secure your organization through key security principles

Leading risk teams have established global security principles around identity and access management, cryptography and infrastructure and application security among others. They have also developed a comprehensive cybersecurity strategy anchored by these principles.

Their framework is considered a strategic imperative. As such, they collaborate across lines of businesses such as technology and data teams. They also get executive leadership buy in from the start to get sponsorship and funding.

How Visa can help

Visa has the cybersecurity expertise you need to navigate the changing commerce landscape and protect you from emerging cybersecurity threats through analytics and Artificial Intelligence enabled capabilities.

Meanwhile, VCA is ideally positioned to work with clients to help formulate a cybersecurity strategy, risk governance and compliance assessment and provide cyber training, awareness and education. Similarly, subject matter experts (SMEs) can assist in areas such as operational resilience including vulnerability management and patching, identity and access management, application security and ethical hacking, data protection and incident response readiness assessments.

VCA Cybersecurity Advisory Services

Cybersecurity advisory modules (Created with Visa's SMEs and third-parties)			**Description**
Risk Management (Strategy & Governance)	1	**Cyber Strategy, Architecture and Controls**	Define cyber strategies and actionable roadmaps, security controls and reference architectures in line with the findings of a maturity assessment
	2	**Risk Governance & Compliance**	Enable organization to identify and understand key business risks and cyberthreat exposures and implement necessary enhancements
	3	**Cyber Training, Education and Awareness**	Develop a mature cyber-risk culture by defining and delivering programs to improve technical skills and foster security awareness
Operational Resilience (Operational & Defense Preparedness)	4	**Vulnerability Management & Patching**	Assist with program design and management for the identification, prioritization and remediation of security vulnerabilities and infrastructure weaknesses
	5	**Identity & Access Management (IAM)**	Assist with IAM tools, processes, and methods to enhance security while minimizing friction in the user experience
	6	**Dynamic Application Security Testing**	Assess organization's applications and security controls across the different levels of the enterprise systems using dynamic application security testing methods
	7	**Data Protection**	Assist with the protection of confidential / private data and critical assets within and beyond the boundaries of organization
	8	**Incident Response Readiness Assessment**	Review existing security event detection capability and coverage; analyze the response mechanisms to handle payments / transaction related incidents

About Visa Consulting & Analytics

- Our consultants are experts in strategy, product, portfolio management, risk & cybersecurity, 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.

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

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**

About Visa Risk

Securing the payments ecosystem requires continuous investment and innovation in new technology and collaboration with our business partners. Our job is to protect and enable Visa and its ecosystem partners to be the most secure, resilient, and trusted engine of commerce for everyone, everywhere.

We advance global and local market security initiatives by actively sharing intelligence and best practices, discussing evolving security trends and promoting collaboration on interregional and global risk issues.

Visa Risk also leverages a suite of network-level capabilities, analytics and expertise to protect the safety and soundness of the payments ecosystem and minimize fraud losses for its clients.

Visa Consulting & Analytics is a global team of industry experts in strategy, marketing, operations, risk and economics consulting, with decades of experience in the payments industry. Using analytics from the payment network with the most purchase transactions worldwide, our team of subject matter experts can provide you with proven strategies and data-driven insights that support your business objectives.

