FACT SHEET

Technology Innovation Programme

The Visa Europe Technology Innovation Programme (TIP) was designed to complement the Payment Card Industry (PCI) Data Security Standard (DSS) by reflecting the risk of account data compromise in the EMV-based European environment. It is three years since TIP was announced and many retailers have taken advantage of the simplified compliance offered by TIP to focus their security and compliance efforts.

The PCI SSC has recently released version 3.0 of PCI DSS and Visa Europe has revised TIP for EMV-mature markets

Qualifying for TIP
TIP is designed for face-to-face retailers that use PCI approved Points of Interaction (POIs), also known as PIN Entry Devices (PEDs). It is not designed for e-commerce or mail-order/telephone-order merchants. Multi-channel merchants that can adequately separate their face-to-face (F2F) environment from their other environments can choose to validate the compliance of their face-to-face channel using TIP, and their non-face-to-face channels using the normal PCI DSS prioritised approach.

To qualify for TIP:

1. The acquirer must agree that the merchant can join TIP. At a minimum the merchant must be able to demonstrate a plan to segment their F2F and non-F2F channels, and provide individual compliance plans for each channel.
2. Annually, at least 95% of the merchant's total face-to-face POS transaction count must originate from chip-enabled devices. To qualify, a chip-enabled device must:
    - be a Visa approved device;
    - have a valid and current EMV type approval;
    - have passed Visa's Acquirer Device Validation Toolkit (ADVT) and, where contactless technology is used, VpTT testing requirements; and
    - have no reported and/or outstanding interoperability issues.
3. The merchant must not have been involved in an account data compromise within the last 12 months. This criterion may be waived at Visa Europe's discretion if the merchant has subsequently validated PCI DSS compliance after the compromise event.

TIP is risk-based

TIP is designed to reflect the risk of attack and exploitation of EMV transaction data. Visa Europe believes that that there is a lower risk of compromise of EMV transaction data than full track data or card number plus CVV2, and so has reduced the compliance validation requirements for merchants that just store, process or transmit EMV transaction data. Additionally Visa Europe recognises that some PCI DSS requirements are not cost-effective or unsuited to large retailers with multiple outlets, imposing large compliance and security costs for a relatively small reduction in risk

The initial version of TIP required merchants to achieve all milestones 1 and 2 of the PCI DSS prioritised approach to be considered compliant with Visa Europe's requirement for all merchants to conform to PCI DSS. In this revised version of TIP, Visa Europe has taken the requirements from milestones 1 and 2 and identified some as *mandatory*, and others as *recommended*. PCI DSS has always included the requirement (12.2) for organisations to conduct an annual risk assessment. Merchants can now use this risk assessment to justify to their acquirer which of the *recommended* requirements within TIP are not appropriate for their particular environment. Together the merchant and acquirer can agree which of the *recommended* requirements are needed in the merchant's environment.

TIP Environments

In revising TIP for 2014 Visa Europe has created two options, reflecting the European market.

1. Traditional POI-based environments

Traditional POI based requirements have no encryption within the POI and send unencrypted EMV transaction data over the merchant's network to the acquirer or payment facilitator.

Visa Europe has determined the requirements from PCI DSS that are *mandatory* or *recommended* for this environment.

2. Environments with non-validated encryption solutions

Many merchants have deployed POIs that encrypt the data from the POI through to the acquirer or payment facilitator, meaning that only encrypted EMV transaction data is present on the merchant's network. Where merchants have installed solutions that have been validated against the PCI Point to Point Encryption (P2PE) standard they should use the Self-Assessment Questionnaire SAQ-P2PE to validate their compliance to their acquirer, irrespective of their merchant level.

Visa Europe recognises that although solutions that have not been validated to the P2PE standard don't offer the same degree of assurance as validated solutions, they may improve the merchant's security. However Visa Europe is also aware that some POI encryption solutions have been poorly implemented, giving the merchant a false sense of security. Where merchants have deployed

non-validated solution, the solution provider, along with the solution provider's P2PE Qualified Security Assessor (QSA), must provide a solution risk assessment to Visa Europe, along with an assessment of the controls that would still be mandatory in the merchant environment. Visa Europe will then produce a TIP profile for the solution, detailing the *mandatory* and *recommended* requirements for a merchant environment using the non-validated solution.

An individual merchant should then conduct their own risk-assessment of the solution and agree with their acquirer which of the *recommended* controls are appropriate for the merchant's environment.

TIP Validation
Merchants should validate their compliance to the TIP requirements to their acquirer via a partially completed SAQ D or a partial report on compliance dependent on the acquirer's requirements.

TIP Requirements
The following table details the proposed *Mandatory* (**M**) and *Recommended* (**R**) requirements for the EMV-mature market TIP.

No	Requirement	Mile-stone	TIP
12.2	Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal risk assessment. […]	**1**	**M**
1.1.2	Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	**1**	**M**
1.1.3	Current diagram that shows all cardholder data flows across systems and networks.	**1**	**M**
1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**2**	**M**
1.1.6	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	**2**	**R**
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.		
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	**2**	**M**

No	Requirement	Mile-stone	TIP
1.2.2	Secure and synchronize router configuration files.	**2**	**R**
1.2.3	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	**2**	**M**
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.[1]		
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	**2**	**M**
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	**2**	**R**
1.3.3	Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	**2**	**M**
1.3.4	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. […]	**2**	**R**
1.3.5	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	**2**	**R**
1.3.6	Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.)	**2**	**M**
1.3.7	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	**2**	**R**
1.3.8	Do not disclose private IP addresses and routing information to unauthorized parties.	**2**	**R**
1.4	Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network.	**2**	**R**
1.5	Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	**2**	**R**
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	**2**	**M**

[1] It is envisaged that these requirements will be able to be implemented using the telco-supplied router/firewall that connects an individual outlet to the Internet.

No	Requirement	Mile-stone	TIP
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings	**2**	**M**
2.3	Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	**2**	**R**
2.4	Maintain an inventory of system components that are in scope for PCI DSS	**2**	**R**
2.5	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**2**	**R**
3.1	Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: […]	**1**	**M**
3.2	Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	**1**	**M**
3.2.1	Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.	**1**	**M**
3.2.2	Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.	**1**	**M**
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.	**1**	**M**
4.1	Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.	**2**	**M**
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.	**2**	**M**

No	Requirement	Mile-stone	TIP
4.2	Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	**2**	**M**
4.3	Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	**2**	**R**
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**2**	**R**
5.1.1	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	**2**	**R**
5.1.2	For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software	**2**	**R**
5.2	Ensure that all anti-virus mechanisms are maintained as follows: - Are kept current, - Perform periodic scans - Generate audit logs which are retained per PCI DSS Requirement 10.7	**2**	**R**
5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	**2**	**R**
5.4	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	**2**	**R**
8.3	Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).	**2**	**M**
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	**2**	**R**

No	Requirement	Mile-stone	TIP
9.1.1	Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: “Sensitive areas” refers to any data centre, server room or any area that houses systems that store, process, or transmit cardholder data. **This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store**.	**2**	**R**
9.1.2	Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.	**2**	**R**
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	**2**	**R**
9.3	Control physical access for onsite personnel to the sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled	**2**	**R**
9.8.1	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	**1**	**M**
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	**1**	**M**
9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.		
9.9.1	Maintain an up-to-date list of point of sale (POS) devices. The list should include the following: […]	**2**	**M**

No	Requirement	Mile-stone	TIP
9.9.2	Periodically inspect POS device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).	**2**	**M**
9.9.3	Provide training for personnel to be aware of attempted tampering or replacement of POS devices.	**2**	**M**
11.1.2	Implement incident response procedures in the event unauthorized wireless access points are detected..	**2**	**M**
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades)[2].		
11.2.1	Perform quarterly internal vulnerability scans and rescans as needed, until all “high-risk” vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.	**2**	**M**
11.2.2	Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.	**2**	**M**
11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	**2**	**R**
11.3	Implement a methodology for penetration testing […]	**2**	**M**
11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification […]	**2**	**M**
11.3.2	Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification[…]	**2**	**M**
11.3.3	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	**2**	**M**
11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.	**2**	**M**

[2] In multi-outlet environments scan and test all points of consolidation, vulnerability scan and test a sample individual outlets based on the risk assessment.

No	Requirement	Mile-stone	TIP
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	**2**	**M**[3] **R**[4]
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	**2**	**M**
12.8	Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	**2**	**M**
12.8.1	Maintain a list of service providers.	**2**	**M**
12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. […]	**2**	**M**
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	**2**	**M**
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	**2**	**M**
12.8.5	Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	**2**	**M**
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.		
12.10.1	Create the incident response plan to be implemented in the event of system breach. […]	**2**	**M**
12.10.2	Test the plan at least annually.	**2**	**M**

[3] *Mandatory* for areas of consolidation
[4] *Recommend* for individual outlets

No	Requirement	Mile-stone	TIP
12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.	**2**	**R**
12.10.4	Provide appropriate training to staff with security breach response responsibilities.	**2**	**R**
12.10.5	Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	**2**	**R**
12.10.6	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**2**	**R**