Committee on Payments and Market Infrastructures and Board of International Organization of Securities Commissions

Guidance on Cyber Resilience for Financial Market Infrastructures

Visa Europe response 23 February 2016

Visa Europe ('Visa') welcomes the opportunity to comment on the Committee on Payments and Market Infrastructures and Board of International Organization of Securities Commissions Guidance on Cyber Resilience for Financial Market Infrastructures (the 'Guidance') given the relevance of cyber resilience to the financial services and technology sector.

Visa is a technology company with a mission to create innovative and secure electronic payment solutions with heightened customer experience. Visa's secure systems and procedures allow us to maintain trust, build deep partnerships, enable access and accelerate growth in order that customers obtain an efficient and secure payments experience.

As of March 2015 Visa has been designated as a payment system under the oversight of the Bank of England. As part of the process Visa has conducted a self-assessment under the CPMI-IOSCO principles for financial market infrastructures and is currently assessed by the Bank of England under these principles.

Executive Summary

Visa's strategy recognises that risk management is a key element of the organisation's culture to ensure the security of the payment system. It is a key priority that the Visa systems are secure, stable and resilient in all eventualities; cyber resilience is a core business enabler, directly supporting all elements of the business.

In order to achieve effective cyber resilience, Visa Europe supports the notion that it is necessary to undertake coordinated efforts throughout the entire organisation that go beyond the security of the informational technology systems.

Visa recognises the importance of a thoroughly comprehensive cyber resilience framework and raising organisational awareness of cyber resilience in order to ensure the stability and resilience of the systems.

Whereas Visa recognises that this Guidance furthers certain PFMI principals, it supports that there are no prescribed solutions in achieving enhanced cyber resilience and would encourage that this aspect of the Guidance remains.

Introduction to Guidance

Visa appreciates the importance of a solid cyber resilience strategy as a foundation for the security of information and systems. The Visa Corporate Key Controls in place guard against security threats to Visa information and information systems, and Visa appreciates the importance of these key controls.

Visa supports the concept that cyber resilience is a collective endeavour of the financial services ecosystem and relevant to all stakeholders.

Visa would encourage that the underlying principles of this Guidance extend across the financial services network in order to ensure stable and resilient systems, and supports that relevant authorities may decide to apply this Guidance to types of infrastructure not specifically covered by the Guidance.

Visa encourages a harmonized approach to the eventual implementation of this Guidance by the relevant regulatory, supervisory and oversight authorities in order to ensure consistent standards across the Europe.

Visa structures our response across the five primary risk management categories – 'governance', 'identification', 'protection', 'detection', and 'response and recovery' – plus the three overarching components of 'testing', 'situational awareness', and 'learning and evolving'.

1. Primary risk management categories

1.1 Governance

Visa places risk management at the heart of an operational and governance structure, which includes a cyber-resilience strategy operating off a strong and dedicated framework. Visa supports that cyber resilience reaches beyond a robust information technology systems and includes a holistic vision of raising cyber resilience awareness throughout the organisation, addressing communications, people and processes. Visa considers it important to realise that cyber resilience frameworks are proportionate to the risks anticipated by the organisation.

Visa sees the benefit in clearly defining the remit of the responsibilities in organisations for those who are involved in the key processes in a cyber-resilience framework, however, believes that accountability for cyber resilience is a shared organisational issue, requiring each area of the business to be accountable and responsible for various aspects of cyber resilience. For instance, compliance with cyber resilience may be enforceable by the area of the organisation principally managing risk, whereas the legalities of cyber resilience policies may be checked by the legal department. In this instance Visa strongly suggests that section 2.2.7 of the Guidance be revisited.

- *Visa would suggest that that Guidance note on accountability 2.2.7 be amended to reflect that cyber resilience is a shared organisation responsibility*[1]

1.2 Identification

Visa agrees with the importance of an FMI identifying its information assets and understanding its processes, procedures, systems and other dependencies to strengthen its overall cyber resilience posture. Visa supports work in this regard to regularly review and update to ensure that they remain current, accurate and complete.

[1] Please refer to Annex 1 item 1 for a draft version of this text

- *Visa encourages the harmonised use of the PCI DSS assessment which contributes and directly supports this section of the Guidance*

Visa appreciates that coordination between the entities in the financial ecosystem is key to ensure cyber resilience. Visa Europe works collaboratively with other payment schemes, its members, regulators and industry bodies to promote new and globally interoperable innovations that enhance the security of the payment eco-system, as well as upholding and encouraging compliance with appropriate industry standards (such as PCI DSS, EMVCo or 3D Secure).

1.3 Protection

- *Visa would recommend that section 4.4 of this area of the Guidance in relation to 'Insider threats' is implemented as practically as possible and consistent within the remit of the appropriate European guidelines relating to the rights of privacy for employees and that this only applies to individuals that have direct access to systems that control the financial stability/network.*

Visa ensures that all staff accessing key information and assets in the performance of their jobs are required to complete rigorous training. It should be noted that the requirement of PCI DSS v3.1 is that awareness training is conducted annually for all staff, Visa Europe has been fully compliant for 5 years with the PCI DSS requirements.

Visa supports this section of the Guidance and has no further comments.

1.4 Detection

Visa encourages uses a multi-layered approached to detection and encourages that all parties involved are managed to industry standard accreditations, with ongoing requirements for training.

Visa supports this section of the Guidance and has no further comments.

1.5 Response and Recovery

Visa supports the principles behinds this section of the Guidance and appreciates that the ability to resume operations quickly and safely after a successful cyber-attack is paramount in order to guarantee the stability of the European financial systems.

Visa agrees FMIs should plan in advance for communication requirements in crisis scenarios. As part of Visa's established incident response process we have specialist resources and processes in place to evaluate whether communication is required for relevant audiences (e.g. Visa's clients, customers, authorities, regulators, etc), what messages are required, and what communication channels are most appropriate (e.g. Visa's website, the 'traditional media', social media, etc). Visa has a dedicated Corporate Communications department to evaluate communication requirements, working within clearly defined escalation and decision making procedures. It is important to remain responsive and flexible to each crisis scenario so Visa can choose the most appropriate communication audiences, messages and channcels.

Visa has no further comments.

2. Overarching components

2.1 Testing

Visa Europe supports this section of the Guidance and has no further comments.

2.2 Situational awareness

Visa suggests that this section of the Guidance is expanded to also include government and local authorities to help ensure timely communication of intelligence from those organisations into financial market groups given the critical need for the appropriate and timely sharing of information in a standardised format. Shared threat intelligence is often released too late after the event, and, when it is released, normally in a format which has been redacted to such a level that it is difficult to use.

- *Visa Europe encourages the expansion of this section of the Guidance to include government and local authorities, and detail the standardisation of intelligence reporting.*[2]

2.3 Learning and evolving

Visa continues to support and encourage an industry wide and collaborative approach towards the learning and evolving of cyber resilience strategies in order to seek to ensure the resilience and stability of financial systems.

- *Visa would encourage an industry wide effort to share information on incidents in order to further boast the security and resilience of systems.*

3. Other

3.1 Legal framework

Visa is a payment system and benefits from the fact that the provision of payment and ancillary services is subject to a harmonised legal framework at EU and EEA levels.

3.2 PCI DSS Certification

In addition to this Guidance, Visa encourages the industry wide use of the Payment Card Industry Data Security Standard (PCI DSS) Certification. The Payment Cards Industry Security Standards Council (PCI SSC) is responsible for the development, management, education, and awareness of the PCI Security Standards.

Visa's commitment to industry standards supports the development of common processes to ensure secure and resilient financial systems. Visa is one of the Council's five founding global payments brands and has successfully retained its PCI DSS certification since this standard was introduced four years ago.

The PCI DSS is a robust and comprehensive standard and has supporting materials which aim to enhance payment card data security. Attention should be given to the alignment between PCI DSS

[2]Please refer to Annex 1 note 2 for a draft version of this text

and the Guidelines, because an organisation which is PCI DSS compliant will already satisfy many of the aspects of this Guidance. Any duplication between the two should be avoided to best optimise the global standard that is already independently assessed.

Visa Europe, 23 February 2016

Annex 1

Proposed additional draft text for Guidance

1. *Clear roles and responsibilities*: An FMI's cyber resilience framework should clearly define the roles and responsibilities within the organisation for managing cyber risk. In particular, an FMI should clearly define the roles and responsibilities of the individuals responsible for decisions concerning cyber resilience, including in emergencies and in a crisis.

2. *Roles of governmental authorities*: Government and local authorities should seek to help ensure that intelligence from those organisations into financial market groups is shared with and communicated to FMIs in a timely manner and in an agreed standardised format.