SecureTrust
a Trustwave division

Service Description

Merchant Compliance Validation & Security Service

Contents

Merchant Compliance Validation & Security Service (CVS4 / L4) 3

SERVICE DESCRIPTION 3
BASE TIER 3 SERVICE FEATURES 3
Technology (Tier 3) 3
Services (Tier 3) 4
ESSENTIALS TIER 2 SERVICE FEATURES 5
Technology (Tier 2) 5
Services (Tier 2) 5
PREMIUM TIER 1 SERVICE FEATURES 7
Technology (Tier 1) 7
Services (Tier 1) 7
DELIVERY AND OPERATIONS 8
Operations and Support Services 8
Localization 9
OPTIONAL ADD-ONS 10
Technology (Add-On) 10
Services (Add-On) 11

Merchant Compliance Validation & Security Service (CVS4 / L4)

SecureTrust™ is a division of Trustwave Holdings, Inc.

“Partner” refers to program sponsor, client of SecureTrust.

“Merchant” refers to end-user of compliance validation service.

How to use this document: features organized by service tier, starting with Tier 3. Subsequent tiers build upon previous tier (unless otherwise noted). Refer to your account manager or master service agreement for details on any custom offerings.

SERVICE DESCRIPTION

Merchant Compliance Validation & Security Service is powered by SecureTrust’s PCI Manager product and accompanying services. PCI Manager provides an industry-leading compliance validation service that helps merchants of all sizes achieve and maintain compliance. It simplifies the self-assessment process for merchants by presenting a pathway customized to their business type. SecureTrust’s intelligent PCI Wizard walks the merchant step-by-step through the entire process of validating compliance, including the ability to complete the PCI Self-Assessment Questionnaire (SAQ) that’s most appropriate for their business type, and generate their certification documents. Vulnerability scanning by a PCI Approved Scanning Vendor (ASV) may be included and integrated into the overall merchant experience. Program administrators also receive access to PCI Sponsor View, powered by PCI Manager. PCI Sponsor View provides the ability to track and manage the merchant portfolio, query and download reports and view merchant details.

Based on the contracted tier, the solution may include additional products and services like dedicated program management, marketing resources, strategic planning guidance, security tools and an integrated cloud platform.

BASE TIER 3 SERVICE FEATURES

SecureTrust’s Merchant Compliance Validation & Security Service includes a combination of technology products and managed services, including but not limited to the following features. Unless noted, English is the default support language.

Technology (Tier 3)

TrustKeeper® cloud-based portal

PCI Manager Merchant View with Wizard and Self-Assessment Questionnaire (SAQ): PCI Manager Merchant View allows merchants to work on their compliance validation by completing the right PCI self-assessment questionnaire (SAQ). The included smart PCI Wizard makes the process easier, guiding the merchant step-by-step by asking simpler profiling questions and automatically determining and completing the right SAQ type, where applicable.

- **SAQ Express Renewal:** Annual re-assessments are made easier for eligible merchants by providing an automatically generated new SAQ based on previously compliant form.
- **Vulnerability Scan Management:** For those merchants required to perform external vulnerability scanning of their card-processing environment, the scan engine is integrated into the process. An easy-to-use interface facilitates scan set up, maintenance, scan results and dispute management. Trustwave is a PCI-listed Approved Scanning Vendor (ASV).
- **Security Policy Advisor:** All users have access to a library of security policy templates designed to comply with PCI DSS. This feature helps merchants certify specific PCI requirements around

documented procedures, including those related to Requirement 12.x. Available in supported languages.

- **Security Awareness Training:** PCI Manager's integrated self-guided educational courses break down each step of the compliance process and help merchants meet PCI compliance requirements related to education and training. Security Awareness Training consists of online modules that are available for a variety of businesses and employee roles. Available in English only by default.
- **Trusted Commerce Seal and Certification:** Compliant merchants may display the Trusted Commerce site seal on their website to reflect their validation against PCI DSS. This integrated seal may also confirm the merchant's digital server certificate (SSL), if using SecureTrust certificates. Printable PDFs of the Certificate of Compliance and the PCI Attestation of Compliance (AoC) are also available.

PCI Manager Sponsor View (for Program Administrators)

PCI Manager Sponsor View, powered by PCI Manager, is the program administrators' tool to see an aggregate snapshot of their merchant compliance program, providing information on merchant milestones, such as progress made toward the program's objectives and compliance status by merchant type. Sponsor View provides the ability to track and drill into account specifics, like PCI details and compliance history, as well as filter and sort groups of accounts to facilitate reporting and other purposes. Role-based access is supported to serve the needs of different administrator user types, including read-only and managers. Standard pre-formatted program reports are automatically generated every month and made available for download through the cloud platform, providing current compliance insights and other valuable metrics. By default, PCI Manager Sponsor View includes:

- Cloud-based administrator's dashboard powered by PCI Manager.
- Role-based access with six (6) user roles included.
- Ability to track and manage portfolio including bulk operations, view account details, manage administrator users, view and download portfolio reports, and view support issues (if applicable).
- Set of account service email notification templates for program.

Services (Tier 3)

Marketing services are included with SecureTrust's Merchant Compliance Validation & Security service including:

Automated Account Service Email Templates: Powered by PCI Manager, a library of service email notification templates is included by default. These service emails include account registration, SAQ submission, expiry and vulnerability scanning notifications.

Co-branded Splash/Landing Page (optional): Powered by PCI Manager, SecureTrust may host a co-branded landing page that guides merchants towards registration.

ESSENTIALS TIER 2 SERVICE FEATURES

Unless otherwise noted, default Essentials Tier 2 includes all features from Base Tier 3 service plus the following:

Technology (Tier 2)

Endpoint Protection Suite (desktop and mobile software): *A sample summary of the features are provided here for convenience; see Endpoint Protection Suite Service Description for full details, terms and conditions.* SecureTrust Endpoint Protection is a powerful security solution that delivers integrated core endpoint protection functions to help merchants simplify security and compliance management. The integrated software solution lowers security operational costs for greater adoption and optimal defense-in-depth against the full threat spectrum. Note that offering limits, and terms and conditions may apply. Modules bundled with SecureTrust Endpoint Protection software include (availability depends on program offering):

Tier 2

- IP Beacon: Helps automatically detect the public IP address to facilitate external vulnerability scanning integration with the cloud-based portal.
- Security Health Check: Helps monitor endpoint essential security settings.
- Security Configuration Monitoring: Helps discover policy and security configuration weaknesses.
- Credit Card Data Storage Monitoring (DLP): Helps discover prohibited cardholder data on endpoints.

PCI Fast Track Validation (optional): Fast Track Validation can pre-populate portions of the SAQ based on key pieces of information known about a merchant. This may be layered on top of the PCI Wizard to shorten the overall assessment process for the merchant. Fast Tracks may be linked to several types of information:

- Payment Applications and other POS equipment (i.e., Payment Product).
- Service Provider(s) used by the merchant.
- Program (sponsor and sub-sponsors) to which the merchant belongs (e.g., a franchise or affiliate program).

If multiple Fast Tracks apply, they will be layered over the SAQ to pre-fill the combined requirements to reduce the time the merchant needs to spend answering questions. Merchant remains responsible for meeting any remaining PCI requirements and questions. Certain constraints and limitations apply. **Partner must provide SecureTrust with written approval for use in the merchant program, including but not limited to acknowledgement of any associated liability and releasing SecureTrust of any damages.**

PCI Sponsor Automation Data Feed (optional): Automate boarding and/or reporting of portfolio accounts into the system. Program account management automation, enabling Partner to enroll and load accounts into the system, close and reopen accounts, and receive account data out of the system. Automation is performed over data file exchange on SecureTrust-support file types only. Automation scheduling options include: daily, weekly, monthly. Unless otherwise agreed, only one (1) instance of each automation is included. Technical specifications will be provided by SecureTrust.

Services (Tier 2)

Automated Account Service Email Template Customizations: Email notification templates may be customized to include Partner logo, name and support contact information. Customization of content must be submitted and approved by SecureTrust before production release. Non-English custom content may be localized upon request and approval by SecureTrust, and additional fees may apply.

Merchant Virtual Training: Virtual training sessions such as informational webinars conducted over SecureTrust training platform. By default, training content is designed for small-medium-business audiences with a focus on PCI DSS compliance, validation and related security topics. Training content may be catered to the Partner's merchants upon agreement. By default, one (1) training session is included each calendar year. Scheduling of training requires sixty (60) days' advance notice and may be longer in cases with customized content. SecureTrust will select and provide a Trainer. Session may be recorded upon request.

PREMIUM TIER 1 SERVICE FEATURES

Unless otherwise noted, default Premium Tier 1 includes all features in the Essentials Tier 2 service plus the following:

Technology (Tier 1)

Endpoint Protection Suite (desktop and mobile software):

Tier 1

- *All features in Tier 2.*
- Unauthorized Device Monitoring: Helps discover rogue devices on the local network.
- File Integrity Monitoring (FIM): Helps detect unexpected or malicious changes to critical files, directories and registry settings.
- Anti-virus (AV): Helps prevent, detect and remove malicious computer viruses.
- Remote Access Security: Helps detect insecure remote access and provide guidance on remediation.
- Mobile Device Security (iOS & Android): Provides security checks including alert of tampering with applications or device to aid in improving overall security. Helps deliver proactive protection and defense against malware and other threats (Android-only).

Security Policy Generator: This feature makes the process to comply with all the sub-requirements in PCI DSS requirement 12 easier by automatically generated the right template for the merchant and filling in their key information like company name and officer's title, so that a ready-to-use document may be downloaded with one click. This tool will also automatically pre-fill the merchant's questionnaire, specifically those in 12.x. Merchant must review SAQ before final submission.

Point-of-Sale Inventory Review: This online portal tool facilitates a merchant's ongoing compliance to PCI DSS requirement 9.9 by making it easier to maintain and track their point of sale and hardware inventory. Inspection reminder email notifications are included.

Merchant Web Malware Monitor: Service to help reduce business risk and increase e-commerce conversions through ongoing monitoring of potential security and reputational issues on the website. This service monitors for malware, search engine blacklists, domain registration hijack attempts, website platform issues and website certificate validity issues. Powered by SecureTrust's Web Risk Monitoring technology.

Services (Tier 1)

Online Chat: Provides additional convenient method for accessing the customer support team during supported hours. Integrated portal online chat powered by the SecureTrust Customer Support team. Available in English only by default. Online chat does not support branding.

Managed Marketing Service: SecureTrust will provide partner with a managed marketing service including but not limited to program launch materials such as emails, letter and postcard samples, and statement messages samples. In addition to the initial program launch, SecureTrust will run one (1) email activation campaign once per year for the term of the contract.

DELIVERY AND OPERATIONS

Program/Project Management: SecureTrust will provide guidance to support the launch of the program. A SecureTrust resource will be assigned to the program to help ensure its success in meeting defined program goals and objectives. Responsibilities may include but are not limited to pre-launch activities, coordination between organizations and teams, resource allocation and escalations, establishing standard operations procedures and ongoing program monitoring. Deliverables includes establishing a standard operating procedure document (also known as Operations Guide) that defines mutually-agreed roles and responsibilities for the Partner and SecureTrust. Service available in English only by default.

Administrators Success Training: Customer success resources dedicated to help ensure program success. Service provided to the Partner administrators for product training, launch strategy planning and guidance, best practices for maintaining a compliance program and PCI DSS training, if needed. Conducted over virtual meetings, recordings and published guides. Available in English only by default.

Operations and Support Services

Telephone and Email Customer Support: The support team consists of support analysts, team leaders, supervisors, managers, quality assurance and a work force management team to ensure that correct, consistent and timely support is provided to both our merchants and Partners. Locations[1] of global SOC and Support Centers include but are not limited to Chicago, Denver, Manila, and Warsaw. The operations management team are active participants in ongoing Partner calls and are engaged to help ensure merchant needs are met and issues are solved quickly. Generally, the support organization handles all program and PCI questions except Partner-established deadlines, fees, fines and Partner billing questions. Standard customer support is accessed by telephone and/or email. Standard customer support categories include the following:

- General questions
- PCI compliance and reporting process
- Wizard & SAQ support
- Vulnerability scan support
- Portal navigation support
- Merchant boarding questions
- PCI compliance and reporting escalations
- Portal support escalations
- Endpoint Protection support escalations
- Vulnerability scan finding disputes

Standard support service level:

- Telephone (English): 24 hours / 7 days per week.
- Email (English): 24 hours / 7 days per week

[1] SecureTrust reserves the right to appropriately utilize its resources as needed in its sole judgment.

Localization

Summary of the general language capabilities based on key areas of the program, including the technology product and the services:

- PCI Manager Merchant View: Default PCI Language Set[2]
- PCI Manager Merchant Standard Account Service Email Templates: Default PCI Language Set
- Endpoint Protection software: Endpoint Language Set[3]
- Security Awareness Training online courses (embedded): Default PCI SAE Language Set[4]
- Co-branded Splash/Landing Page: English[5]
- PCI Manager Sponsor View: English
- PCI Manager Vulnerability Scan Report and Disputes: English
- PCI Manager Merchant Add-on Emails (optional): English
- Customer Support: *See Customer Support section*
- Web Risk Monitoring (optional): *See Web Risk Monitoring service description*

[2] "**Default PCI Language Set**" is defined as:

- English (US), English (UK), Spanish, French, French (Canada), German, Polish, Swedish, Chinese (Traditional), Chinese (Simplified), Japanese, Portuguese, Dutch, Norwegian, Danish, Finnish, Icelandic. – 17 total languages. *SecureTrust reserves the right to make changes without notification.*

[3] "**Default Endpoint Language Set**" is defined as:

- English (US), Spanish, French, French (Canada), German, Polish, Greek, Japanese, Korean. – 9 total languages. *SecureTrust reserves the right to make changes without notification.*

[4] "**Default PCI SAE Language Set**" is defined as:

- English (US), Spanish, French – 3 total languages. *SecureTrust reserves the right to make changes without notification.*

[5] Other languages must submit change request, additional fee may apply. Terms and conditions apply.

OPTIONAL ADD-ONS

Technology (Add-On)

Digital Certificates: For merchants that need to secure e-commerce transactions or secure communications over the Internet, SecureTrust Digital Certificates (SSL) are available as an add-on to the program. Three (3) types of server certificates are available: Domain Validation (DV), Organization Validation (OV) or Extended Validation (EV). Additionally, code-signing, email (S/MIME), MyIdentity™ VPN and private CA certificates are available. SecureTrust is a globally recognized certificate authority (CA).

Enterprise Security Awareness Education: Users may upgrade to Enterprise Security Awareness Education (SAE) to teach employees the importance of protecting cardholder data and other sensitive information, with role-specific courses and real-time tracking and training completion reports, powered by Trustwave's enterprise learning management system.

Enterprise Vulnerability Scan Management: Enterprise-class vulnerability scanning and management solution powered by Trustwave provides more sophisticated scanning services for merchants that need to scan a large number of IP addresses or additional management capabilities. Merchants will receive enhanced scanning and reporting on additional IP addresses.

Managed Firewalls and Drop-Ship Firewalls: Network protection is one of the top deficiencies found in merchants that suffer data breaches, and is a requirement to become PCI-compliant. Several options are available for merchants – both managed by Trustwave and drop-ship devices. (If interested, please consult your account manager for additional details)

Portal Single Sign-On (SSO): The portal supports SSO via SAML 2.0 protocol and allows the end user to seamlessly access the portal from the Partner's portal without additional authentication. SSO interaction requires that SecureTrust (defined as the Service Provider) and the Partner (defined as the Identity Provider) make arrangements as to how the two parties will communicate. The Partner is responsible for making necessary updates to their portal with a click through link that allows access to the SecureTrust portal via SSO. End-to-end integration testing service is included and concludes with a production release of the SSO feature. Maintenance of the integration is included for the duration of the agreement. Requirements and specification will be provided upon execution of agreement. Merchant must review SAQ before final submission. Partner is responsible for creating, hosting and maintaining ancillary or exception landing pages (e.g. Error, redirect). Certain constraints and limitations may apply.

Web Risk Monitoring Merchant Category Code (MCC) Matching: *A sample summary of the features are provided here for convenience; see Web Risk Monitoring Service Description for full details, terms and conditions.* MCC Matching is a service to help confirm the accuracy of a merchant's previously assigned MCC. MCC Matching may also be used to initially define a merchant's appropriate MCC at the time the service is performed by SecureTrust.

Web Risk Monitoring (WRM) for Administrators: *A sample summary of the features are provided here for convenience; see Web Risk Monitoring Service Description for full details, terms and conditions.* The WRM solution offers acquirers and independent sales organizations a full suite of protection for monitoring and reducing risk, to help reduce costs and increase revenues. It helps efficiently satisfy card brand monitoring requirements, detect merchant violations, and reduce risks. WRM makes it easy to deliver additional services, such as web malware monitoring, which add value to merchant programs. The WRM process is managed through the secure cloud-based portal, setting parameters for the identification of questionable and illegal content and malware scanning.

Web Risk Monitoring (WRM) Merchant Discovery: *A sample summary of the features are provided here for convenience; see Web Risk Monitoring Service Description for full details, terms and conditions.* Service where SecureTrust attempts, on a best-effort basis, to determine the website domain names of merchants based on other readily-available business contact information provided by Partner.

Services (Add-On)

Automated Account Service Email Template Customizations: Refer to Tier 2 services section.

Custom Development: Development limited to Marketing or Product. Contact Account Manager.

Customer Support Additional Languages: Contact Account Manager.

Managed Marketing Service: Refer to Tier 1 services section.

Merchant Breach Coverage: See service description on Trustwave.com or contact Account Manager.

Merchant Concierge Service: See service description on Trustwave.com or contact Account Manager.

Merchant Website Identity Risk Report: Provides insight into merchant risk by providing a report of their website digital certificate status. Unless otherwise agreed, one-time scoped service to scan and report inventory of the merchant portfolio's deployed digital certificates (SSL) for those with a public domain name.

Online Chat: Provides an additional convenient method for accessing the customer support team during supported hours. Integrated portal online chat powered by the SecureTrust Customer Support team. Available in English only by default. Online chat does not support branding. Contact Account Manager.

PCI Manager Branding: PCI Manager supports the ability to be co-branded or “white-labeled”, matching the look and feel for the end user merchant to the Partner’s requirements. Service must have SecureTrust approval for scope, development schedule and launch of branding package. Branding package includes the following:

- One (1) Partner logo as the primary image for the branded portal.
- One (1) Domain Name URL may be utilized for branded portal (optional). Requires advance notice.
- Only Trustwave portal components that currently support branding may be customized. In other words, only supported fields and labels may use customized color scheme.
- Support helpdesk Email inbox may utilize one (1) custom email domain name.
- PCI Certificate of Compliance may utilize custom branding profile.
- Only standard service email templates may utilize custom branding. Requires advance notice.
- Integration testing service is included and concludes with production release of the branding package.
- Certain areas CANNOT be branded due to legal or other regulatory reasons (e.g., Trustwave is the PCI approved scanning vendor).
- Other conditions and limitations may apply.

Note: Support helpdesk custom phone line is NOT included by default; requires add-on and advance notice.