Big on helping you protect small businesses

Enhancing small and medium sized business (SMB) cybersecurity and payment fraud prevention



NOTICE OF DISCLAIMER

Case studies, statistics, research, and recommendations are provided "AS IS"; and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial, or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings, and benefits of any recommendations or programmes may vary based upon your specific business needs and programme requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties, and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions, expected future developments, and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy, or non- timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error-free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental, or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Please note that whilst reasonable endeavours have been taken to ensure that the information in this document is accurate, Visa does not accept any responsibility or liability (whether arising due to breach of contract, negligence, or any other reason) for any incomplete or inaccurate information; or for any loss which may arise from reliance on or use of the information contained in this document. All brand names, logos and/or trademarks are the property of their respective owners, are used for identification purposes only, and do not necessarily imply product endorsement or affiliation with Visa.

©2024 Visa. All rights reserved. Visa Confidential

CONTENTS

01 SMB Security in Asia Pacific 04

02 Enhancing SMB Security: Strategic Approaches 20

03 Conclusion 40

©2024 Visa. All rights reserved. Visa Confidential

01

SMB SECURITY IN ASIA PACIFIC

In Asia Pacific, SMBs are central to a region known for its digital connectivity, technological innovation, and disruptive trends. SMBs also make a crucial contribution to local economies.

>200
MILLION SMALL BUSINESSES SPREAD ACROSS ASIA EMPLOY...

70%
OF THE WORKFORCE AND ARE RESPONSIBLE FOR...

60%
OF THE REGION'S TOTAL GDP.[1]

As digitalisation accelerates, SMBs are increasingly adopting eCommerce and digital technologies, such as digital payments, to bolster their competitive edge. This transition introduces new considerations, particularly in cybersecurity and payment security. While the digital landscape offers substantial opportunities for growth and innovation, it also necessitates a thoughtful approach to managing security challenges. The increase in payment methods and the presence of sophisticated bad actors mean that SMBs must be vigilant in safeguarding their operations and financial stability.

1. Visa, 'Enabling Small Business – The Engine of Growth', September 2023, accessed April 2024.

©2024 Visa. All rights reserved. Visa Confidential

The risk is palpable. According to a recent IBM report, Asia Pacific was the region most impacted by cyber-attacks in 2021 and 2022.[2] In Q1 2024 alone, the Asia Pacific region saw an average of...

2,133 CYBER-ATTACKS ▶ **PER WEEK**
▶ **PER ORGANISATION**

16% ▲ **INCREASE**
FROM THE SAME PERIOD IN 2023.[3]

This alarming rise in cyber-attacks is driven by the widespread availability of advanced technology, including automation and artificial intelligence (AI), which has lowered the barriers to entry for cybercrime, enabling a new generation of cybercriminals – from individual hackers to organised syndicates – to exploit the digital domain for illicit gain.

2. IBM Security, 'X-Force Threat Intelligence Index 2024', 2024, accessed June 2024 (note: ranking is according to the proportion of incident response cases by region to which X-Force responded from 2021 through 2023).
3. Check Point, 'Shifting Attack Landscapes and Sectors in Q1 2024 with a 28% increase in cyber attacks globally', April 2024, https://blog.checkpoint.com/research/shifting-attack-landscapes-and-sectors-in-q1-2024-with-a-28-increase-in-cyber-attacks-globally/

©2024 Visa. All rights reserved. Visa Confidential



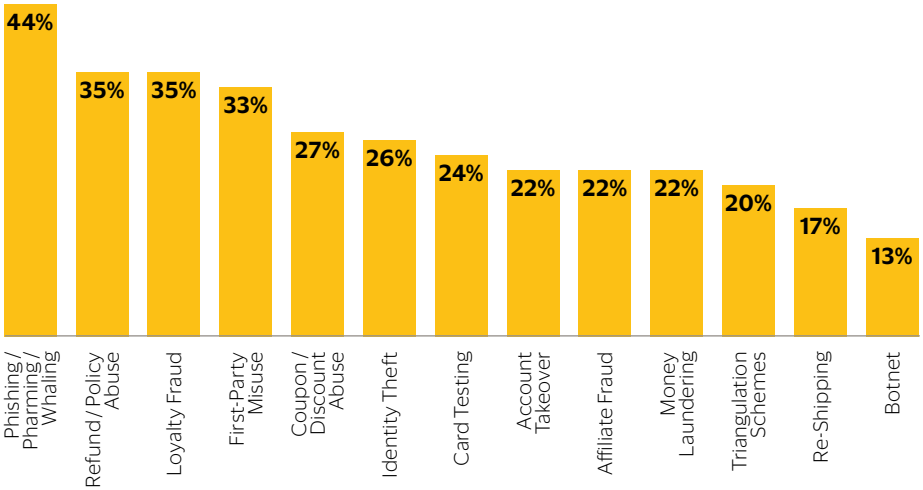
In addition to cybersecurity threats, SMBs in Asia Pacific are facing a rising tide of fraud that threatens their financial stability and business integrity. The rapid adoption of digital payment methods and the growth of eCommerce have made these businesses targets for various types of fraud and scams, including payment fraud, phishing scams, and identity theft. The financial impact of fraud and scams is significant, with SMBs often suffering substantial monetary losses and damage to their reputations. Therefore, SMBs need to adopt a considered approach to digital payments, implementing robust security measures to protect against these evolving threats.

©2024 Visa. All rights reserved. Visa Confidential

Top payment fraud and cybersecurity threats facing merchants and SMBs in Asia Pacific.

According to research by Visa and Cybersource[4], merchants in Asia Pacific, who are often SMBs themselves, experienced an average of 3.4 different types of fraud over the past 12 months. That was fewer than merchants in North America (4.8) and Europe (4.2) but about on par with Latin America (3.2). The most prominent type of fraud, impacting just under half of the region's merchants, is phishing/pharming/whaling. That is followed by refund/policy abuse, loyalty fraud, and first-party misuse, which impacts around one-third of merchants in the region. Globally, refund/policy abuse emerges as the most prominent type of fraud overall, followed by first-party misuse. The findings reflect the susceptibility of merchants in Asia Pacific to various forms of payment fraud, as they digitise and accept a wider array of payment methods.

% merchants in Asia Pacific experiencing each type of fraud in past 12 months, 2024, n=95



Ave. Number of Different Types of Fraud Experienced2024 = 3.4

Source: Visa

4. MRC, Visa Acceptance Solutions, Cybersource, Verifi, '2024 Global eCommerce Payments & Fraud Report, 25th Edition', 2024, accessed May 2024.

©2024 Visa. All rights reserved. Visa Confidential

WHAT IS FIRST-PARTY MISUSE?

First-party misuse, also known as friendly fraud, occurs when a customer makes a purchase and then disputes the transaction with their bank or credit card company to get a refund, despite having received the goods or services. This type of fraud is committed by the customer who originally made the purchase, as opposed to third-party fraud, where an external party uses stolen payment information.

1

HOW IT WORKS

First-party misuse typically involves the following steps:

- **Purchase:** The customer buys goods or services using a credit card.
- **Receipt:** The customer receives the purchased items or services.
- **Dispute:** The customer contacts their bank or credit card company to dispute the charge, claiming that they did not receive the item, the item was defective, or they did not authorise the transaction.
- **Chargeback:** The bank or credit card company issues a chargeback, reversing the transaction and refunding the customer, while the merchant loses the sale amount and incurs additional chargeback fees.

VISA

©2024 Visa. All rights reserved. Visa Confidential

2 WHY SHOULD SMBS CARE?

SMBs should be concerned about first-party misuse for several reasons:

- **Financial Losses:** Chargebacks result in direct financial losses from reversed transactions and additional fees.
- **Increased Operational Costs:** Managing and disputing chargebacks requires time and resources.
- **Inventory Loss:** Merchants lose the goods without receiving payment, impacting inventory management and profitability.
- **Reputation Damage:** High chargeback rates can damage a merchant's reputation with payment processors, potentially leading to higher processing fees or termination of the merchant account.

3 VISA'S VIEW

Visa acknowledges the growing challenge this form of fraud presents to merchants in the digital economy and advocates for robust dispute management and evidence submission to combat it. Visa emphasises the importance of leveraging advanced authentication solutions and providing compelling evidence to support the legitimacy of transactions, thereby reducing fraud rates and improving authorisation rates.

4 VISA'S COMPELLING EVIDENCE 3.0

Visa's Compelling Evidence 3.0, launched in April 2023, empowers merchants to effectively dispute chargebacks from first-party misuse by presenting substantial evidence such as proof of delivery, transaction records, and customer communications. Key benefits include proving delivery, documenting purchase history, and submitting customer interactions, which shifts liability back to the issuer and streamlines dispute handling. This initiative, expected to save small businesses over US$1 billion globally in five years, addresses the rising threat of first-party misuse reported by over 60% of merchants. With 77% of merchants successfully using the updated rules, Compelling Evidence 3.0 plays a crucial role in enhancing fraud prevention and supporting merchant operations worldwide.

©2024 Visa. All rights reserved. Visa Confidential

WHAT ARE PHISHING, PHARMING, AND WHALING?

Phishing, pharming, and whaling are sophisticated cyber-attacks aimed at stealing sensitive information.

1

HOW IT WORKS

Phishing involves attackers sending deceptive emails or messages that appear to come from trusted sources, leading victims to fake websites to capture personal data or install malware. Pharming exploits vulnerabilities or compromises computers to redirect users to fraudulent websites that mimic legitimate ones, tricking them into entering sensitive information. Whaling targets high-profile individuals, using personalised messages that mimic internal communications or trusted partners to convince victims to disclose sensitive information or authorise significant transactions.



©2024 Visa. All rights reserved. Visa Confidential

2 WHY SHOULD SMBS CARE?

SMBs are particularly vulnerable to these attacks due to often limited cybersecurity measures. The consequences of falling victim to phishing, pharming, or whaling can be severe:

- **Financial Losses:** SMBs may suffer significant financial damage from fraudulent transactions or data breaches.
- **Reputation Damage:** Trust and reputation can be severely harmed, affecting customer relationships and business prospects.
- **Operational Disruption:** Cyber-attacks can disrupt business operations, leading to downtime and loss of productivity.
- **Regulatory Penalties:** Failing to protect customer data can result in fines and legal repercussions under data protection regulations.

3 VISA'S VIEW

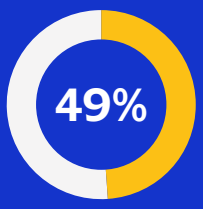
Visa emphasises a multi-layered security approach to protect against phishing, pharming, and whaling. According to Visa, financial institutions and businesses must deploy advanced fraud detection technologies, enhance real-time monitoring, and educate their employees about the latest cybersecurity threats and best practices. Visa advocates for the adoption of strong authentication methods, continuous learning and adaptation of fraud detection models, and robust compliance with data security standards such as the Payment Card Industry Data Security Standard (PCI DSS).

4 VISA SECURE WITH EMV 3-D SECURE

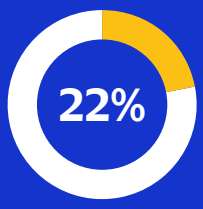
Visa Secure with EMV 3-D Secure is a cutting-edge solution for card-not-present and eCommerce transactions, enhancing security and preventing fraud. Key features include advanced authentication techniques to verify cardholders' identities, real-time risk assessment for informed decision-making, and a seamless user experience across devices to reduce cart abandonment rates. Compliant with PCI DSS, this solution protects cardholder data and maintains high security standards. Since its introduction over 15 years ago, it has processed over 15 billion authentication transactions and achieved a 50% reduction in fraud rates and a 1.22% increase in approval rates globally, helping SMBs safeguard their customers and businesses from cyber threats.

©2024 Visa. All rights reserved. Visa Confidential

Building on these insights, another recent study by Visa[5] found that SMBs globally are more frequently impacted by non-card fraud

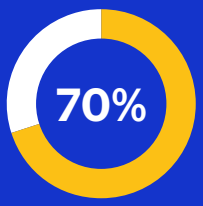


of SMBs reporting such incidents compared with...

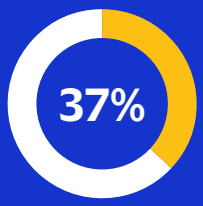


affected by card-related fraud

Among businesses that accept card payments, the disparity is even greater:



have encountered non-card fraud, while...



have faced card-related fraud

INTERESTINGLY

36%

of card-accepting SMBs perceive online card transactions to be more secure than bank transfers.

ADDITIONALLY

39%

believe that card transactions reduce the risk of having cash on the premises.

These findings highlight that SMBs value the security of card transactions, both online and offline. While new forms of digital payments offer flexibility and convenience, they also expose businesses to bad actors and fraud types, particularly in card-not-present scenarios. This underscores the importance of tokenisation, which can enhance the security of these transactions.

5. Visa SMB research conducted by Visa Merchant Sales & Acquisition Asia Pacific, 2023.

©2024 Visa. All rights reserved. Visa Confidential

Top cybersecurity and payment fraud management challenges for SMBs and merchants in Asia Pacific.

SMBs face significant challenges in managing cybersecurity and payment fraud, making them prime targets for sophisticated fraudsters. One of the primary reasons SMBs are vulnerable is their often inadequate cybersecurity solutions. Keeping pace with rapid technological changes and the ever-changing landscape of cyber threats is daunting for these businesses. Many SMBs acknowledge the difficulty of staying updated with security requirements and threat dynamics. Furthermore, internal challenges such as engaging employees in security responsibilities, navigating the complexity of the industry, and recruiting skilled personnel add layers of difficulty in enhancing cybersecurity resilience.

When it comes to eCommerce, merchants of all sizes across the region identify challenges along similar lines. Gaps in fraud tool capabilities represent merchants' biggest overall challenge in fraud management. Data availability and access, responding to new fraud attacks, lack of internal resources, and fraud tool customisation are other high-level challenges inhibiting many merchants in Asia Pacific in their fraud prevention efforts.

©2024 Visa. All rights reserved. Visa Confidential

Top five fraud management challenges for merchants in Asia Pacific, all sizes, 2024

1. Gaps in fraud tool capabilities
2. Data availability and access
3. Responding to new fraud attacks
4. Lack of internal resources
5. Fraud tool customisation

Source: Visa

Given these challenges, there is a pressing need for assertive leadership and strategic guidance from ecosystem players to help SMBs navigate the intricate landscape of financial security and fraud. The marketplace's competitive nature, where product features can be quickly replicated and price wars are common, underscores the importance of being a trusted and secure business.

For SMBs, elevating trust and security from operational necessities to strategic imperatives is not just beneficial – it is essential. Doing so not only protects the business from potential threats but also strengthens its position in the market, building lasting trust with customers, partners, and the broader business ecosystem.

©2024 Visa. All rights reserved. Visa Confidential

Impact of security breaches and fraud on SMBs and merchants in Asia Pacific.

The impact of security breaches and fraud on SMBs and merchants in the region is profound. They affect not only businesses' immediate financial health but also their long-term viability and relationships with customers and partners.

Starting with eCommerce payment fraud, metrics from a recent survey conducted by Visa and Cybersource[6] underscore the severity of the issue: merchants of all sizes in Asia Pacific report that 3.3%, or US$33 out of every US$1,000, of their total eCommerce revenue is lost annually to payment fraud, a significant financial drain. Furthermore, 3.6%, or US$36 out of every US$1,000, of Asia Pacific merchants' accepted eCommerce orders turn out to be fraudulent, and an additional 5.5%, or US$55 out of every US$1,000, of Asia Pacific merchants' orders are rejected due to fraud suspicions. Complicating matters, these merchants have a dispute win rate of less than 20 %, or US$156 out of every US$1,000, highlighting the difficulties they face in contesting fraudulent transactions successfully.

Fraud Impact KPIs – Asia Pacific merchants, all sizes, 2024

Fraud impact KPIs (trimmed averages shown)		2024
Fraud rate by revenue	% of total annual e-commerce revenue lost to payment fraud globally	**3.3%** **2.9%**
Fraud rate by order	% accepted orders in past 12 months that turned out to be fraudulent	**3.6%**
Order rejection rate	% eCommerce orders rejected due to suspicion of fraud in past 12 months	**5.5%**
Chargeback / dispute win rate	Annual % of fraud-coded chargebacks & disputes won by the merchant	**15.6%**

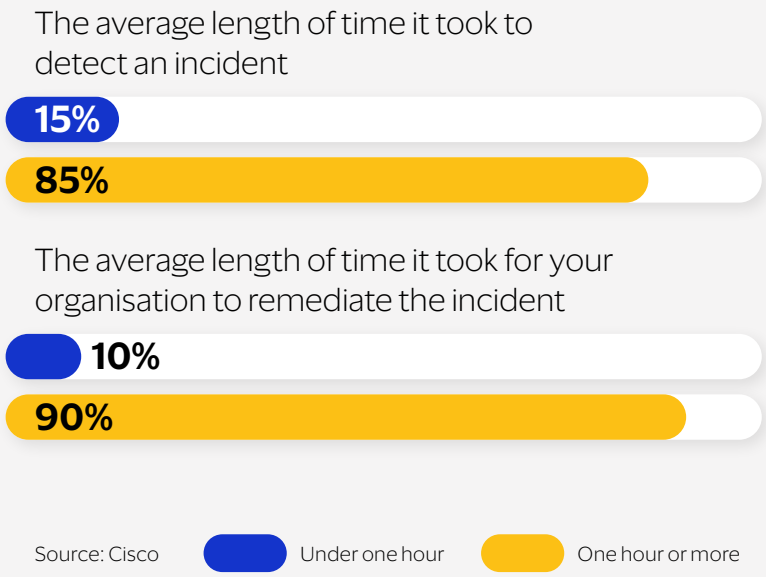
Source: Visa 2023 figures

6. MRC, Visa Acceptance Solutions, Cybersource, Verifi, '2024 Global eCommerce Payments & Fraud Report, 25th Edition', 2024, accessed May 2024.

©2024 Visa. All rights reserved. Visa Confidential

Turning to security breaches, the significant challenge SMBs face in the region is underscored by the finding that only 15% of respondents can detect a cyber incident within an hour. Even fewer, just 10% of surveyed respondents, can resolve it in the same time frame.[7]

Average detection and remediation times for cyber incidents in Asia Pacific SMBs in past 12 months prior to 2021 survey, % of respondents

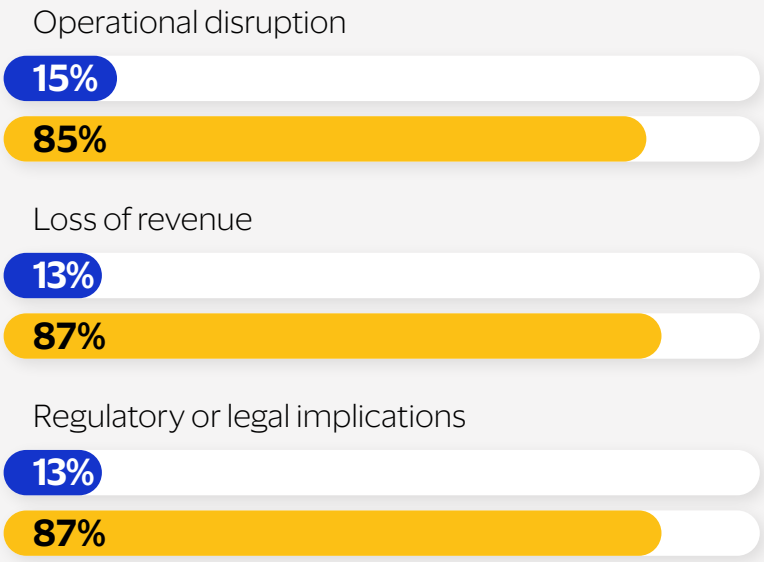


7. Cisco, 'Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense', September 2021, accessed April 2024.

©2024 Visa. All rights reserved. Visa Confidential

The speed of response is crucial, as a slow reaction can severely impact a business. A majority (85%) of SMBs in Asia Pacific indicated that downtime extending beyond one hour disrupts operations, while 87% said that such downtime results in revenue loss and regulatory or legal implications for them.[8]

Escalation of impact due to length of downtime for Asia Pacific SMBs, % reporting, 2021 survey



Source: Cisco

Less than one hour downtime

One hour or more downtime

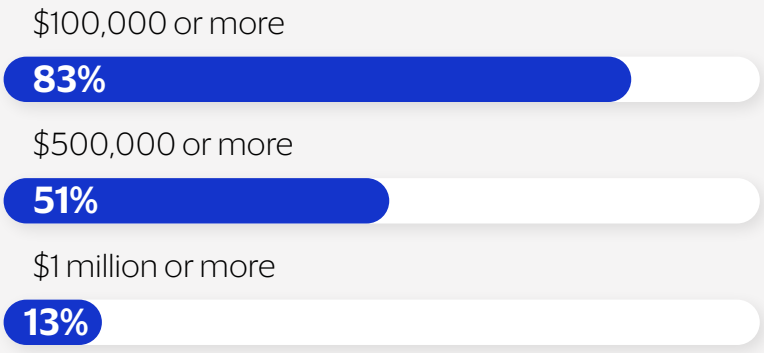
8. Ibid.

©2024 Visa. All rights reserved. Visa Confidential

There is also a monetary impact beyond just the loss of revenue. Over half of the SMBs in the region experiencing cyber incidents reported costs of US$500,000 or more; for 13% of respondents, these costs exceeded US$1 million. Overall, 83% of surveyed SMBs in the region said that the cost of incidents was more than US$100,000.[9]

There is also an intangible cost. Many affected SMBs in the region would also have experienced a significant loss of customer trust and a tarnished reputation after such events. While difficult to measure, a decline in reputation and erosion of trust can lead to severe consequences for any business.

Financial impact of cyber incidents on Asia Pacific SMBs in the past 12 months prior to 2021 survey, US$, % of affected businesses



Source: Cisco

9. Cisco, 'Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense', September 2021, accessed April 2024.

©2024 Visa. All rights reserved. Visa Confidential



This challenging environment highlights the urgent need for SMBs in the Asia Pacific region to enhance their cybersecurity and fraud prevention measures. Investing in advanced security technologies, adopting rigorous protocols, and fostering a security culture are essential steps towards mitigating these risks. Furthermore, collaboration with technology partners and adherence to evolving cybersecurity guidelines and regulations are crucial in navigating this perilous landscape. By fortifying their defences and responding swiftly to incidents, SMBs can better protect their financial assets, maintain customer trust, and secure their future in a rapidly evolving digital economy.

©2024 Visa. All rights reserved. Visa Confidential

02

ENHANCING SMB SECURITY: STRATEGIC APPROACHES

To address the threats, SMBs must adopt robust security strategies. These include focusing on data-driven security, leveraging partners' expertise and technology, and being proactive in staying ahead of the fraud curve.

Data-driven security: growing relevance of AI/machine learning (ML).

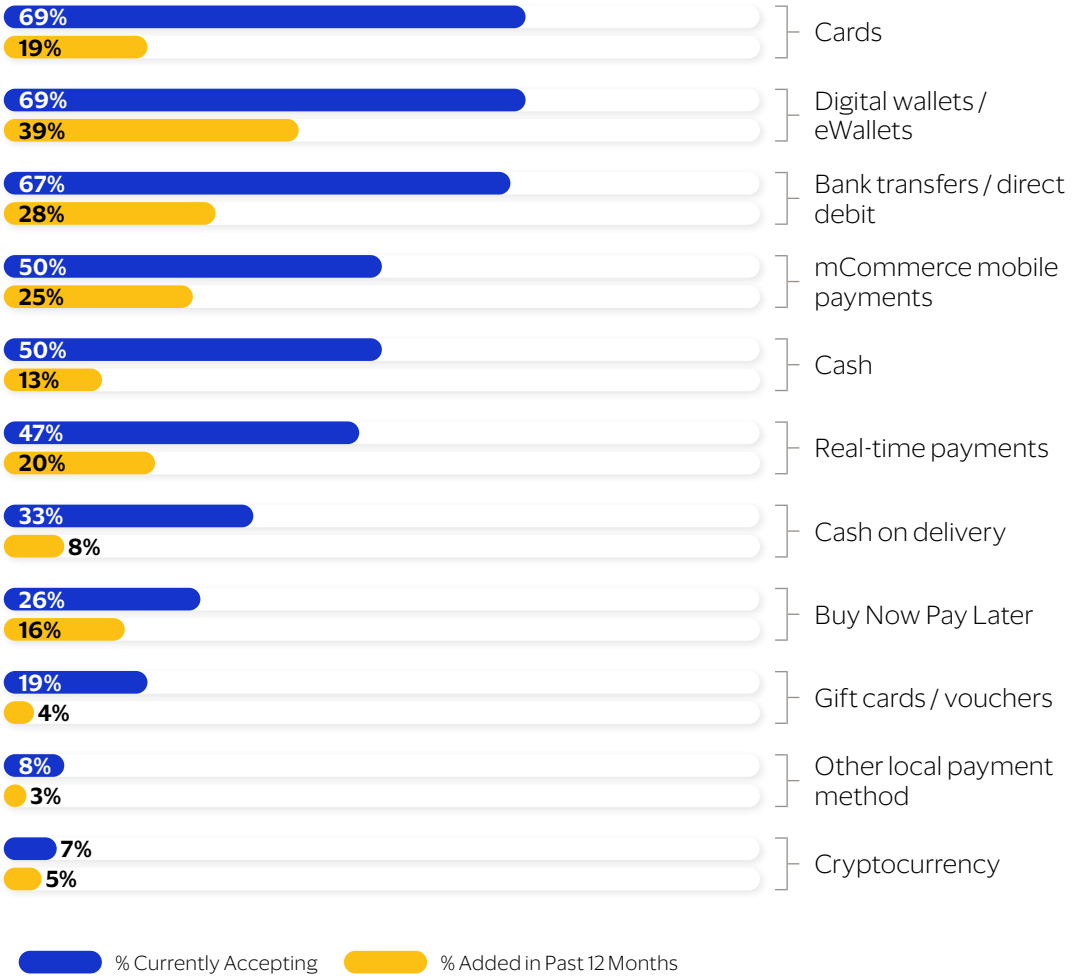
In the rapidly evolving landscape of digital payments, SMBs face the dual challenge of adapting to consumer demands for diverse payment methods while mitigating the increasing risks of fraud accompanying these innovations. Leveraging transaction data and analytics becomes crucial in identifying risks and implementing proactive fraud prevention strategies that balance robust security with seamless customer experiences.

©2024 Visa. All rights reserved. Visa Confidential

Widespread adoption of diverse payment methods.

According to research by Visa and Cybersource[10], merchants of all sizes in Asia Pacific accept four to five different payment methods on average from their customers. Card, digital wallet payments, and debit transfers are the top three acceptance methods, each used by roughly two-thirds of merchants in Asia Pacific. Half of the merchants in the region also accept mobile payments, cash, and real-time payments (RTP). Digital wallets/ eWallets, bank transfers, and mCommerce have experienced the most explosive growth in the past 12 months, while Buy Now Pay Later (BNPL) has also experienced a comparatively high growth rate over the same period.

Payment methods currently accepted & added in past 12 months, 2024 survey of Asia Pacific merchants, all sizes



Ave. Number Currently Accepted = 4.4
Not shown in chart: 18% indicating no new payment methods added in past year

Source: Visa

10. MRC, Visa Acceptance Solutions, Cybersource, Verifi, '2024 Global eCommerce Payments & Fraud Report, 25th Edition', 2024, accessed May 2024.

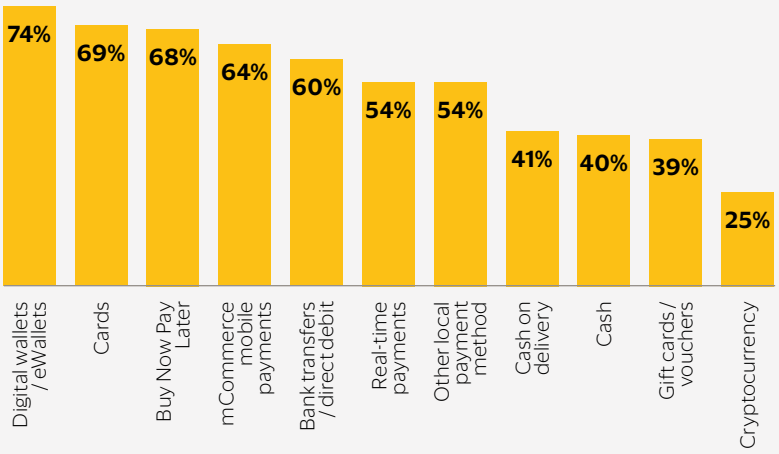
©2024 Visa. All rights reserved. Visa Confidential

However, while enhancing customer experience and potentially increasing sales, the diversity of payment options also broadens the attack surface for fraudsters. There is a clear connection between the popularity of a payment method and its associated fraud risk or rate. When asked about the payment methods with the highest fraud rates, merchants in the region identified digital wallets and cards as the top two, followed by BNPL, mobile payments, debit transfers, and RTP.[11]

Ranking payment methods by highest fraud rates according to merchants in Asia Pacific .

This ranking matches closely with the most popular payment methods, showing a direct link between a payment method's popularity and its fraud risks. Widely accepted methods , such as digital wallets and cards, experience higher fraud rates. This pattern implies that as payment methods become more ingrained in consumer habits, they also become more attractive targets for fraudsters. Similarly, BNPL, mobile payments, debit transfers, and RTP, which are quickly gaining popularity, are seeing rising fraud rates.

% Merchants in Asia Pacific ranking each payment method in top three for highest fraud rates, 2024



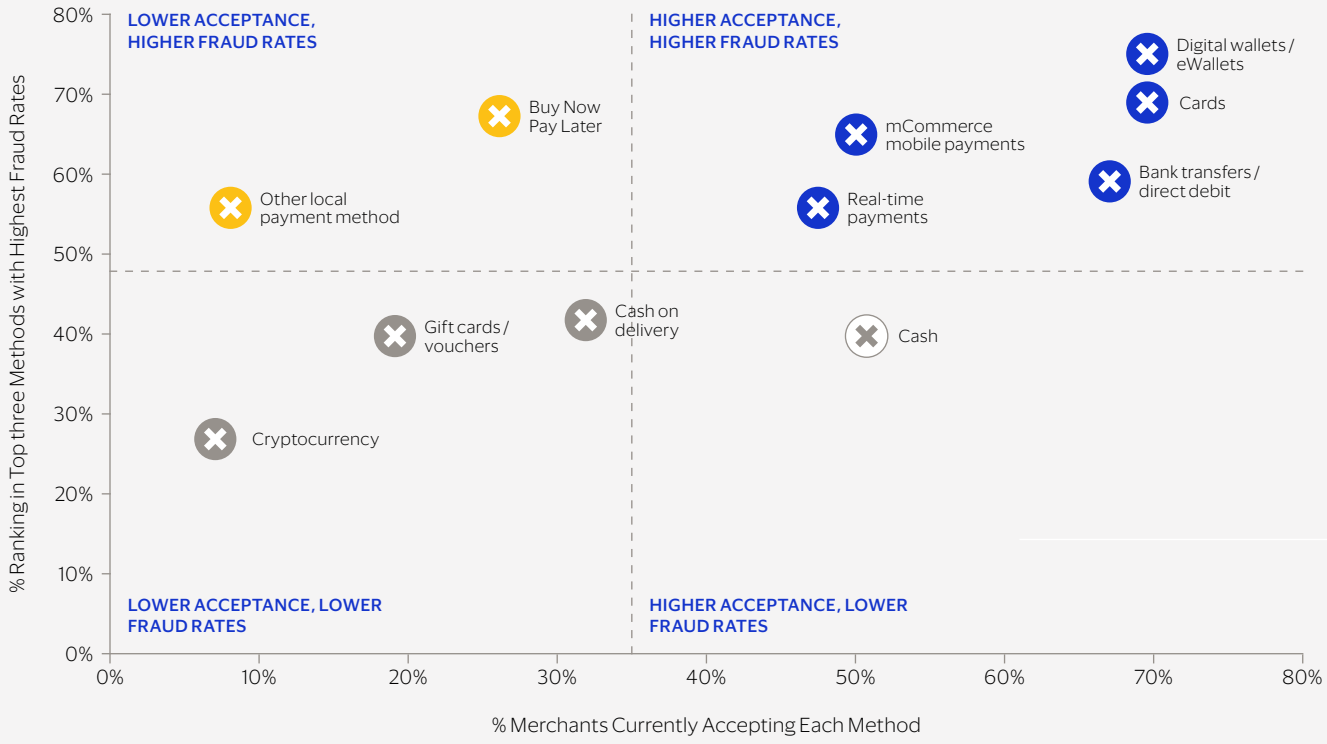
Source: Visa

11. Ibid.

©2024 Visa. All rights reserved. Visa Confidential

The correlation between payment acceptance methods and fraud rates.

Payment method acceptance vs. fraud rates per merchants in Asia Pacific, 2024 survey.



Source: Visa

©2024 Visa. All rights reserved. Visa Confidential

WHAT IS REAL TIME PAYMENTS FRAUD?

RTP fraud refers to fraudulent activities that exploit RTP systems. RTP systems allow the instant transfer of funds between accounts, providing immediate confirmation to both sender and recipient. The speed and irrevocability of these transactions make them attractive targets for fraudsters. Common types of RTP fraud include unauthorised transactions and social engineering scams such as fraud, where individuals are tricked into authorising payments to fraudulent accounts.

1

HOW RTP FRAUD WORKS

RTP fraud typically occurs in two primary ways:

- **Unauthorised Fraud:** Fraudsters gain unauthorised access to a bank account through phishing, malware, or data breaches and initiate transactions without the account consent. The instantaneous nature of RTPs leaves little time to detect and stop these fraudulent transactions.
- **APP Fraud:** Fraudsters manipulate victims into authorising payments to their accounts. This is often done through social engineering tactics, such as pretending to be a legitimate entity (e.g. a bank or a trusted service provider) and convincing the victim to transfer money.

©2024 Visa. All rights reserved. Visa Confidential

2 WHY SHOULD SMBS CARE?

SMBs are particularly vulnerable to RTP fraud due to several reasons:

- **Financial Impact:** Fraudulent transactions can result in significant financial losses, which can be devastating for SMBs operating with limited financial resources.
- **Trust and Reputation:** Incidents of fraud can erode customer trust and damage the reputation, impacting long-term viability.
- **Regulatory Compliance:** SMBs must adhere to financial regulations and standards. Failure to implement adequate fraud prevention measures can lead to regulatory penalties and legal issues.

3 VISA'S VIEW

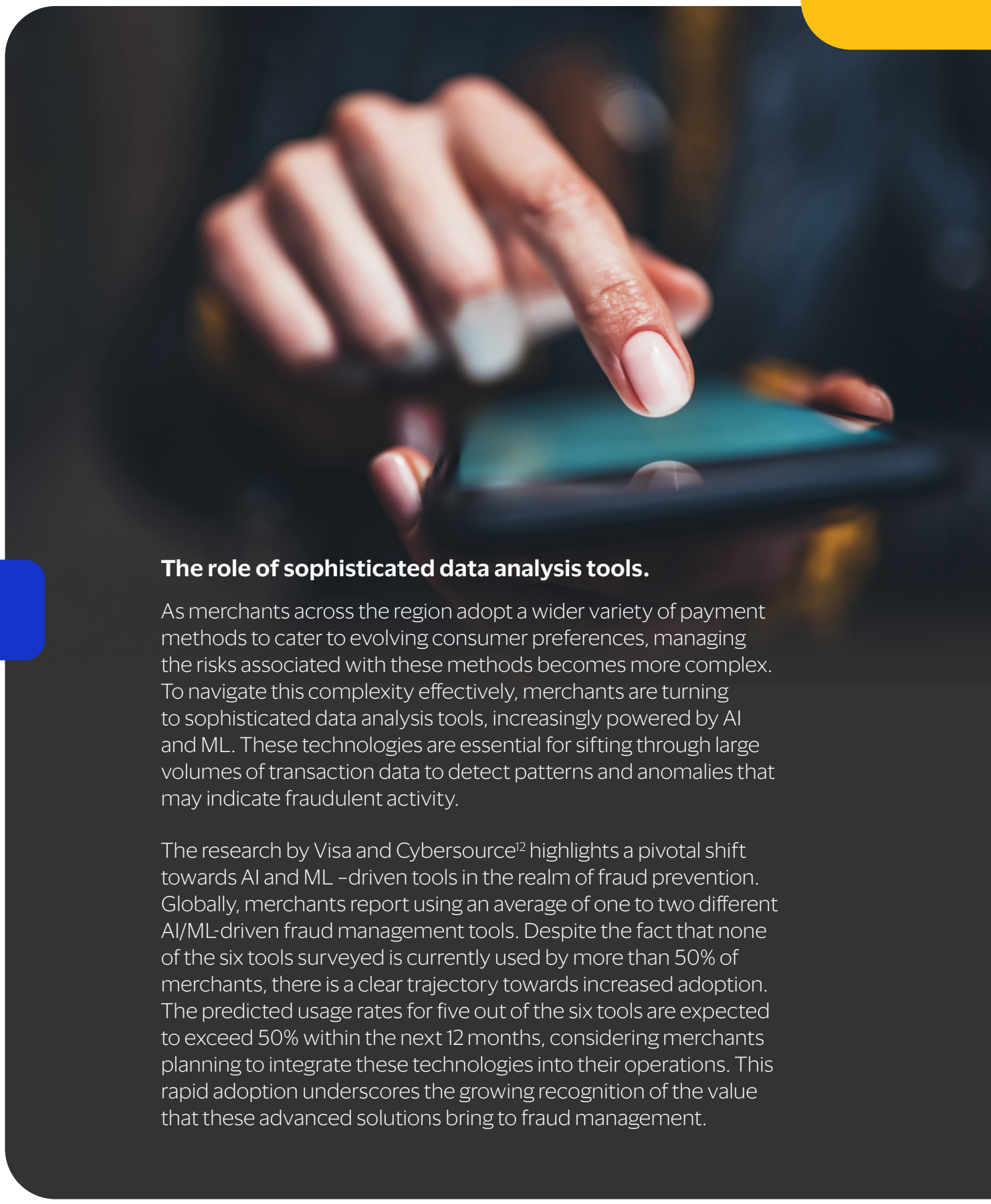
Visa recognises the significant challenges posed by RTP fraud and advocates for a multi-layered approach to mitigate risks. According to Visa, financial institutions must deploy advanced fraud detection technologies, enhance real-time monitoring, and foster collaboration across the payments ecosystem to combat sophisticated fraud tactics.

Visa emphasises the importance of leveraging AI and ML to detect and prevent fraudulent activities in realtime. By continuously evolving fraud detection models, financial institutions can better anticipate and counter emerging fraud schemes.

4 VISA PROTECT FOR A2A PAYMENTS

Visa Protect for A2A Payments is a powerful solution aimed at mitigating RTP fraud. Utilising advanced AI, it offers real-time transaction risk scoring and multi-financial institution risk assessment. Key features include AI-driven real-time risk scoring for informed payment authorisation decisions, assessment of risk associated with both the originating and beneficiary parties, and continuous learning to adapt to new fraud patterns. Successfully implemented globally and set to launch in the AsiaPacific region in Q3 2024, Visa Protect enhances RTP network security, equipping SMBs and financial institutions with essential tools to combat fraud and maintain customer trust.

©2024 Visa. All rights reserved. Visa Confidential



The role of sophisticated data analysis tools.

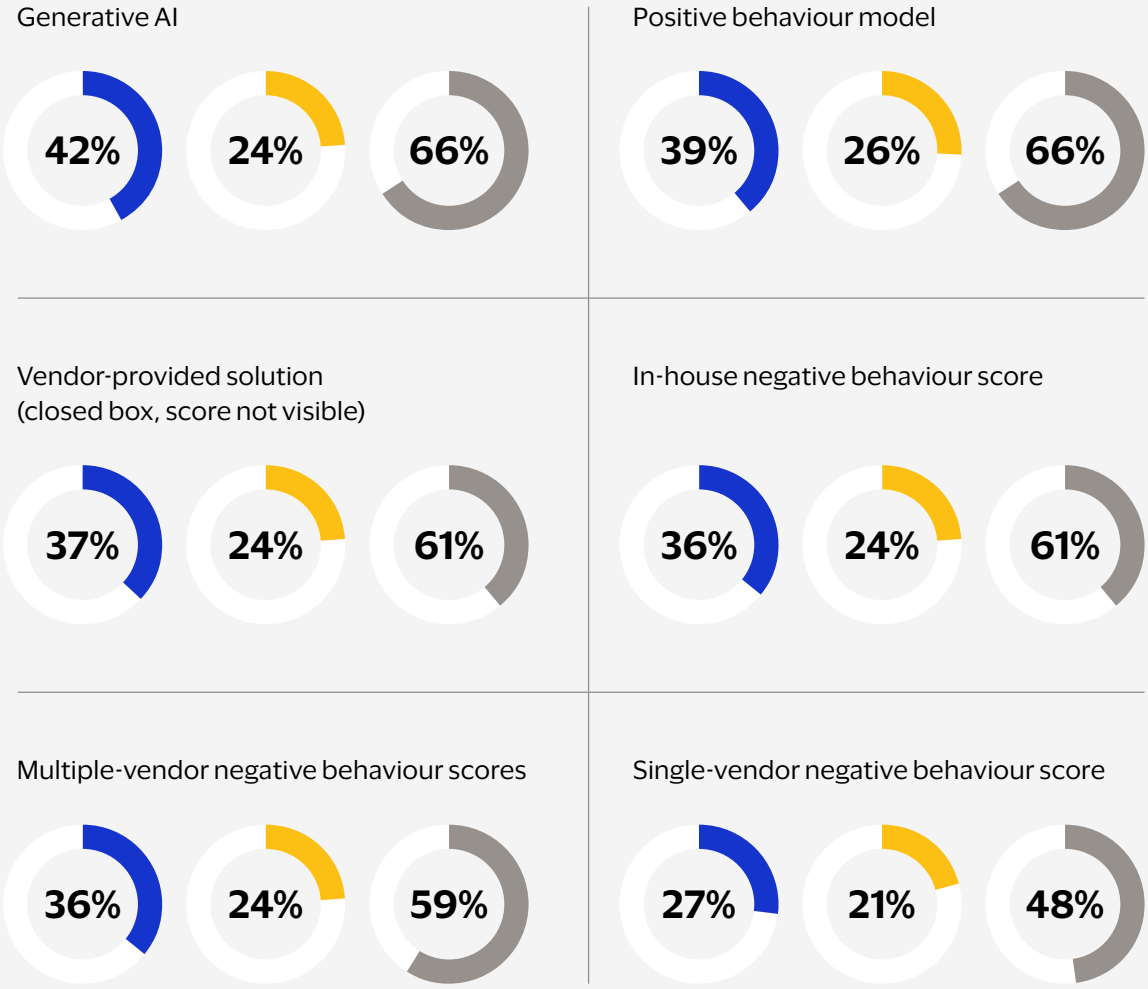
As merchants across the region adopt a wider variety of payment methods to cater to evolving consumer preferences, managing the risks associated with these methods becomes more complex. To navigate this complexity effectively, merchants are turning to sophisticated data analysis tools, increasingly powered by AI and ML. These technologies are essential for sifting through large volumes of transaction data to detect patterns and anomalies that may indicate fraudulent activity.

The research by Visa and Cybersource[12] highlights a pivotal shift towards AI and ML –driven tools in the realm of fraud prevention. Globally, merchants report using an average of one to two different AI/ML-driven fraud management tools. Despite the fact that none of the six tools surveyed is currently used by more than 50% of merchants, there is a clear trajectory towards increased adoption. The predicted usage rates for five out of the six tools are expected to exceed 50% within the next 12 months, considering merchants planning to integrate these technologies into their operations. This rapid adoption underscores the growing recognition of the value that these advanced solutions bring to fraud management.

12. MRC, Visa Acceptance Solutions, Cybersource, Verifi, '2024 Global eCommerce Payments & Fraud Report, 25th Edition', 2024, accessed May 2024.

©2024 Visa. All rights reserved. Visa Confidential

Current+planned usage of AI/ML-driven fraud management tools, all regions, all merchant sizes, 2024, n=499



Source: Visa

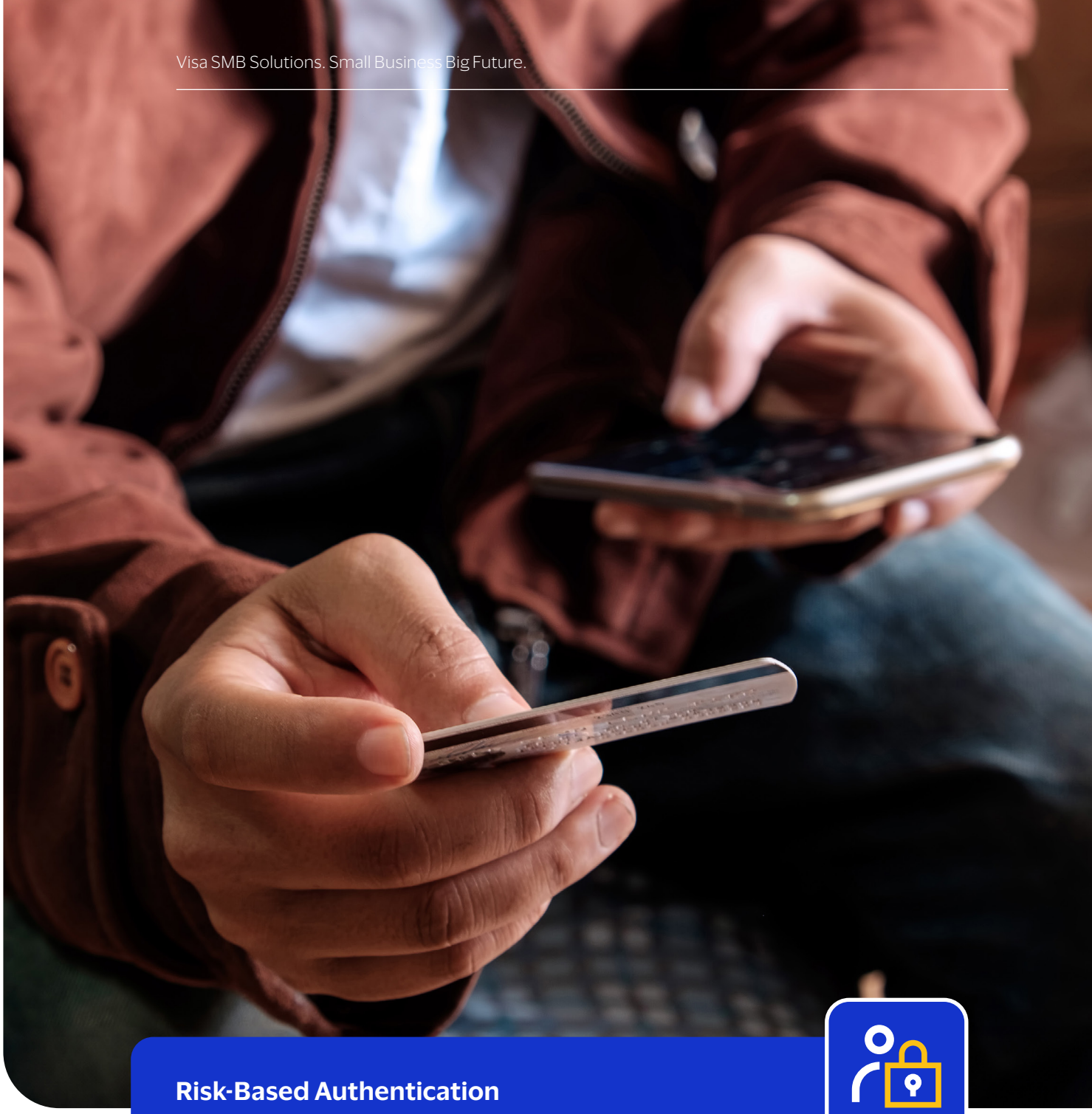
Currently Using

Likely to Add In Next 12 Months

Current + Planned Usage

Not shown in chart: 3% selecting don't know or prefer not to say

©2024 Visa. All rights reserved. Visa Confidential



Risk-Based Authentication

One effective approach to balancing robust security and a seamless customer experience is the implementation of risk-based authentication (RBA). RBA tools assess the real-time risks associated with each transaction, considering factors such as device usage and past spending behaviour. These tools enable issuers to confidently decline high-risk transactions, significantly enhancing security measures. By accurately identifying critical junctures in the customer journey, such as account opening, first transactions, and token provisioning, SMBs can implement appropriate risk controls to ensure a secure yet efficient process.

©2024 Visa. All rights reserved. Visa Confidential

Payment partnerships: leverage the expertise and strength of partners' networks.



Payment partnerships are increasingly pivotal for SMBs in the Asia Pacific region, particularly as these enterprises seek to expand their market reach and enhance transaction security. These partnerships do not merely facilitate the transactional aspects of business but also bring a wealth of technological and security benefits, pivotal for thriving in today's digital economy.

©2024 Visa. All rights reserved. Visa Confidential

Visa and Cybersource's[13] recent survey revealed that the involvement with payment gateways and acquiring banks remains a fundamental aspect of merchants' payment strategies. On average, a merchant in the region collaborates with four to five different payment gateways or processors and three to four acquiring banks.

Usage of Payment Processors and Acquiring Banks – Asia Pacific merchants, all sizes, 2024

Usage of payment partners (trimmed averages shown)	2024
#of payment gateway or processor connections currently supported	**4.4%**
# of merchant acquiring banks currently used	**3.7%**

Source: Visa

Diversifying payment partnerships allows businesses to handle various payment methods and navigate different market landscapes effectively. These partnerships enhance operational flexibility, improve authorisation rates and uptimes, and increase geographic coverage. They also help businesses gain access to distinctive technologies or capabilities, including, but not limited to, enhanced security.

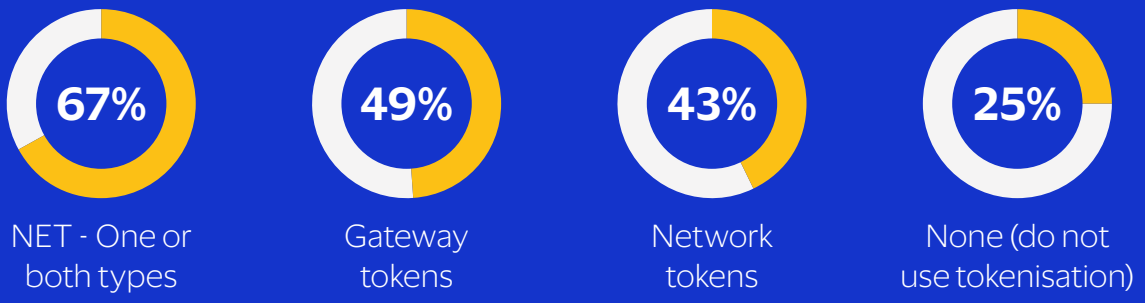
13. MRC, Visa Acceptance Solutions, Cybersource, Verifi, '2024 Global eCommerce Payments & Fraud Report, 25th Edition', 2024, accessed May 2024.

©2024 Visa. All rights reserved. Visa Confidential

A look at tokenisation

In the evolving landscape of digital payments, SMBs are increasingly reliant not just on the transactional benefits of payment services but also on the secure technologies that underpin these services. One of the most significant advancements in this regard is tokenisation, a technology that greatly enhances payment security by replacing sensitive customer data with a unique digital identifier.

Usage of tokenisation in payment management, % merchants, all regions, all sizes, 2024, n=667



Source: Visa

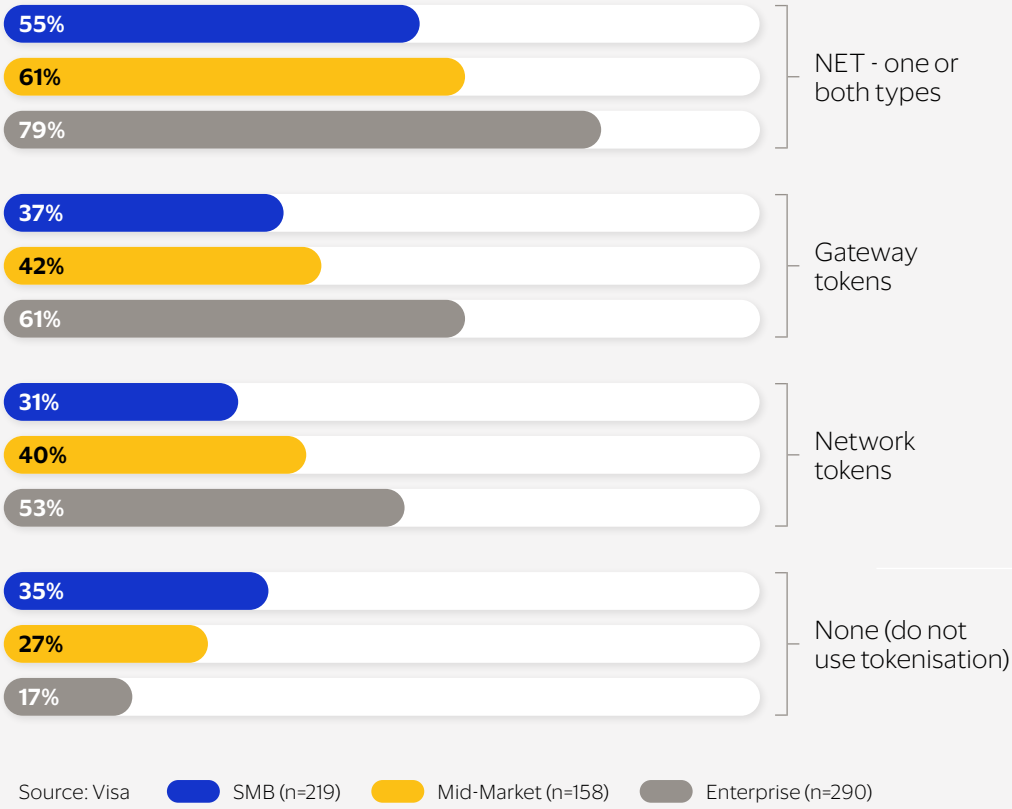
Not shown in chart: 8% selecting don't know or prefer not to say

Tokenisation minimises the exposure of sensitive information during transactions, which is crucial for preventing fraud and enhancing data security. According to research by Visa and Cybersource,[14] while two-thirds of merchants globally already employ some form of tokenisation, there is a notable disparity in adoption rates between larger enterprises and SMBs. While 79% of enterprise merchants use one or both types of tokenisation methods – gateway tokens and network tokens – only about 55% of SMBs are currently utilising any form of tokenisation.

14. MRC, Visa Acceptance Solutions, Cybersource, Verifi, '2024 Global eCommerce Payments & Fraud Report, 25th Edition', 2024, accessed May 2024.

©2024 Visa. All rights reserved. Visa Confidential

Usage of tokenisation in payment management, % merchants, all regions, by merchant size, 2024



This discrepancy underscores a critical gap in the security measures between larger corporations and smaller businesses. Larger enterprises often have more resources to invest in advanced technologies such as tokenisation, which can lead to a more robust security posture. SMBs, on the other hand, might face constraints in resources, but they have a significant opportunity to enhance their security measures by adopting similar technologies.

©2024 Visa. All rights reserved. Visa Confidential

The primary motivation for using tokenisation, as identified by the majority of merchants globally in the survey, is to improve data security and reduce the risks associated with data breaches. Merchants in the Asia Pacific region are especially likely to cite security/data protection as their top reason for using tokenisation. However, the benefits of tokenisation extend beyond just security.

Reasons for using tokenisation in payment management (2022-2024), % merchants, all regions, all merchant sizes



Source: Visa 2024 (n=445) 2023 (n=582) 2022 (n=684)

©2024 Visa. All rights reserved. Visa Confidential

Merchants also recognise that tokenisation can improve authorisation rates and foster greater trust with customers, providing them with better and more innovative payment experiences. These benefits are crucial for SMBs as they seek not only to protect themselves from the increasing threat of cyber-attacks but also to enhance their customer service and operational efficiency.



©2024 Visa. All rights reserved. Visa Confidential

VISA'S TOKENISATION MILESTONES AND ANNOUNCEMENTS

CELEBRATING

1Bn ▸ 2Bn

payment tokens and USD

uplift to digital commerce in Asia Pacific

In 2023, the Asia Pacific digital economy saw an uplift of over US$ 2 billion due to the adoption of Visa Token Service (VTS), with 1 billion tokens issued in the region. VTS enhances digital commerce by replacing sensitive payment information with unique digital identifiers, significantly reducing the risk of fraud and data breaches. Merchants using VTS have experienced a 58% reduction in payment fraud rates and a higher payment success rate, resulting in a US$2 billion increase in revenue. The service also ensures uninterrupted payments despite changes in card credentials, providing a seamless user experience and contributing to a safer, simpler, and smarter digital commerce environment.

©2024 Visa. All rights reserved. Visa Confidential

Education and upskilling: beyond the tools, SMBs must be proactive to stay ahead of the fraud curve.

In the battle against cyber threats, SMBs in the Asia Pacific region are not merely on the defensive; they are actively engaging in tactics to bolster their cybersecurity resilience. Education and upskilling emerge as pivotal elements in this proactive stance.

81% of SMBs in Asia Pacific have engaged in scenario planning and/or simulations, a practice that tests their readiness and, more crucially, exposes vulnerabilities in their current security frameworks.[15]

95% of these SMBs found that they lacked the appropriate technology solutions to detect cyber threats, and an equal number struggled with the integration of multiple technologies.

96% of SMBs surveyed realised that they did not have the necessary technology in place to block an attack effectively. The exercises also shed light on organisational preparedness.

94% of SMBs identifying unclear processes for responding to cyber incidents.[16]

15. Cisco, 'Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense,' September 2021, accessed April 2024.
16. MRC, Visa Acceptance Solutions, Cybersource, Verifi, '2024 Global eCommerce Payments & Fraud Report, 25th Edition', 2024, accessed May 2024.

©2024 Visa. All rights reserved. Visa Confidential

95% 

of respondents acknowledged that although the right technologies were in place, there was a notable shortage of skilled personnel to effectively utilise these systems.

This underscores the critical need for continual employee training and skills development to ensure that staff can operate and maximise the benefits of advanced cybersecurity technologies.[17]

Education extends beyond internal operations to include a broader understanding of the cybersecurity landscape, including compliance with local legal and regulatory requirements. This area represents a significant knowledge gap, with nearly one in five (17%) SMB leaders admitting to a limited understanding of these critical elements.[18]

The scenario clearly illustrates that while SMBs are making strides in scenario planning and technological integration to bolster cybersecurity, there remains a substantial need for enhanced education and upskilling. By addressing these needs, SMBs not only strengthen their defences but also empower their teams to leverage technology more effectively, ensuring that they stay ahead of the rapidly evolving fraud curve.

17. Cisco, 'Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense', September 2021, accessed April 2024.
18. Cisco, 'Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense', September 2021, accessed April 2024.

©2024 Visa. All rights reserved. Visa Confidential

REGULATION & POLICY: HOW GOVERNMENTS CAN EMPOWER SMBS' FINANCIAL SECURITY

1

ENHANCING CYBERSECURITY AWARENESS

Governments can boost SMBs' cybersecurity awareness by funding educational programmes and workshops. These initiatives, often in collaboration with cybersecurity firms, cover essential topics such as phishing prevention, secure online transactions, and data protection. For example, the *'Cyber Wardens Programme'* is a short course funded by the Australian government to protect small businesses from daily online threats.

2

STRENGTHENING FINANCIAL SECURITY PARTNERSHIPS

Encouraging partnerships between SMBs and financial ecosystem players, such as banks and cybersecurity firms, can provide SMBs access to essential resources and expertise. These collaborations can lead to tailored security solutions and shared threat intelligence, enhancing overall financial security. For instance, Singtel has launched its Cyber Elevate Programme, aimed at improving the cybersecurity resilience of SMBs. Through the programme, SMBs can learn how to prepare for, detect, respond to, and recover from cyber-attacks.

VISA

©2024 Visa. All rights reserved. Visa Confidential

3 FACILITATING COMPLIANCE AND REGULATORY SUPPORT

Governments can simplify regulatory compliance for SMBs by providing clear guidelines, resources, and dedicated support channels. For instance, the Cyber Security Agency of Singapore's *'SG Cyber Safe Programme'* provides a comprehensive suite of resources, including guidelines, toolkits, and self-assessment tools, as well as a cybersecurity certification scheme to recognise organisations with good cybersecurity practices.

4 PROMOTING ACCESS TO ADVANCED SECURITY TECHNOLOGIES

Governments can promote the adoption of advanced security technologies by offering subsidies, grants, or tax incentives. Supporting the development of affordable, scalable security solutions tailored to SMBs can help them enhance their defences against sophisticated cyber threats. For example, the Malaysian government offers a 50% matching grant of up to RM5,000 (~ US$1,000) for micro, small, and medium enterprises in the country to adopt digital technologies. This grant covers various digitalisation areas, including cybersecurity.

©2024 Visa. All rights reserved. Visa Confidential

03

CONCLUSION

As the variety of payment methods continues to expand, SMBs in the Asia Pacific region are increasingly exposed to a broad spectrum of fraud and security challenges. This evolution in payment landscapes, driven by customer demand for convenience and speed, has inadvertently created new vulnerabilities. Bad actors exploit these vulnerabilities by leveraging advanced tools and techniques to commit fraud, ranging from sophisticated phishing schemes to exploiting weaknesses in digital payment infrastructure. The sheer diversity of payment methods – from traditional credit card transactions to instant payments and cryptocurrencies – complicates the security landscape, making it harder for SMBs to keep pace with the necessary security measures.

Consequently, SMBs must adopt a more considered and strategic approach to integrating digital payments. While the democratisation of technology empowers businesses, it also lowers the barriers to entry for cybercriminals, necessitating continuous evolution in security strategies. At the forefront of this approach is the adoption of data-driven security measures. Advanced technologies such as AI and ML provide SMBs with powerful fraud prevention tools, which are crucial as the widespread adoption of diverse payment methods, such as digital wallets and BNPL solutions, increases the attack surface for cybercriminals.

©2024 Visa. All rights reserved. Visa Confidential

In an era marked by unprecedented technological disruption, SMBs must adapt and innovate more critically than ever. The rapid digitalisation sweeping across the globe has fundamentally altered the competitive landscape, introducing both remarkable opportunities and significant challenges. To stay relevant, SMBs must meet the evolving expectations of digital-savvy consumers and customers who demand personalised, convenient, and secure experiences.

To enhance fraud prevention capabilities, SMBs must invest in advanced technologies and ensure that their workforce is equipped to leverage these tools effectively. Employee education and upskilling are critical components of a comprehensive security strategy. Beyond implementing advanced tools, SMBs must proactively invest in training their workforce to stay ahead of the ever-evolving fraud landscape. As the technological arms race continues, businesses that can swiftly respond to new trends and threats will thrive.

However, technological solutions alone are not enough. As geopolitical and socioeconomic shifts drive a move from globalism to regionalism, businesses must adapt by fostering collaborative partnerships that respect and integrate local priorities. Commitment to a collaborative approach helps businesses enhance their security measures and align with national and regional agendas, thereby maintaining their competitive edge.

©2024 Visa. All rights reserved. Visa Confidential



In the Asia Pacific region, where digitalisation is rapidly transforming economies, enhancing financial security and fraud prevention is not just an operational necessity but a strategic imperative for SMBs. By adopting a data-driven approach, forging strategic partnerships, and prioritising continuous learning and adaptation, SMBs can secure their future in an increasingly digital world.

The path forward is challenging, but with the right approach, SMBs can turn these challenges into opportunities for growth and resilience. By prioritising trust and security, they can build a robust foundation that not only protects against current threats but also ensures long-term business success in the digital economy.

©2024 Visa. All rights reserved. Visa Confidential

THANK YOU

FOR FURTHER INFORMATION PLEASE CONTACT YOUR VISA REPRESENTATIVE



VISA