Moneris Solutions PCI DSS Responsibility Matrix.

Version 4.0.1

Revised: July 9, 2025

Table of contents.

Table of Figures.

Document overview.

Purpose

The purpose of this document is to provide clear guidance to merchants on how to accurately report their Payment Card Industry Data Security Standards ("PCI DSS") compliance. It helps merchants connect the dots between their specific solutions and the appropriate reporting forms, ensuring they understand which requirements apply to them. By offering straightforward instructions and practical insights, this document empowers merchants to navigate the reporting process with confidence and precision

Scope

This document covers the reporting requirements and processes for PCI DSS compliance specific to merchants using Moneris payment solutions. It addresses the following:

- Terminals – Point to Point Encryption ("P2PE") terminals, non-P2PE terminals, legacy terminals,
- Portals and Web Interfaces,
- Systems Using Moneris Payment Gateway Application Programming Interface ("APIs"), and
- e-Commerce Solutions.

It provides guidance on identifying the correct reporting forms, understanding Self Assessment Questionnaire ("SAQ") eligibility, using SAQ guidance to complete a Report on Compliance ("ROC"), and managing compliance for complex environments.

Audience

This document is intended for merchants who use Moneris payment processing solutions, as well as Information Technology ("IT") administrators, compliance officers, PCI Qualified Security Assessors ("QSA"), PCI Internal Security Assessors ("ISA"), and any personnel responsible for PCI compliance reporting.

PCI DSS reporting overview.

This document can be used by all Moneris merchants for reporting on either an SAQ or a ROC.

Step-by-step process to Knowing Your Scope and Reporting

For each product your organization uses, you need to identify:

1. The specific solution you are using.
2. Which PCI DSS requirements apply to your organization, which requirements are satisfied by Moneris, which requirements do not apply, and any requirements with shared responsibilities.
3. Which compliance form to report on including if and how you can use an SAQ.

For solutions supported by other third parties, the merchant is responsible for ensuring the third party provides any necessary compliance documentation.

Using SAQs vs ROCs

PCI Self-Assessment Questionnaires are intended to provide short-reporting forms for small merchants with simple payment environments. For eligible merchants, they are also a useful shorthand for determining which requirements apply regardless of your reporting form (i.e. SAQ vs ROC).

Important: Merchants that must report using a ROC can use SAQs to consider which requirements apply to them! For details, see PCI FAQ 1331 (Nov 2024).

For the remainder of this document, we will refer to the short form SAQs for the applicable requirements even for merchants completing a ROC per FAQ 1331.

SAQ Eligibility and Complex Environments

Short form SAQs can only be considered if your organization has met the specific eligibility requirements documented in Part 2h of each SAQ. If your environment is ineligible, you must use SAQ D for Merchants or a full ROC.

Before we get into complex environments, some SAQs like P2PE include requirements to address Cardholder Data (“CHD”) on paper. If CHD on paper is not present in the data flow, those requirements can be reported as “N/A No Cardholder Data on paper exists” with appropriate justification.

Merchants with multiple separate environments may need to merge the reporting into a ROC or SAQ D. Some examples:

- Retailer with separate card-present and e-commerce data flows. These are good candidates for separate reporting.
- Call-center using telephony (e.g. Voice over IP (“VoIP”) and payment terminals in a single flow). Combined or mixed flows should be reported in a single document.

SAQ merchants may be able to complete separate specialized SAQs for each environment if allowed by your compliance accepting entity.

ROC merchants can also report separately for each data flow; however, they are more likely to combine all findings into a single ROC.

Each form will need to document the exclusions that you are reporting separately. For example, a merchant filing an SAQ P2PE for their card present and an SAQ A for their ecommerce would use the excluded flows in part 2a and indicate there is a separate assessment.

Moneris products.

The following describes the processes for determining which Moneris' solutions your organization is using, the base reporting form, and which requirements apply to your organization.

Payment terminals and devices

Identify your terminal solution(s)

Use the following table to identify which group your solution belongs to.

Table 1: Identifying your terminal's solution group

Terminal group	Terminal name	Description
Moneris P2PE	Moneris Go DX8000 Moneris Go EX8000 Moneris POSPad P400	P2PE enabled merchants with these products that have retained and followed the PIM can benefit from P2PE compliance. Important: if you are not a P2PE enabled merchant and have one of these terminals, please find your solution in the rows below. If you are uncertain if you are a P2PE enabled merchant contact Moneris.
Moneris Tap-to-Pay	iPhones	PCI MPOC (Mobile Payments on Commercial Off-The Shelf) approved solutions. — Apple Tap-to-Pay for iPhone, reference # 2025-01597.001.

Terminal group	Terminal name	Description
Moneris Terminals	Moneris Go A35 Moneris Go A920 Moneris Go DX8000 Moneris Go EX8000 Moneris Go IM30 Moneris POSPad E355 Moneris POSPad ICMP Moneris POSPad IPP320 Moneris POSPad P400 Direct Connect UX300 Direct Connect UX301 Direct Connect UX410 Moneris Core Desk/5000 Moneris Core Move/5000 Moneris Core V400c Moneris Core V400m	Non-P2PE enabled merchants with these Moneris designed and developed products using PCI PIN Transaction Security (“PTS”) approved devices benefit from strong encryption with no access to cardholder data and no ability to disable or compromise the encryption, out-of-the-box secure configurations and more. These Moneris Terminals come in four families. — GO — POSpad — Direct Connect — Core Moneris Terminals design characteristics: — Connected systems, such as Point-of-Sale (“POS”), cannot receive nor decrypt cardholder data. — Terminal cannot display or export cardholder data — Terminal security controls cannot be disabled No remote access
Moneris Legacy Terminals	Moneris ICT250 Moneris IWL220 Moneris VX 520 Moneris VX 820	Merchants with these PTS approved terminals will need to meet additional PCI DSS requirements. Note: These devices are obsolete and being deprecated.
Non-Moneris Terminals	N/A	Merchants that purchase or contract non-Moneris supplied terminals and products are fully responsible for determining the compliance of those devices and any connected systems and networks. Examples of these include: Automated Fuel Dispensers (“AFD”) and Kiosk devices, and solutions from third-party processors. Moneris takes no responsibility for these solutions and has not determined the applicability of any DSS requirements for any third-party devices.

For compliance reporting you will also need details of the applicable PCI approvals which can be found as follows:

Table 2: Finding supporting PCI approved information

Terminal group	Description
Moneris P2PE	– For PTS and P2PE approval information please refer to the specific P2PE Implementation Manual for your solution
Moneris Tap-to-Pay	– Apple Tap-to-Pay for iPhone – Additionally, Moneris is currently working toward MPOC certifications and will update this document when they are complete.
Moneris Terminals	– For PTS Approval information please refer to https://support.moneris.com/topic/moneris-go-solutions/moneris-go for Moneris Go or to https://support.moneris.com/topic/pos-solutions for other Moneris Terminals
Moneris Legacy Terminals	– For PTS Approval information please refer to https://support.moneris.com/topic/pos-solutions
Non-Moneris Terminals	– Contact your terminal supplier for PTS and any other applicable PCI Approvals

Applicable terminal requirements/responsibilities

The table below shows for each terminal group which requirements apply and/or are not applicable for the full PCI DSS. This allows you to report on a ROC or SAQ D or any of the short form SAQs (see next section).

To simplify the interpretation and maintenance of these tables, responsibilities may be defined in terms of SAQs with additional requirements applying to the merchant or Moneris.

Where a terminal group adds to the requirements of an SAQ (e.g. Moneris Terminals being based on an SAQ P2PE) and there is an eligibility requirement to use a specific approved PCI solution (e.g. P2PE) the requirement should be interpreted as requiring the specific Moneris solution. All other eligibility requirements must be met.

Where requirements are indicated as Moneris or N/A, you should document the requirement as being not applicable. For example, if you are documenting your compliance for a “Moneris Terminals” solution on an SAQ D form, you need to answer all the requirements listed in SAQ P2PE plus the additional requirements listed below. All other requirements in SAQ D would be list as Not Applicable with the reason “N/A Fulfilled by Moneris or N/A for the solution”.

Table 3: Applicable requirements by terminal group

Terminal group	Merchant applicable	Moneris or N/A	Shared responsibilities
Moneris P2PE	– SAQ P2PE		

Terminal group	Merchant applicable	Moneris or N/A	Shared responsibilities
Moneris Tap-to-Pay	– All SAQ MPOC (see note below)	– All other requirements are N/A to merchant.	– None
Moneris Terminals	– All SAQ P2PE requirements plus: 1.2.3, 1.2.4	– All other requirements are N/A to merchant. — Moneris is responsible for minor changes and updates to the solution	– Where manual updates are required, merchants must coordinate changes with Moneris
Moneris Legacy Terminals	– All SAQ B-IP requirements plus: 1.2.2, 1.2.3, 1.2.4, 1.4.1, 1.4.2, 3.2.1, 4.2.2, 6.5.1, 6.5.2	– The following are requirements in this SAQ are N/A: 1.2.5, 1.2.6, 2.2.7, 3.3.1, 3.3.1.1, 3.3.1.3, 4.2.1, 6.3.1, 7.2.2, 8.2.2, 8.2.7, 8.4.3 – Cellular standalone terminals can mark 1.3.x, 1.4.x as N/A – All other requirements are N/A to merchant. – Moneris is responsible for minor changes and updates to the solution	– Where manual updates are required, merchants must coordinate changes with Moneris
Non-Moneris Terminals	– SAQ D — Connected systems are in scope	– None	– Must be approved by Moneris and operationally certified

Notes:

- Moneris Tap-to-Pay: Solutions listed with a PCI MPOC approval can be reported on SAQ MPOC. Any Moneris approved solutions that have not yet been listed PCI MPOC solution should be reported on SAQ D indicating requirements that are not applicable per the instructions above.
- Moneris whitepapers have strongly recommend the use of firewalls to protect devices in the “Moneris Terminals” group but did not require them for PCI DSS.

Identify your base reporting template (SAQ)

Use this table below to understand the communications modes supported by Moneris Terminals and Moneris Legacy terminals. These will be used with the next table to identify the PCI SAQ reporting form.

This table is not needed if you have a validated Moneris P2PE Terminal or a Moneris Tap-to-Pay solution.

Table 4: Identifying your reporting template – part 1—communication modes

Mode	Terminal group/family	Description of mode
Dial	Moneris Legacy Terminals	Standalone terminals that only connect to Moneris over Dial-up (non-VoIP).
Standalone	Moneris Terminals (Go), Moneris Legacy Terminals	Stand-alone terminals that connect to Moneris over Transmission Control Protocol / Internet Protocol (“TCP/IP”), Wi-Fi, or cellular.
Cloud	Moneris Terminals (Go, POSpad)	Standalone terminals that connect to Moneris over TCP, Wi-Fi, or cellular that interacts indirectly with the merchant’s POS via Moneris’ Cloud POS system and pairing tokens.
Direct-to-Host and Legacy semi-integrated	Moneris Terminals (Go, POSpad, Direct Connect, Other Core products), Moneris Legacy Terminals	Semi-Integrated terminals with direct network connections to Moneris for authorization and other connections (e.g. serial, Universal Serial Bus (“USB”), TCP/IP, Wi-Fi, or Bluetooth) to merchant systems to support POS integration.
Secure-PassThru	Moneris Terminals (POSpad)	Fully integrated terminals that encrypt all cardholder data. The terminal does not connect directly to Moneris. Instead, the connected POS facilitates transmission of encrypted cardholder data to Moneris but does not receive nor can it decrypt cardholder data.
App-to-App	Moneris Terminals (Go)	Moneris GO terminals that support App-to-App integration allow for the inclusion of third-party non-payment applications (i.e. no access to cardholder data) that run inside the terminal alongside Moneris’ payment application. The communication resembles the networked Direct-to-host mode and compliance is reported in the same manner. Third party applications must be signed and provisioned by Moneris and may require additional security review before being accepted.

Use this table to identify which SAQ form to use as a base for reporting compliance depending on the communication mode of the solution.

This table is not needed if you have a validated Moneris P2PE Terminal.

Table 5: Identifying your reporting template – part 2 – SAQ forms

Communication mode	Reporting SAQ
Standalone (dial)	B
Standalone (cellular)	B-IP
Standalone (network/wi-fi)	B-IP
Direct-to-host (Serial/USB)	B-IP
Direct-to-host (network/wi-fi) and legacy semi-integrated	D
Cloud	B-IP
Secure pass through	D
App to app	D

Please note that there is no SAQ short form that addresses semi-integrated payment terminals (e.g. Direct-to-host network/Wi-Fi). Neither SAQ B-IP nor SAQ C can be used as they fail the “not connected to any other systems within the merchant environment” eligibility requirements. SAQ D is required for “Merchants that do not store account data electronically but that do not meet the criteria of another SAQ type.”

A practical example

Let’s look at a practical example of a Moneris merchant reporting their compliance using the method above. While someone with PCI DSS training should be able to follow the process, it may be difficult for someone less well versed.

A fictional merchant, ACME gifts, runs a small chain of brick-and-mortar stores. They recently upgraded to Moneris Go DX8000 standalone terminals connected to their store Local Area Network (“LAN”). This example is a simple cardholder data flow with no mail-in, telephone, e-commerce card acceptance flows, and no use of any virtual terminal solution to enter cardholder data (For more complex flows see SAQ Eligibility and Complex Environments above).

1. The DX8000 is part of the “Moneris Terminals” group which says the merchant is responsible for all the requirements in SAQ P2PE plus requirements 1.2.3, 1.2.4.
2. The communication mode “Standalone (Network/Wi-Fi)” needs to be reported on an SAQ B-IP form.
3. The merchant should retrieve the current SAQ B-IP and SAQ P2PE forms from the PCI Document Library.
4. Review the SAQ B-IP eligibility requirements (Part 2h). Additionally, this must be a terminal from the “Moneris Terminals” group. If any of the eligibility requirements are not true, then you will need to report using SAQ D Merchant.
5. Using your reporting SAQ (B-IP or D Merchant).
   a) Complete the executive summary including the PCI PTS references for your terminals.
   b) In section 2 you will be answering all questions that are listed in SAQ P2PE plus the additional requirements identified.

c) All other requirements (e.g. 1.2.5) can be marked N/A and listed in Appendix C: Explanation of Requirements Noted as Not Applicable with the reason “Fulfilled by Moneris or N/A for the solution” and update Part 2g of the executive summary.

Portals and web interfaces

Use the following table to identify which group your solution belongs to.

Table 6: Identifying your portal’s functionality under PCI DSS

Portal solution	Portal group
Merchant Resource Centre	Portals with Virtual Terminals that allow entry of cardholder data from merchant systems.
Moneris Go Portal	Includes Moneris token vault card registration.
Merchant Direct	Portals that do not accept entry of nor have access to cardholder data

Table 7: Applicable requirements for portal solutions

Portal group	Merchant applicable	Moneris or N/A	Shared responsibilities
Portals with Virtual Terminals	Use SAQ C-VT for merchant workstations/systems	Moneris is fully responsible for the portal infrastructure	None
Portals without Access to Cardholder Data	Merchant workstations/systems not in scope for merchant PCI DSS	Moneris is fully responsible for the portal infrastructure	None

Notes:

- The merchant may have non-PCI DSS security requirements over portal functionality.
- The above responsibilities do not override obligations and previous legal agreements for customized interfaces that may exist.

Systems using Moneris payment gateway APIs

Moneris provides several API solutions for use with the following payment gateways:

Table 8: Payment API applicable requirements and shared responsibilities

Gateway APIs	Merchant applicable	Moneris or N/A	Shared responsibilities
IPGate, Moneris Gateway, Terminal Gateway, Transit Gateway	– Merchant and third parties are fully responsible for all application code that sees cardholder or sensitive authentication data and relies upon Moneris' Gateway APIs or integrates with Moneris gateways. – Third-Party payment software may require PCI Secure Software Assessment approval.	– Moneris is responsible for specification documents and secure development of API code that they supply to merchants for inclusion in merchant/third-party applications. – Moneris is fully responsible for the payment gateway infrastructure.	– Merchants must coordinate changes and updates to their applications with Moneris including for any security changes in the APIs.

Moneris checkout e-commerce

Responsibilities

The following tables identify the different types of e-commerce solutions used by Moneris merchants and the compliance reporting framework for each.

Table 9: Identifying the type of e-commerce implementation

Solution		Reporting SAQ
Moneris Checkout	The merchant's shopping cart calls the Moneris Checkout script which builds an IFRAME that contains the form that sends all cardholder and sensitive authentication data elements (e.g. PAN, Expiry Date, Security Codes) directly to Moneris.	A
Moneris Checkout w/hosted Shopping Cart	The merchant is using a third-party integration to Moneris Checkout for their shopping cart. The shopping cart links or redirects to a Moneris hosted page that builds the Moneris Checkout IFRAME,	A
Merchant Shopping Cart with Third Party Processor	The merchant's e-commerce solution uses a third-party processor's IFRAME, Link, Redirection, Direct Post Form, or Gateway. The merchant's reporting form will be determined by the mechanism that transmits cardholder data to the third party.	A, A-EP. D
Merchant Payment Page	The merchant's e-commerce solution receives all cardholder data and relays it directly or indirectly to Moneris using one of the Gateway APIs (see above) or a third-party processor.	D

Table 10: Moneris checkout responsibilities

Solution	Merchant applicable	Moneris or N/A	Shared responsibilities
Moneris Checkout	– Merchant is responsible for their shopping cart and must protect the Moneris Checkout script.	– Moneris is responsible for the development and content of the Moneris Checkout script and Moneris Gateways receiving the cardholder data.	– See note below

Solution	Merchant applicable	Moneris or N/A	Shared responsibilities
Moneris Checkout w/hosted Shopping Cart	– Merchant is responsible for their shopping cart and must protect the Moneris Checkout linkage.	– Moneris is responsible for the development and content of the Moneris Checkout script and Moneris Gateways receiving the cardholder data. Moneris is also responsible for the protection of the Moneris Checkout script.	– See note below
Merchant Shopping Cart with Third Party Processor, Merchant Payment Page	– Merchant is responsible for ensuring compliance of their e-commerce solution and any third-party service providers.	– None	– None

Notes:

- Moneris Checkout does not use direct POST forms to transmit cardholder data.
- For Moneris Checkout Product Documentation please refer to https://developer.moneris.com/.
- For requirements 6.4.3 and 11.6.1, the responsibilities are essentially shared. Moneris is responsible for the implementation of these controls within the Moneris Checkout IFRAME and the client is responsible for these requirements in their shopping cart (i.e. they must protect the script they invoke that builds Moneris Checkout.

Evolving PCI DSS e-commerce guidance

PCI DSS v4.0 introduced two new requirements, 6.4.3 and 11.6.1, that became effective in April 2025 which are intended to protect JavaScript integrity and combat the threat of e-skimming (a.k.a. Magecart) attacks. The precise guidance for these requirements is technical and evolving. It is not uncommon for new PCI DSS requirements to go through a period of fine tuning after they are introduced.

Both the PCI DSS reporting form and the new requirements depend on the mechanisms used in e-commerce.

- Shopping carts using mechanisms like IFRAMEs, links, redirection create a new Document Object Model ("DOM") in the cardholder's browser prevent scripts on their pages from eavesdropping on the payment fields.

- Different mechanisms can be dynamically tampered in the cardholder’s browser by JavaScripts. The mechanisms linking the merchant shopping cart and the processors payment page require ant-tampering controls.

Below is a list of the PCI guidance available at the time of writing. It is strongly recommended that merchants verify they are using the most recent guidance.

Notes:

- Organizations completing SAQ A do not need to address requirements 6.4.3 and 11.6.1 directly but answer the eligibility question “The merchant has confirmed that their site is not susceptible to attacks from scripts that could affect the merchant’s e-commerce system(s)”. (See SAQ A r1).
- Organizations completing a ROC based on SAQ A applicability, should address requirements 6.4.3 and 11.6.1 directly. (see Guidance for PCI DSS Requirements 6.4.3 and 11.6.1 v1.0).
- Not all linkage mechanisms may require integrity controls (e.g. certain types of redirections); however, this may change. We recommend merchants review the current guidance, their risk, and carefully consider integrity controls for all linkage mechanisms.

Below is a list of the PCI E-Commerce Guidance and Frequently Asked Questions (“FAQ”) available at the time of writing. It is strongly recommended that merchants verify they are using the most recent guidance.

- Guidance for PCI DSS Requirements 6.4.3 and 11.6.1 v1.0R1 (April 2025)
- FAQ 1592 (Mar 2025) Are providers of third-party scripts for e-commerce environments considered third-party service providers for PCI DSS Requirements 12.8 and 12.9?
- FAQ 1588 (Mar 2025) How does an e-commerce merchant meet the SAQ A eligibility criteria for scripts?
- FAQ 1581 (Aug 2024) How does PCI DSS Requirement 6.4.3 apply to 3DS scripts called from a merchant check-out page as part of 3DS processing?
- Best Practices for Securing E-commerce (Apr 2017)
- FAQ 1438 (Nov 2016) How is the payment page determined for SAQ A merchants using iframe?
- FAQ 1291 (Aug 2015) Why is SAQ A-EP used for Direct Post while SAQ A is used for iFrame or URL redirect?
- FAQ 1293 (Jun 2014) If a merchant's e-commerce implementation meets the criteria that all elements of payment pages originate from a PCI DSS compliant service provider, is the merchant eligible to complete SAQ A or SAQ A-EP?

Assistance with PCI DSS.

If your organization requires assistance with interpreting PCI DSS requirements, validation activities, documenting compliance, or other advice please contact a Qualified Security Assessor (QSA) or your organization's approved Internal Security Assessor (ISA) if you have one.

PCI References

PCI DSS and SAQs: https://www.pcisecuritystandards.org/document_library/. In particular, the SAQ instructions and guidelines, SAQ: A, A-EP, P2PE, MPOC, B, B-IP, C, C-VT, D - published and/or updated between Oct 2024 and April 2025.

PCI Frequently Asked Questions: https://www.pcisecuritystandards.org/faqs/.

PCI Listings

P2PE Solutions:
https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions.

Mobile Payment on COTS solutions:
https://listings.pcisecuritystandards.org/assessors_and_solutions/mpoc_solutions.

Secure Software: https://listings.pcisecuritystandards.org/assessors_and_solutions/payment_software.

PA-DSS Solutions:
https://listings.pcisecuritystandards.org/assessors_and_solutions/payment_applications.

PTS Devices (Current):
https://listings.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices.

PTS Devices (Expired/Legacy):
https://listings.pcisecuritystandards.org/assessors_and_solutions/approved_pin_transaction_security_expired.

Note:

- Expired PCI listed products may still be acceptable for pre-existing deployments.

Contacting Moneris.

If you have questions about the solutions in this document or about Moneris' solutions, please review the following.

For solution information, the following Moneris resources referenced in this document:

- Moneris Go Terminals: https://support.moneris.com/topic/moneris-go-solutions/moneris-go.
- Moneris Terminals: https://support.moneris.com/topic/pos-solutions.
- Moneris developer resources including Merchant Resource Centre, Virtual Terminal, Gateway API's, and Moneris Checkout: https://developer.moneris.com/.

For questions about this compliance document please contact your Moneris Account Executive or PCIDSS@moneris.com.

For all other inquiries please use our contact page: https://www.moneris.com/en/support/contact.

Definitions and acronyms.

For a complete list of PCI glossary terms and acronyms, please refer to the official PCI Security Standards Council glossary at: PCI Glossary:

- **PIM:** P2PE Instruction Manual.
- **PCI DSS:** Payment Card Industry Data Security Standard.
- **P2PE:** The Point-to-Point Encryption standard and approved P2PE products.
- **MPOC:** The Mobile Payments on COTS (Commercial Off-the-Shelf) standard.
- **AOC:** Attestation of Compliance for a ROC or AOC.
- **ROC:** Report on Compliance.
- **SAQ:** Self-Assessment Questionnaire for small merchant compliance reporting.
- **SAQ Eligibility:** The eligibility requirements that must be met to use each specific SAQ for reporting.
- **CHD:** Cardholder Data.
- **SAD:** Sensitive Authentication Data.
- **POS:** Point of Sale, typically the electronic cash register systems.
- **POI:** Point of Interaction, the device that accepts the card.
- **PTS:** PIN Transaction Security, a standard for Payment Terminals/devices.
- **API:** Application Programming Interface.
- **QSA:** Qualified Security Assessor.
- **ISA:** Internal Security Assessor.

Review and revision history.

Version	Date	Description
1.0	24.04.25	Initial version for PCI DSS 4.0.1
1.0.1	05.05.25	Minor clarifications and elaboration. Addition of Apple Tap-To-Pay.