
# Cybersecurity Standards and Programs

*Frequently Asked Questions*

15 March 2021

## Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

### Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively "Mastercard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

### Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

### Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third-party patents, copyrights, trade secrets or other rights.

### Translation

A translation of any Mastercard manual, bulletin, release, or other Mastercard document into a language other than English is intended solely as a convenience to Mastercard customers. Mastercard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall Mastercard be liable for any damages resulting from reliance on any translated document. The English version of any Mastercard document will take precedence over any translated version in any legal proceeding.

# Contents


## Cybersecurity Standards and Programs Frequently Asked Questions

Document Purpose
Reference Document

## Cybersecurity Standards

What are Mastercard's Cybersecurity Standards?
Who must comply with Cybersecurity Standards?
What does Mastercard consider "confidential information"?
How is "account data" defined?
Do I need to comply with the PCI DSS if I store, process, or transmit account data?
What do I need to comply with if I only store, process, or transmit confidential information?
What is the National Institute of Standards and Technology Cybersecurity Framework?
Why is Mastercard recommending that customers that store, process, or transmit confidential information comply with the NIST CSF OR one of its "Informative References"?
Are customers that store, process, or transmit account data required to validate PCI DSS compliance to Mastercard?
Are customers that store, process, or transmit confidential information required to validate NIST CSF compliance to Mastercard?
Where can I find Cybersecurity Standards documents such as the PCI DSS, the NIST CSF and the NIST CSF "Informative References"?

## Payment Card Industry (PCI) Security Standards

What are the PCI Security Standards?
Who is responsible for developing and managing the security standards?
Does Mastercard manage PCI compliance requirements and validation?
Who must comply with PCI Security Standards?
What is the PCI Data Security Standard? Where can I find supporting documents?
What are the PCI Card Production & Provisioning Physical & Logical Security Requirements?
What are the PCI PIN Transaction Security (PTS) Requirements and where can I find approved PTS devices?
What other PCI Security Standards does Mastercard require entities to comply with?
Where can I find PCI standards documentation, reporting templates and forms?
Does Mastercard accept PCI compliance certificates as validation?
How do I find PCI SSC-certified organizations and individuals to assess and validate PCI compliance?
Where can I find PCI SSC-approved products, solutions and providers?
What is the PCI SSC FAQs resource database?

## Mastercard Site Data Protection (SDP) Program

What is the Mastercard SDP Program?
Who must comply with the PCI DSS under the SDP Program?
Which entities are required to validate their PCI compliance to Mastercard?
I am a Mastercard customer. Do I need to validate PCI DSS compliance to Mastercard?
I am an issuer. What do I need to do to meet SDP Program requirements?
I am an acquirer. What do I need to do to meet SDP Program requirements?
I am a merchant. What do I need to do to meet SDP Program requirements?
I am a service provider. What do I need to do to meet SDP Program requirements?
How can I be listed on *The Mastercard SDP Compliant Registered Service Provider List*?
What is the Mastercard Cybersecurity Incentive Program (CSIP) for merchants?
Where can I find eligibility requirements for the PCI DSS Risk-based Approach and PCI DSS Validation Exemption Program?
What is Mastercard's ISA mandate for Level 1 merchants?
What is Mastercard's mandate for merchants and service providers that use eligible third party-provided payment applications or payment software?
Are there fines for entities that are noncompliant with the SDP Program?
Where can I find Mastercard SDP Standards?

## Card Production Security Standards

What do card production activities consist of?
Who is required to ensure that all card production activities are performed in compliance with Card Production Security Standards and Card Design Standards?
What is the Mastercard Global Vendor Certification Program (GVCP)?
What is GVCP certification?
What entities require GVCP certification?
What PCI Security Standards apply to GVCP certification?
How do I begin the GVCP certification process?
What are the key milestones for GVCP certification?
How long does it take a vendor to achieve GVCP certification?
After GVCP certification is achieved, how does a vendor maintain their certification?
How do I determine if an auditor is qualified to assess card production security?
How can I validate that a card production facility is GVCP certified?
Where can I find additional information about GVCP?

## Terminal and PIN Entry Security Standards

*Terminal and PIN Entry Security Standards FAQs* can be found in a separate document available on the Mastercard PCI 360 site.

# Cybersecurity Standards and Programs—Frequently Asked Questions

## Document Purpose

The purpose of this document is to answer commonly asked questions about Mastercard Cybersecurity Standards and Programs.

## Reference Document

The ***Security Rules and Procedures***—*Chapter 2 Cybersecurity Standards and Programs*—is available on Mastercard Connect™ for further references.

# Cybersecurity Standards

*The following list of questions is designed to assist Mastercard customers with Cybersecurity Standards requirements.*

**Q. What are Mastercard's Cybersecurity Standards?**

Mastercard's Cybersecurity Standards consist of mandates and best practice recommendations for the implementation and maintenance of baseline cybersecurity controls. Cybersecurity Standards include standards published by the Payment Card Industry Security Standards Council (PCI SSC) and the National Institute of Standards and Technology (NIST) agency of the United States Department of Commerce.

**Q. Who must comply with Cybersecurity Standards?**

Each Mastercard customer and their agents must comply with Cybersecurity Standards by establishing and maintaining meaningful cybersecurity controls for any environment, system, or device used to store or process confidential information or account data.

**Q. What does Mastercard consider "confidential information"?**

Mastercard considers confidential information as any information resulting from activity, digital activity, payment transfer activity, or any service provided by or product of Mastercard and which information is deemed by a person other than Mastercard (including, by way of example and not limitation, a customer or merchant or cardholder) to be confidential information of such person.

**Q. How is "account data" defined?**

Account data is defined as any cardholder data and/or sensitive authentication data.

*Cardholder Data*—The cardholder name, primary account number (PAN), and expiration date associated with an account (including any token or virtual account), and the service code on a magnetic stripe card.

*Sensitive Authentication Data*—The full contents of a card's magnetic stripe, card validation code 2 (CVC 2) data, and PIN or PIN block data.

**Q. Do I need to comply with the PCI DSS if I store, process, or transmit account data?**

Yes. Customer environments that store, process, or transmit account data must comply with the PCI Data Security Standard in accordance with the Mastercard Site Data Protection (SDP) Program, and with all other applicable PCI Security Standards and Mastercard cybersecurity programs.

**Q. What do I need to comply with if I only store, process, or transmit confidential information?**

As a best practice to ensure sufficient cybersecurity controls are established and maintained, all customer environments, systems, or devices used to store, process, or transmit confidential information are recommended to comply with at least one of the following:

- The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF); **OR**
- One of the standards included as "Informative References" to the NIST CSF, currently:
  - Control Objectives for Information and Related Technology (COBIT)
  - Center for Internet Security (CIS) Critical Security Controls for Effective Cyber Defense (CIS Controls)
  - American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009
  - International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001
  - NIST Special Publication (SP) 800-53 Rev. 4 - NIST SP 800-53

**Q. What is the National Institute of Standards and Technology Cybersecurity Framework?**

The NIST CSF is a globally recognized cybersecurity standard with an overarching security and risk management structure. The framework provides guidance and is based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk.

**Q. Why is Mastercard recommending that customers that store, process, or transmit confidential information comply with the NIST CSF OR one of its "Informative References"?**

Security of all customer environments where confidential information is stored, processed, or transmitted is vital to the safety and security of the global payments system. While the PCI standards have successfully helped secure Cardholder Data Environments (CDE) around the world, their applicability and scope are limited to specific environments. For customer environments where the PCI Security Standards do not apply, but where security assurance remains necessary, the NIST CSF or one of its "Informative References" are recommended as a best practice.

**Q. Are customers that store, process, or transmit account data required to validate PCI DSS compliance to Mastercard?**

No. While customers that store, process, or transmit account data are required to comply with the PCI DSS in accordance with the Mastercard SDP Program and all other applicable PCI Security Standards, validation of compliance to Mastercard is not required.

**Q. Are customers that store, process, or transmit confidential information required to validate NIST CSF compliance to Mastercard?**

At this time, compliance with the NIST CSF is recommended as a best practice only. Validation of compliance to Mastercard is not required.

**Q. Where can I find Cybersecurity Standards documents such as the PCI DSS, the NIST CSF and the NIST CSF "Informative References"?**

The following Cybersecurity Standards documents can be found at:

- PCI Security Standards—https://www.pcisecuritystandards.org
- NIST CSF and NIST CSF "Informative References"—https://www.nist.gov/cyberframework

# Payment Card Industry (PCI) Security Standards

*The following list of questions is designed to assist customers, merchants, service providers and card production vendors with PCI Security Standards programs and compliance requirements.*

**Q: What are the PCI Security Standards?**

PCI Security Standards are technical and operational requirements established by the PCI SSC to act as a minimum baseline to protect account data. The standards apply to all entities that store, process, or transmit cardholder data – with requirements for software developers and manufacturers of applications and devices used in transactions.

**Q: Who is responsible for developing and managing the security standards?**

The PCI SSC is responsible for developing and managing the security standards as well as promoting the standards globally. The PCI SSC also provides critical tools needed for the implementation of the standards such as assessment and scanning qualifications, self-assessment questionnaires, training and education, and product certification programs.

**Q: Does Mastercard manage PCI compliance requirements and validation?**

Yes. Mastercard is responsible for managing PCI compliance requirements, validation of compliance, and tracking and enforcement of PCI compliance.

**Q: Who must comply with PCI Security Standards?**

Mastercard requires that all issuers, acquirers, merchants, service providers, card production vendors, and other customer agents that store, process, or transmit card, cardholder, or transaction data comply with PCI Security Standards.

**Q: What is the PCI Data Security Standard? Where can I find supporting documents?**

The PCI DSS is a set of comprehensive requirements for enhancing security of payment card account data. It covers technical and operational system components included in or connected to cardholder data. If an entity accepts or processes payment cards, then the PCI DSS will apply.

The PCI DSS and supporting documents are available on the PCI SSC website at www.pcisecuritystandards.org.

**Q: What are the PCI Card Production & Provisioning Physical & Logical Security Requirements?**

The PCI Card Production Logical and Physical Security Requirements address card production activities including card manufacturing, chip embedding, data preparation, pre-personalization, card personalization, chip personalization, fulfillment, packaging, storage, mailing, shipping, PIN printing and mailing (personalized, credit or debit), PIN printing (non-personalized prepaid cards), and electronic PIN distribution.

**Q: What are the PCI PIN Transaction Security (PTS) Requirements and where can I find approved PTS devices?**

The PCI PTS is a set of security requirements focused on characteristics and management of devices used in the protection of cardholder PINs and other payment processing related activities. The PTS standards include PIN Security Requirements, Point of Interaction (POI) Modular Security Requirements, and Hardware Security Module (HSM) Security Requirements. The device requirements are for manufacturers to follow in the design, manufacture and transport of a device to the entity that implements it.

PCI approved devices can be found on the PCI SSC website at www.pcisecuritystandards.org/assessors_and_solutions.

**Q: What other PCI Security Standards does Mastercard require entities to comply with?**

Other PCI Security Standards and compliance requirements applicable to issuers, acquirers, merchants, service providers, card production vendors, and other customer agents can be found in *Table 2.1—PCI Security Standards Documentation and Compliance Requirements and Recommendations* in the SR&P.

**Q: Where can I find PCI standards documentation, reporting templates and forms?**

PCI standards documentation, reporting templates and forms can be found at www.pcisecuritystandards.org/document_library. The PCI SSC website is the only source of official reporting templates and forms that are approved and accepted by all payment brands. These include Report on Compliance (ROC) templates, Attestations of Compliance (AOC), Self-Assessment Questionnaires (SAQ), and Attestations of Scan Compliance from external vulnerability scans.

**Q: Does Mastercard accept PCI compliance certificates as validation?**

No. The only documentation recognized for PCI Security Standards validation and accepted by Mastercard are the official documents from the PCI SSC website. Any other form of certificate or

documentation issued for the purposes of illustrating PCI compliance are not acceptable for validating compliance to Mastercard.

**Q: How do I find PCI SSC-certified organizations and individuals to assess and validate PCI compliance?**

PCI SSC-certified organizations and individuals to assess and validate PCI compliance can be found on the PCI SSC website at www.pcisecuritystandards.org/assessors_and_solutions.

**Q: Where can I find PCI SSC-approved products, solutions and providers?**

PCI SSC-approved products, solutions and providers can be found on the PCI SSC website at www.pcisecuritystandards.org/assessors_and_solutions.

**Q: What is the PCI SSC FAQs resource database?**

The PCI SSC FAQs resource database is a searchable tool that includes a library of questions and answers on a variety of topics across PCI Security Standards and programs. It is updated regularly to address common questions PCI SSC receives from stakeholders.

The PCI SSC FAQs can be found on the PCI SSC website at www.pcisecuritystandards.org/faqs.

# Mastercard Site Data Protection (SDP) Program

*The following list of questions is designed to assist issuers, acquirers, merchants and service providers with Mastercard SDP Program compliance requirements.*

**Q: What is the Mastercard SDP Program?**

The Mastercard SDP Program consists of rules, guidelines, best practices and approved compliance validation tools to foster broad compliance with the PCI Security Standards. The SDP Program is designed to help customers, merchants, and service providers protect against Account Data Compromise (ADC) Events.

**Q: Who must comply with the PCI DSS under the SDP Program?**

Compliance with the PCI DSS and all other applicable PCI Security Standards is required for all issuers, acquirers, merchants, service providers and any other person or entity that a customer permits, directly or indirectly, to store, transmit, or process account data.

**Q: Which entities are required to validate their PCI compliance to Mastercard?**

Only merchants and service providers are required to validate their PCI compliance to Mastercard in order to be deemed compliant with the Mastercard SDP Program.

**Q: I am a Mastercard customer. Do I need to validate PCI DSS compliance to Mastercard?**

No. While compliance with the PCI DSS is required for all issuers and acquirers, validation of a customer's compliance is not required.

**Q: I am an issuer. What do I need to do to meet SDP Program requirements?**

To ensure compliance with the Mastercard SDP Program, an issuer must:

- Communicate the SDP Program requirements to each Level 1 and Level 2 service provider and validate the service provider's compliance with the PCI DSS and any other applicable PCI Security Standard by reviewing the PCI Self-Assessment Questionnaire or the Report on Compliance; and
- Submit the annual PCI compliance validation for each Level 1 and Level 2 service provider to pcireports@mastercard.com after initial registration with Mastercard and every year thereafter.

**Q: I am an acquirer. What do I need to do to meet SDP Program requirements?**

To ensure compliance with the Mastercard SDP Program, an acquirer must:

- Communicate the SDP Program requirements to each Level 1, Level 2, and Level 3 merchant, and validate the merchant's compliance with the PCI DSS by reviewing the PCI Self-Assessment Questionnaire or the Report on Compliance;
- Submit the *SDP Acquirer Submission and Compliance Status Form* for each Level 1, Level 2, and Level 3 merchant semi-annually to sdp@mastercard.com;
- Validate to Mastercard that the acquirer has a risk management program in place to identify and manage payment security risk within the acquirer's Level 4 merchant portfolio;
- Communicate the SDP Program requirements to each Level 1 and Level 2 service provider and validate the service provider's compliance with the PCI DSS and any other applicable PCI Security Standard by reviewing the PCI Self-Assessment Questionnaire or the Report on Compliance; and
- Submit annual PCI validation for each Level 1 and Level 2 service provider to pcireports@mastercard.com after initial registration with Mastercard and every year thereafter.

**Q: I am a merchant. What do I need to do to meet SDP Program requirements?**

Mastercard requires Level 1, Level 2, Level 3 and Level 4 merchants to comply with the PCI DSS and successfully validate compliance as follows:

- *Level 1 merchants*—must successfully undergo an annual PCI DSS assessment resulting in the completion of a ROC conducted by a PCI SSC-approved Qualified Security Assessor (QSA) or PCI SSC-approved Internal Security Assessor (ISA)
- *Level 2 merchants*—must complete an annual SAQ. Level 2 merchants completing SAQ A, SAQ A-EP or SAQ D must additionally engage a PCI SSC-approved QSA or PCI SSC-approved ISA for compliance validation. Level 2 merchants may alternatively, at their own discretion, engage a PCI SSC-approved QSA or PCI SSC-certified ISA to complete a ROC.
- *Level 3 merchants*—must complete an annual SAQ or alternatively, at their own discretion, engage a PCI SSC-approved QSA to complete a ROC
- *Level 4 merchants*—may complete an annual SAQ or alternatively, at their own discretion, engage a PCI SSC-approved QSA to complete a ROC. Note—validation of compliance to Mastercard is **optional** for Level 4 merchants.

Mastercard does not accept PCI DSS validation documentation sent by a merchant. It is your acquirer who will manage your PCI DSS compliance and report your status directly to Mastercard.

**Q: I am a service provider. What do I need to do to meet SDP Program requirements?**

Mastercard requires registered Level 1 and Level 2 service providers to comply with the PCI DSS and all other applicable PCI Security Standards as follows:

- A Level 1 service provider is any Third Party Processor (TPP), Staged Digital Wallet Operator (SDWO), Digital Activity Service Provider (DASP), Token Service Provider (TSP), AML/Sanctions Service Provider or 3-D Secure Service Provider (3-DSSP) (regardless of volume); and any Data Storage Entity (DSE) or Payment Facilitator (PF) that stores, transmits, or processes more than 300,000 total combined Mastercard and Maestro

Transactions annually. Level 1 service providers must validate compliance with the PCI DSS, TSPs must additionally validate compliance with the *PCI TSP Security Requirements* and 3-DSSPs must validate compliance with the *PCI 3DS Core Security Standard* by successfully undergoing an annual PCI assessment resulting in the completion of a ROC conducted by an appropriate PCI SSC-approved QSA.

- A Level 2 service provider is any DSE or PF that stores, transmits, or processes 300,000 or less total combined Mastercard and Maestro Transactions annually; and any Terminal Servicer (TS). Level 2 service providers must validate compliance with the PCI DSS by successfully completing an annual SAQ.
  - As an alternative to validating compliance with an annual SAQ, a qualifying Level 2 DSE may submit a *PCI PIN Security Requirements* AOC from a PCI SSC-approved Qualified PIN Assessor (QPA) every two years.
  - As an alternative to validating compliance with an annual SAQ a TS, if eligible, may submit a completed *Terminal Servicer QIR Participation Validation Form*.

The service provider's PCI AOC must be submitted to pcireports@mastercard.com after initial registration with Mastercard and every year thereafter. If a newly registered service provider is not yet compliant, the *PCI Action Plan* available on the service provider page of the SDP Program website must be completed and submitted for review.

Level 1 and Level 2 service provider classifications are determined by the Mastercard Service Provider Registration Team.

### Q: How can I be listed on *The Mastercard SDP Compliant Registered Service Provider List*?

To be listed on *The Mastercard SDP Compliant Registered Service Provider List* updated monthly on the Service Provider page of the SDP Program website, a service provider must have submitted to pcireports@mastercard.com a copy of their PCI DSS AOC by a PCI SSC-approved QSA reflecting validation of compliance and been registered as a service provider by one or more Mastercard customers.

Note—only registered service providers that validate compliance with an annual PCI DSS assessment resulting in the completion of a ROC conducted by a PCI SSC-approved QSA will be listed on *The Mastercard SDP Compliant Registered Service Provider List*. A registered service provider that validates compliance with a PCI Security Standard other than the PCI DSS (such as the *PCI PIN Security Requirements*) will not be listed on *The Mastercard SDP Compliant Registered Service Provider List*.

### Q: What is the Mastercard Cybersecurity Incentive Program (CSIP) for merchants?

The Mastercard Cybersecurity Incentive Program (CSIP) provides eligible merchants using secure technologies such as EMV chip, PCI point-to-point encryption (P2PE) solutions, and EMV Payment Tokenization increased flexibility within the SDP Standards. The CSIP is a component of the SDP Program and is optional for merchants. The CSIP incentivizes merchant participation by either reducing PCI compliance validation requirements through the *Mastercard PCI DSS Risk-based*

*Approach* or by eliminating the requirement to annually validate compliance with the PCI DSS through the *Mastercard PCI DSS Validation Exemption Program*.

**Q: Where can I find eligibility requirements for the *PCI DSS Risk-based Approach* and *PCI DSS Validation Exemption Program*?**

Eligibility requirements for the *PCI DSS Risk-based Approach* and *PCI DSS Validation Exemption Program* can be found in section 2.2.4 Mastercard Cybersecurity Incentive Program (CSIP) in the *Security Rules and Procedures*.

**Q: What is Mastercard's ISA mandate for Level 1 merchants?**

Mastercard requires that Level 1 merchants successfully complete their annual PCI DSS compliance validation requirements using a PCI SSC-approved QSA or PCI SSC-approved ISA. ISA sponsor companies are organizations that have been qualified by the PCI SSC.

**Q: What is Mastercard's mandate for merchants and service providers that use eligible third party-provided payment applications or payment software?**

Mastercard requires all merchants and service providers that use third party-provided payment applications or payment software to only use payment applications or payment software listed on the PCI SSC website at www.pcisecuritystandards.org as compliant with either the *Payment Card Industry Payment Application Data Security Standard* or the *Payment Card Industry Secure Software Standard*, as applicable.

Mastercard also recommends that merchants and service providers using third party-provided payment software ensure the payment software vendor complies with the *Payment Card Industry Secure Software Lifecycle Standard*.

**Q: Are there fines for entities that are noncompliant with the SDP Program?**

Yes. A merchant or service provider that is noncompliant with the SDP Program could be affected by potential SDP noncompliance assessments. Table 2.2—Assessments for Noncompliance with the SDP Program of the *Security Rules and Procedures* details escalating fines for merchants and service providers that are noncompliant with the SDP Program.

**Q: Where can I find Mastercard SDP Standards?**

Mastercard SDP Standards can be found in section 2.2 Mastercard Site Data Protection (SDP) Program of the *Security Rules and Procedures* on Mastercard Connect™.

Customers, merchants and service providers with questions about SDP Program requirements should contact the SDP Team at sdp@mastercard.com.

# Card Production Security Standards

*The following list of questions is designed to assist issuers and card production vendors with Card Production Security Standards compliance requirements.*

**Q: What do card production activities consist of?**

Card production activities consist of card manufacture services, card personalization services, and other specialized services performed in connection with card production. This includes the treatment and safeguarding of cards, printing, embossing, encoding and mailing as well as any phase of the production and distribution of cards or card account information.

**Q: Who is required to ensure that all card production activities are performed in compliance with Card Production Security Standards and Card Design Standards?**

Issuers and card production vendors must ensure that all card production activities are performed in compliance with Card Production Security Standards and Card Design Standards, as applicable. The physical, logical, and mobile provisioning security requirements set forth in the PCI Card Production Logical and Physical Security Requirements can be found on the PCI SSC website at www.pcisecuritystandards.org/document_library and the Card Design Standards manual is available on Mastercard Connect™.

**Q: What is the Mastercard Global Vendor Certification Program (GVCP)?**

The Mastercard GVCP defines and enforces security requirements that provide a high-security environment within which third party vendors perform card manufacture, personalization and provisioning services on behalf of Mastercard issuers.

**Q: What is GVCP certification?**

GVCP certification indicates that a vendor has demonstrated compliance with the PCI Card Production & Provisioning Physical & Logical Security Requirements and is authorized to provide card production services to Mastercard issuers. Mastercard GVCP Standards require issuers that outsource their card production activities to only utilize GVCP certified vendors.

**Q: What entities require GVCP certification?**

Vendors that perform card production activities for Mastercard issuers (such as card manufacturing, personalization, provisioning and specialized production services) require GVCP certification. Issuers that perform card production activities for themselves or their affiliate members are not subject to GVCP certification.

**Q: What PCI Security Standards apply to GVCP certification?**

The PCI Card Production & Provisioning Physical Security Requirements and the PCI Card Production & Provisioning Logical Security Requirements apply to GVCP certification. These security requirements are separate documents and can be found at www.pcisecuritystandards.org/document_library.

**Q: How do I begin the GVCP certification process?**

To begin the GVCP certification process, vendors should send an email to gvcp-helpdesk@mastercard.com that includes their company name, facility location, service(s) to be provided and their contact information.

**Q: What are the key milestones for GVCP certification?**

The key milestones for GVCP certification include:

- forms completion
- program fees (contact gvcp-helpdesk@mastercard.com for associated fees)
- compliance assessment
- audit finding, reporting and remediation
- certification
- annual certification renewal

**Q: How long does it take a vendor to achieve GVCP certification?**

The length of time required to achieve GVCP certification may vary from vendor to vendor. The duration is influenced by the maturity of the vendor's security environment and ability to complete essential milestones in a timely manner.

**Q: After GVCP certification is achieved, how does a vendor maintain their certification?**

To maintain GVCP certification, a vendor must complete their renewal certification requirements annually.

**Q: How do I determine if an auditor is qualified to assess card production security?**

Card production security assessments must be performed by a PCI SSC-approved Card Production Security Assessor (CPSA). A list of CPSA security organizations can be found on the PCI SSC website at www.pcisecuritystandards.org/assessors_and_solutions/card_production_security_assessors.

**Q: How can I validate that a card production facility is GVCP certified?**

To validate whether a card production facility is GVCP certified, Mastercard AN1157—List of Certified Vendors is published monthly and confirms that vendors are certified for card production services they provide. The List of Certified Vendors is available on the Technical Resource Center on Mastercard Connect™.

**Q: Where can I find additional information about GVCP?**

Mastercard GVCP Standards can be found in section 2.3 Card Production Security Standards of the *Security Rules and Procedures* on Mastercard Connect™. In addition, the GVCP policies and procedures published in the *Card Vendor Certification Standards* manual can also be found on Mastercard Connect™.

Issuers and vendors with questions about Card Production Security Standards should contact gvcp-helpdesk@mastercard.com.