AMERICAN EXPRESS
Annual Security Technology Enhancement Program (STEP)

Frequently Asked Questions

What is the Security Technology Enhancement Program or STEP?

Security Technology Enhancement Program (STEP) is a way that American Express recognizes the investments Merchants make in improving the security of Cardholder Data and Sensitive Authentication Data.

Merchants that qualify for STEP are required only to submit a simplified one-page annual attestation. In addition, STEP-qualified Merchants are no longer required to submit quarterly vulnerability scan results.

Do I qualify for STEP?

To qualify for Security Technology Enhancement Program (STEP) there are several qualifications to which you must attest.

- Current compliance with the Payment Card Industry Data Security Standard (PCI DSS)
- No Data Incidents in the previous 12 months
- At least 75% of your American Express Card transactions occur:
  - Through EMV-compliant terminals, OR
  - Using a PCI-listed Point-to-Point Encryption solution (which appears on the PCI Security Standards Council website (www.pcisecuritystandards.org), OR
  - Using a Point-to-Point Encryption solution that is approved by a Qualified Security Assessor (QSA)

Must I still comply with the PCI DSS?

Yes. Compliance with the PCI DSS is required to qualify for STEP.

What is Point-to-Point Encryption (P2PE)?

A point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a Merchant accepts the payment card to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach.

How does STEP compare with the current PCI validation program?

The Security Technology Enhancement Program (STEP) reduces the number and complexity of PCI DSS validation documents required by American Express

Merchant Level (Annual Amex Transactions)	Required documentation before STEP availability	STEP documentation requirement
Level 1 (>2.5 million) Level 2 (50k to 2.5 million) Level 3 (<50k >10K) Level 4 (<10K)	Annual PCI Assessment (ROC or SAQ) External Network Vulnerability Scan, if applicable for your business	Annual STEP Attestation Form

How do I submit my application for STEP eligibility?

If you are already required to submit PCI Validation Documentation to American Express, you have an account established with the SecureTrust portal.

- Log into SecureTrust™ PCI Manager. Go to the Documents page. Download the annual STEP Attestation document from the Program Documents folder.
- Complete all sections of the form.
- Log back into SecureTrust™ PCI Manager. Upload your completed annual STEP Attestation form.

I am eligible for STEP. Am I required to participate?

No. Even though a Merchant has adopted Point-to-Point Encryption (P2PE) or EMV in its systems, there is no requirement to adopt the STEP Attestation as their annual validation documentation.

How does STEP compare with other validation relief programs?

The American Express Security Technology Enhancement Program (STEP) makes it easier for Merchants to validate their PCI compliance, which is a requirement by all U.S. card brands. Merchants who are eligible for STEP have significantly reduced PCI assessment requirements. Other card brands also offer PCI validation reduction/relief in some cases.

Information current as of February, 2017

Merchant has deployed to at least 75% of its transactions:	American Express	Visa	Mastercard
EMV	Yes	Yes	Yes
PCI-approved P2PE	Yes	Yes	Yes
QSA-approved P2PE	Yes	No	No

What if American Express requires different PCI validation documentation than other card brands?

Merchants are not required to participate in the American Express Security Technology Enhancement Program.

If you are still required to submit an annual Report on Compliance (ROC) or Self Assessment Questionnaire (SAQ) to another card brand, the American Express PCI Compliance Program will also accept those same documents.

Please note that Merchants submitting an SAQ (and not the STEP Attestation) may also be required to submit quarterly vulnerability scan results as well, if applicable for their card payment environment.

What are the benefits if I qualify for STEP?

Merchants that qualify for STEP:

- Submit only an annual STEP Attestation form as their annual PCI validation documentation
- Will not be required to submit any other annual PCI document (ROC or SAQ) or a quarterly vulnerability scans

What is EMV?

EMV means an integrated circuit card (sometimes called an "IC Card," "chip card," "smart card," "EMV card," or "ICC"). It is based on a standard called "Europay, Mastercard, Visa" which is managed by EMVCo (www.emvco.com).

What is PCI-Approved P2PE?

The Payment Card Industry Security Standards Council (PCI SSC) has established technical criteria and publishes a list of P2PE solutions that have successful completed the validation testing. The list of compliant solutions is listed on the PCI web site (www.pcisecuritystandards.org).

What is QSA-Approved P2PE?

In some cases, a Merchant may have installed an effective Point-to-Point Encryption (P2PE) Solution that has not yet been approved by PCI SSC. In this case, a Qualified Security Assessor (QSA) who has been trained by Payment Card Industry Security Standards Council (PCI SSC) may validate and approve that the P2PE solution installed in the Merchant's systems meets the intent of the PCI SSC Point to Point Encryption requirements.

What are the STEP requirements for Merchants who are using EMV terminals?

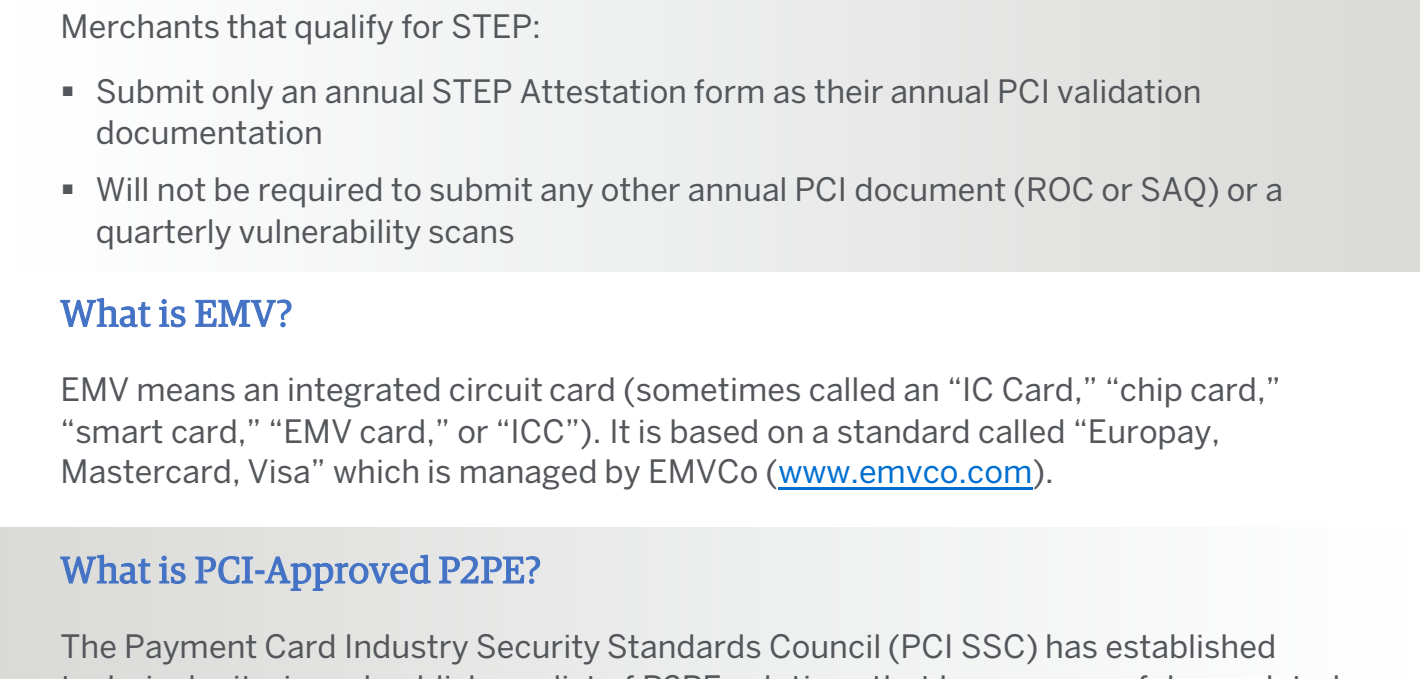
At least 75% of the Merchant's total American Express Card transaction count are made with the physical Card present and originate from EMV Chip-Enabled Devices capable of processing American Express EMV transactions.

Are Service Providers or Payment Processors eligible for STEP?

No. Only Merchants are eligible for the American Express Security Technology Enhancement Program.

What if I have additional questions or need help?

Contact SecureTrust using the contact information below.



americanexpresscompliance@securetrust.com
+1-312-267-3208

DON'T *do business* WITHOUT IT™