Response to Treasury on the Scams - Mandatory Industry Codes: Consultation Paper

Table of Contents

Group Country Manager Letter

29 January 2023

Scams Taskforce

Market Conduct and Digital Division

The Treasury

Langton Crescent

PARKES ACT 2600

Via email: scamspolicy@treasury.gov.au

Dear Scams Taskforce representative,

Visa submission to Treasury on the Scams - Mandatory Industry Codes Consultation Paper

Visa welcomes the opportunity to share our perspectives on the Scams – Mandatory Industry Codes Consultation Paper (consultation paper) and supports Treasury's commitment to ensuring that key sectors in the scams ecosystems have measures in place to prevent, detect, disrupt and respond to scams.[1]

Visa is committed to promoting trust and security in the payments ecosystem. This trust is built on our dedication to connecting and protecting the ecosystem and its users through a multi-layered approach. We collaborate with our partners and industry stakeholders to keep payments secure and prevent fraud. We deploy multi-layered security measures that have kept fraud rates low[2], despite significant growth in digital payments. These include real-time fraud monitoring, and active anti-phishing initiatives. This security approach is complemented by a comprehensive set of rules and policies focused on safeguarding transactions and protecting consumers. We also offer resources to help businesses and consumers protect themselves from fraud[3].

A key aspect of Visa's consumer protection strategy is our long-standing Zero Liability policy.[4] This policy ensures that consumers are not held responsible for unauthorised purchases, thereby giving them a peace of mind and strengthening their trust in our payment network. Even though scams often involve authorised fraud, Visa's Zero Liability policy demonstrates our commitment to consumer protection and our deep insights into the measures necessary to ensure it.

In responding to the consultation paper, Visa's submission focuses on several topics, including the importance of a collaborative industry approach and continuous education and awareness to ensure an efficient implementation of the scams framework. We also highlight the necessity of a clear and concise Framework, which reduces ambiguity and ensures that all aspects are well understood and executable. In addition, we provide our perspectives on a number of specific

[1] Treasury (2023), Scams - Mandatory Industry Codes - Consultation paper (treasury.gov.au), p6.
[2] https://www.visa.com.au/content/dam/VCOM/regional/ap/australia/global-elements/Documents/visa-security-roadmap-2021-2023.pdf
[3] https://www.visa.com.au/pay-with-visa/security/future-of-security-roadmap.html
[4] https://usa.visa.com/pay-with-visa/visa-chip-technology-consumers/zero-liability-policy.html

questions in the consultation paper, such as additional overarching obligations, including reporting obligations and data sharing.

It is important to note that Visa does not have a direct relationship with cardholders. Our role in the ecosystem is, among other things, to equip issuers and acquirers with the necessary tools to help protect their cardholders and merchants, respectively. Although we are not directly in scope of the proposed Framework, our objective is to contribute to the larger discussion that seeks to raise awareness and contribute to the collective effort to combat scams.

Visa is available to provide further details on our submission if helpful.

Yours sincerely,

Julian Potter

Group Country Manager, Australia, New Zealand, and South Pacific

Overview

Visa acknowledges the growing concern that scams are affecting Australian consumers and businesses. We appreciate the Government's ongoing efforts and commitment to creating a secure and scam-free environment in Australia.

Visa supports the proposed Scams Code Framework's (the Framework) principles-based approach, which allows for flexibility and adaptability in response to the evolving threat landscape. This approach aligns with Visa's own strategies to evolve capabilities with the shifting landscape through securing new channels and flows, tailored risk management and consumer education.

Visa also supports the Framework's comprehensive approach addressing the 'scams ecosystem'. This approach aligns with Visa's own efforts to work with all stakeholders across payments landscape and the wider economy to ensure that consumers and businesses can successfully minimise the impact of scams.

Reducing the prevalence of scams and fraud

Worldwide, Visa has invested approximately USD 10 billion[5] in technology and innovation over the last five years to stop fraudsters and protect merchants and consumers from taking on fraud losses. Visa helps secure the payments ecosystem by:

1) Protecting the ecosystem against potential threats via secure technologies, risk management, and ecosystem rules;

2) Defending against ongoing attacks through real-time countermeasures, actionable intelligence, and compliance programs;

3) Evolving capabilities as the landscape shifts by securing new channels and flows, and supporting consumer education; and

4) Tailoring risk management to our clients' specific needs through 24/7/365 monitoring, advanced fraud alerting, real-time threat containment, and comprehensive threat detection.

While Visa is a non-consumer and non-merchant-facing entity, we are deeply committed to supporting our financial institution clients, which are the entities that provide services directly to consumers and merchants, and are involved in protecting consumers and merchants from scams. We – for our part – offer multiple services that, in turn, assist financial institutions in these efforts, including in the card space and more recently for account-to-account payments via our new AI-based risk scoring service, RTP Fraud Prevent.

RTP Fraud Prevent can score transactions on Real Time Payment (RTP) rails and assist participating financial institutions to determine the likelihood of fraud. It provides a real time risk score, and a supporting set of attributes, that participating financial institutions can use to determine the likelihood of a scam before funds are sent, thereby protecting consumers and helping maintain the integrity of the payment system. The service is being piloted in the UK with Pay.UK[6], among other countries and territories around the world.

We believe that such proactive, real-time measures should be considered in the implementation of anti-scam strategies and tools.

Visa believes that a collective industry approach to education and awareness is key to helping prevent consumers and businesses from becoming victims of scams. Visa works closely with our clients on delivering best practices in consumer

[5] https://usa.visa.com/visa-everywhere/blog/bdp/2023/10/18/bringing-innovation-and-1697633266330.html
[6] https://newseventsinsights.wearepay.uk/media-centre/press-releases/payuk-partners-with-visa-synectics-solutions-and-featurespace-on-pioneering-fraud-detection-and-prevention-initiative/

education and ecosystem awareness to combat fraud and scams. Visa also works with law enforcement agencies and across industry groups globally to share insights and recent data on what to look out for as well as common scam sources.

Response to specific questions

Questions on the proposed Framework:

5. Is the Framework sufficiently capable of capturing other sectors where scams may take place or move to in the future?

Scams can be fast-moving targets to address, as criminals are continually seeking out the weakest points in the ecosystem to attempt to infiltrate. As technology evolves, their goal is to exploit new channels and sectors. Because of the pace of change, it is challenging to future-proof a framework to fully address scams. However, open dialogue and collaboration is the best foundation to ensure any framework remains fit for purpose, effective and responsive.

Visa recognises that collaboration across all sectors is crucial in combating scams, both in traditional and emerging sectors. Visa, as a key player in the payments ecosystem, is committed to such collaboration.

Visa's investment in technology and innovation. Our various AI-based risk solutions are examples of how technology can be effectively used in this fight against fraud and scams across the payments ecosystem. These solutions have proven highly effective in detecting and preventing fraud, and they serve as a model for how technology can be leveraged to combat fraud and scams in the ecosystem. For example, Visa's AI and predictive machine learning capabilities helped prevent an estimated $27 billion in fraud-related losses in 2022 alone[7]. Our experience in reducing card transaction fraud globally is a testament to the effectiveness of this approach. By sharing knowledge and best practices, working with law enforcement agencies and industry groups, and leveraging technology, we have been able to significantly reduce fraud in card transactions worldwide.

As scams and their modus operandi evolve, all participants in the scams ecosystem should be responsible for regularly reviewing and updating their own internal anti-scam or fraud management frameworks.

7. What impacts should the Government consider in deciding a final structure of the Framework?

As the Government contemplates the final structure of the Framework, it is vital to consider the impacts on the players within the ecosystem and the consumers they serve. It should also include addressing current scam methods while being adaptable to emerging scam tactics that may arise due to technological advancements or changes in fraud strategies.

While Visa is dedicated to playing a leadership role within the payments ecosystem and contributing to the collective effort to combat scams, it is crucial to highlight that because Visa does not have a direct relationship with cardholders, we have a limited line of sight into cardholder-facing activity, like scams. Instead, our role is to equip issuers and acquirers with the necessary tools to protect their cardholders and merchants. We believe that an industry approach, involving education, awareness, and the use of advanced fraud detection and prevention tools, is key to helping issuers and acquirers prevent consumers and businesses, respectively, from becoming victims of scams.

[7] https://usa.visa.com/visa-everywhere/blog/bdp/2023/09/13/30-years-of-1694624229357.html

Questions on definitions:

8. Is maintaining alignment between the definition of 'scam' and 'fraud' appropriate, and are there any unintended consequences of this approach that the Government should consider?

Visa notes Treasury's proposed definition of a scam[8] under the Framework. Maintaining alignment between the definitions of 'scam' and 'fraud' can be beneficial in creating a clear and consistent understanding of these terms across different sectors. However, it is important to recognise that while all scams can be considered fraud, not all frauds are necessarily scams. Scams often involve deceptive practices where the consumer is misled into making a transaction, while fraud can occur without the consumer's knowledge or involvement.

Visa supports the distinction between authorised and unauthorised fraud included in the Framework. In cases of authorised fraud, consumers knowingly authorise payments to the scammer, often under false pretenses. On the other hand, unauthorised fraud occurs when transactions are made without the consumer's knowledge or consent.

For unauthorised card fraud, there are well-established and effective scheme rules and a liability framework in place. Visa has a long-standing history of combatting unauthorised card fraud. We have developed and implemented advanced security measures, and we work closely with financial institutions to ensure the integrity of payments ecosystem. Our Zero Liability policy, along with our other security measures, demonstrates our unwavering commitment to protecting consumers and maintaining trust in the payments ecosystem.

However, authorised fraud (scams) represent a newer and different challenge. Unlike traditional fraud, scams often involve deception and manipulation, leading consumers to authorise payments under false pretenses. Therefore, the Framework's focus should be on addressing authorised fraud, particularly in the context of account-to-account scams, where consumers are often deceived into authorising payments.

While maintaining alignment between the definitions of 'scam' and 'fraud' will be beneficial for clarity and consistency, the Framework should also consider the complex and evolving nature of scams. This includes recognising the various tactics used by fraudsters, differentiating between authorised and unauthorised fraud, and addressing the varying degrees of consumer involvement in scams.

Visa notes that there is currently no agreed formal definition of a scam in Australian legislation[9]. A consistent taxonomy would help ensure that all entities are using the same terminology and definitions when identifying and reporting scams. The absence of a consistent definition of scams and fraud could result in unintended consequence such as: inconsistent and incomparable, ineffective information sharing, as well as confusion and misinterpretation from different entities when reporting scams or fraud.

11. What impacts should be considered in legislating a definition of a scam for the purposes of this Framework?

[8] Scams – Mandatory Industry Codes Consultation paper (treasury.gov.au) pg. 9
[9] Scams – Mandatory Industry Codes Consultation paper (treasury.gov.au) pg. 9

In our view, the definition should be clear and precise to avoid ambiguity. The definition should also be inclusive and flexible, covering all types of scams, including both digital and non-digital scams, and appropriately making the distinction between authorised (which is a scam) and unauthorised fraud (which is not necessarily a scam). It should also be adaptable to accommodate new types of scams that might emerge in the future due to technological advancements or changes in scammer tactics.

Moreover, it is important to consider the implications for various stakeholders, including consumers, financial institutions, and law enforcement agencies. Consistency with existing laws and scheme frameworks is another key consideration.

Finally, the definition will play a crucial role in consumer education efforts. A clear and understandable definition can help consumers better understand what constitutes a scam, enabling them to protect themselves more effectively.

Questions on overarching principles-based obligations:

15. Are there additional overarching obligations the Government should consider for the Framework?

Visa supports Treasury's view of taking a consistently proactive approach to combatting scams[10]. One consideration for the Government is the emphasis on consumers' individual responsibility to be vigilant against scams. A discerning and vigilant public remains the first line of defence against scams. Individuals have a direct responsibility to mitigate the occurrence of scams by exercising proper cyber hygiene and discernment over disclosure of personal credentials. For instance, the Monetary Authority of Singapore's (MAS) Proposed Shared Responsibility Framework places a strong emphasis on the role of individuals in combating scams. It underscores the importance of consumers being vigilant, especially in the context of phishing scams, and practicing proper cyber hygiene.[11]

To aid in this regard, banks and other consumer-facing ecosystem participants should ensure they empower consumers to be vigilant and act as the first line of defence. This could be through educational campaigns, clear and readily available information on how to protect themselves, as well as capabilities delivered through channels such as mobile banking apps which notify customers of suspicious activity or allow consumers to restrict or block certain activity, which may alleviate some of their concerns.

16. Are the obligations set at the right level and are there areas that would benefit from greater specificity e.g., required timeframes for taking a specific action or length of time for scam-related record-keeping?

Visa believes that the obligations set out in the Framework are generally at the right level, striking a balance between providing clear expectations for designated institutions and allowing for flexibility in how those obligations are met. This approach recognises that institutions may have different capabilities and resources, and that a one-size-fits-all approach may not be effective.

It is important to ensure that any additional specificity does not unduly burden institutions or stifle innovation in scam prevention and detection. Therefore, Visa recommends that any changes be subject to public consultation.

[10] Scams – Mandatory Industry Codes Consultation paper (treasury.gov.au) pg. 11

[11] Monetary Authority of Singapore, Consultation Paper on Proposed Shared Responsibility Framework, paragraph 2.6 p. https://www.mas.gov.sg/-/media/mas-media-library/publications/consultations/pd/2023/srf/consultation-paper-on-proposed-shared-responsibility-framework.pdf

18. Are there opportunities to minimise the burden of any reporting obligations on businesses, such as by ensuring the same information can be shared once with multiple entities?

One potential way to minimise the burden of reporting obligations could be the usage of a centralised reporting system or hub. This would allow businesses to submit required information once, which could then be shared with multiple entities as needed.

Another option could be to align any reporting obligations with existing processes and systems as much as possible, including based on the definitions of scams (or authorised fraud compared to unauthorised fraud). For example, if businesses are already collecting certain information for their own internal purposes or for other regulatory requirements, it would be beneficial to employ this existing data collection rather than requiring separate reporting.

However, it is important to consider the potential privacy and security implications of sharing information more widely. Any system for sharing information must have robust safeguards in place to protect sensitive data and comply with privacy laws.

Questions on information sharing requirements:

28. What other information sharing arrangements exist that the Government should consider/leverage for the implementation of the Framework?

In Visa's view, information sharing can significantly enhance the ability of entities to detect and prevent scams. Data sharing exchanges like the Australian Financial Crimes Exchange (AFCX) provide a platform for entities to share information about potential scams in a secure and efficient manner. This collective intelligence can help to identify new scam tactics more quickly, and enable all participants to take preventive measures.

In addition to formal data sharing exchanges, industry forums play a crucial role in information sharing. These forums provide an opportunity for entities across the industry to share insights, discuss emerging trends, and collaborate on solutions. Furthermore, they foster a sense of community and collective responsibility in combating scams.

Visa notes Treasury's requirement to share and act on information to ensure that all businesses within the scams ecosystem have quality information to enable them to detect and prevent scams[12]. As also stated in Visa's response to Question 18 above, it is important to consider the potential privacy and security implications of sharing information. Robust safeguards must be in place to prevent unauthorised access or misuse of shared information.

[12] Scams – Mandatory Industry Codes Consultation paper (treasury.gov.au) pg. 14

About Visa

Visa's mission is to connect the world through the most secure, reliable, and innovative payment network – enabling individuals, businesses, and economies to thrive. Our advanced global processing network, VisaNet, provides secure and reliable payments around the world, and is capable of handling more than 65,000 transaction messages a second.

In Australia, Visa has offices in Sydney and Melbourne. Together with our Australian financial institutions, fintech and business clients, and our technology partners, we are committed to building a future of commerce that fosters Australian economic growth, security and innovation. Visa continues to expand acceptance across the payments ecosystem, ensuring that every Australian can not only pay, but also be paid in a convenient and secure way. Visa invested US$10 billion (A$14.95 billion) in technology over the past five years, including to reduce fraud and improve security. In 2021, Visa's AI-driven security helped financial institutions prevent more than AU$354 million in fraud from impacting Australian businesses[13].

As commerce moves rapidly online, Visa recently released its updated Australian Security Roadmap 2021-23[14] in response to the increasing risk of cyber crime and scams facing Australian businesses and consumers. The roadmap highlights the steps that Visa, together with industry, are taking to continue to secure digital payments in Australia, including:

- Preventing enumeration attacks through new ecommerce requirements
- Driving adoption of secure technologies
- Securing digital first payment experiences, including contactless ATM access
- Enhancing the cyber security posture of payments ecosystem participants
- Preventing Australian consumers and businesses from becoming victims of scams
- Ensuring payments ecosystem resilience through real-time AI solutions.

[13] Visa (2021) https://www.visa.com.au/about-visa/newsroom/press-releases/visas-ai-prevents-more-than-350-million-in-fraud-from-disrupting-australian-businesses.html
[14] Visa (2021) https://www.visa.com.au/pay-with-visa/security/future-of-security-roadmap.html