DISCOVER NETWORK

Discover® Information Security & Compliance (DISC) Program

Merchant Security Compliance Innovation Program (SCIP) Application

Security Compliance Innovation Program (SCIP) Eligibility

Discover® Network merchants that are currently PCI Data Security Standard (PCI-DSS) compliant and that attest to the criteria noted below are qualified to apply for DISC PCI Data Security Standard (DSS) reporting relief. Once received, a DISC team member will review the SCIP Application and respond accordingly with a decision regarding acceptance or further questions. Merchants that are acquired by an entity outside of Discover Network (acquired merchants) should consult with their direct Acquirer to determine their candidacy for this program.

Instructions for Submission

The Discover Network merchant must complete each of the below sections and submit this application to the Discover Network Data Security team at DISCCompliance@discover.com.

1 Merchant Information

*all fields required

Merchant Name _____

Doing Business As _____

Merchant Level (select one):

◉ Level 1 ○ Level 2 ○ Level 3

2 Merchant Attestation

We, the merchant (named above), attest to the following:

○ Merchant has documented and annually tested Data Security Breach incident response program in accordance with the Payment Card Industry Data Security Standard (PCI-DSS) requirements.

○ And merchant has not been involved in a Data Security Breach in the past 12 months.

○ And merchant is not storing Sensitive Authentication Data (i.e., full contents of magnetic stripe, CVV2, CID or PIN data) on any system subsequent to transaction authorization.

- ☐ And merchant has met at least 75% of the merchant's transactions originated from using the security technologies of one or more of the following criteria:
  - ☐ Merchant's transactions originated from Chip Card Terminals* enabled to accept Chip Card Transactions (including, without limitation, Discover® D-PAS transactions).
    *Chip Card Terminals must have current, valid EMV approval and Discover D- PAS Certification.
  - ☐ Point-to-Point Encryption (P2PE): Implemented a PCI Security Standard Council (PCI SSC) approved P2PE solution listed on the PCI SSC website or independently validated by a PCI SSC Qualified Point-to-Point Encryption Assessor Company.
  - ☐ Tokenization: All tokenization solutions must comply with EMVCo Specifications. Additionally, tokens must not be reversible to reveal unmasked Primary Account Numbers (PANs) to the merchant.

3 Data Security Contact

Merchant must complete the information below designating a primary contact for any Data Security matters.

*all fields required

Name _____ Title _____

Email Address _____ Telephone _____

4 Authorized Approval

This form must be signed by an individual with signatory authority at the merchant. I attest the information above is accurate and acknowledge that the merchant must maintain compliance with PCI DSS at all times.

*all fields required

Print Name _____ Title _____

Email Address _____ Telephone _____

Official Authorized Signature _____ Date _____

Acceptance of this form by Discover Network provides the merchant reporting relief for the annual PCI DSS validation requirement. However, all merchants are required to maintain compliance with PCI DSS at all times. In the event of a Data Security Breach, merchant may be responsible for fraud losses and damages. Discover Network maintains the right to require full PCI DSS compliance validation documentation upon request.

Confidential and Proprietary | © 2026 DFS Services LLC