SecureTrust Service Description

Web Risk Monitoring

Web Risk Monitoring (WRM)

SERVICE DESCRIPTION

The SecureTrust WRM solution ("WRM") offers acquirers and independent sales organizations a full suite of protection for monitoring and reducing risk, to help reduce costs and increase revenues. WRM supports compliance with card brand monitoring requirements, detects merchant violations, reduces risks, and simplifies the delivery of additional services (e.g. web malware monitoring, which adds value to merchant programs). The WRM process is managed through the SecureTrust web portal (the "Portal"). SecureTrust will set the parameters for the identification of questionable and illegal content and malware scanning.

BASE SERVICE FEATURES

Clients can purchase each of the WRM features described below separately or in a bundle.

WRM Overview

Analysis

WRM analyzes e-commerce websites (provided by SecureTrust's partners as URLs) by applying SecureTrust's patented automated content-analysis techniques, which reviews standard categories identified as being critical to risk management and brand protection programs. SecureTrust's Web Risk Analysis Team (each member shall be referred to herein as an "Analyst") utilizes the WRM Analyst Workstation, a data and evidence collection platform, to review all websites identified by the automated analysis system as potentially violating card brand rules or Client Terms of Service, including the content and links of such websites. This analysis process provides a multi-tier workflow, in which an Analyst may escalate a finding to a Senior Analyst for review. All suspected website findings are reviewed by a Senior Analyst prior to being reported to the Client. This process produces more thorough results and reduces false positive cases.

WRM also performs automated website security analysis using industry leading vulnerability and security scanning systems.

Reporting and Data Access

All WRM components produce data that is available either in reports or through the online data explorers in the Client's Portal account. These reports and data are intended to provide a detailed look into a specific merchant or trends affecting the merchant portfolio.

WRM allows automated reporting to card brand protection programs such as the MasterCard MMP. The MasterCard MMP Reporting Tool allows Client to review an automatically generated report that meets MasterCard's specification within the Portal, send the report on-demand, or enlist the tool to automatically send the report securely to MasterCard on a monthly basis. This tool is designed to allow the Client a simple and effective way to meet MasterCard MMP's requirements after Client has registered SecureTrust as Client's Merchant Monitoring Service Provider (MMSP) per MasterCard MMP program requirements.

Portal Access

WRM provides a modern, user-friendly Portal which provides access for Client's users. The information available includes a top-level summary dashboard covering the types of violations found on merchant websites which allows the Client to view the evidence needed to make educated decisions regarding each violation. The evidence gathered and stored with each violation can be downloaded in a PDF report and used when following up with the merchant involved.

The URL of the Portal is: https://portal.securetrust.com/.

Sponsor Hierarchy

WRM features a multi-tiered Sponsor View hierarchy set-up, allowing a global view for Clients with disparate entities that want to have a single view into the overall merchant risk of their organization. Each Client sponsor in the hierarchy will have its own merchants, scan schedules, and users defined. Users at the top sponsor level will have visibility into their sub-sponsors.

The WRM dashboard provides aggregate summary information across the current sponsor and any sub-sponsors. Client may also select specific sponsors for concentrated analysis.

Scan Types and Frequency

WRM offers three types of merchant website scanning for Clients who purchase Content Monitoring, Merchant Intelligence, Malware Monitoring, and/or Custom Monitoring services.

Each scan of a merchant website follows a similar process, detailed as follows:

- Test that the website is valid and is available via IPV4 on the public internet
- Crawl the first 100 pages of the website and store the HTML code in temporary storage
- Analyze the content of the HTML code that was retrieved by the crawler
- Content violations detected are reported for Analyst review
- SecureTrust Web Risk Analyst team reviews and classifies potential violations or clears them
- Results of each scan are made available in the Portal for review by Client

Onboarding Scan:

A Onboarding Scan assists the Client with onboarding and underwriting online merchants. Client may submit scans to the Portal at any time and receive a result within minutes. Results are aggregated in a Score Card Report to identify a merchant's areas of risk.

Automated Routine Scan:

The content analysis engine will scan merchant websites on an automated routine schedule. The most common frequency for scanning of merchant websites is once per month; however, the frequency can be adjusted to match specific program goals for additional services fees. Different merchant portfolios may be scanned at varying frequencies. Client will be billed for each successful scan of a merchant website.

On-Demand Scan:

An On-Demand Scan can be submitted by the Client via the Portal at any time for any active merchant in the portfolio to assist with investigations outside of the Automated Routine Scan schedule.

Content Monitoring

Card Brand Program Specification

Content Monitoring in WRM is designed to monitor the content and activity of a merchant's website against the policies of Visa and MasterCard. Content Monitoring is routinely updated to align with changes to the card brand policies forwarded from the Client to SecureTrust.

Card Brand Violation Process and Reporting

Once Content Monitoring identifies a potential violation, an Analyst will review the finding and determine whether the suspected website will be reported to Client or cleared. This reduces the number of false positive websites submitted for Client review, thereby allowing the Client to focus its resources on potentially noncompliant merchants within their portfolio.

Card Brand Violation

When a SecureTrust auditor identifies a card brand violation, an email notification is sent to Client's user base specifying which merchant was assigned the violation and prompts Client to login to the Portal to review the findings and act upon the alert. This email notification also specifies which card brand policy the merchant is violating, provides a written report of the audit, and screen capture evidence to record the grounds of the card brand violation.

Card Brand Warning Violation

The Client will receive an email notification for each Card Brand Warning Violation assigned by a SecureTrust auditor. The Card Brand Warning Violation findings summarize the auditors' review of the merchant website; however, with Card Brand Warning Violations, there is no evidence to report a definite Card Brand Violation. Rather, such Card Brand Warning Violations are based on the auditors' experience and knowledge of card brand policies.

Website Redirects

When a merchant website returns an HTTP redirect response code, the site included in that redirect response will be added automatically to the merchant's list of sites to be included in content monitoring. This additional site will be scanned separately and will count as an additional scan for all enabled monitoring services during billing invoice calculation unless Client requests in the Portal that these sites be disabled and cleared. Redirect sites will be made available for Client review in the Portal. Client will not be billed for any redirect sites that have been disabled and cleared before the next scheduled scan.

Merchant Intelligence

Merchant Intelligence is a service designed to provide a summary of the merchant's online presence. Providing the Client with an understanding of which services the merchant website is associated with and background information about the merchant website is beneficial in a thorough merchant risk mitigation program.

Scorecard Report

The Merchant Intelligence Scorecard is available upon completion of a merchant onboarding scan and features up to 13 validations, each aimed at helping guide the final merchant onboarding decision.

The Merchant Intelligence Scorecard includes the following features:

- Displays the information WRM has collected about the merchant's website in a single report
- Provides a summary with a risk rating for each validation that is tested and checked
- Provides a detailed view of sections listed in the summary section

The Merchant Intelligence Scorecard report will also be available for regular scheduled scans to persistently check all the risk areas for a merchant's public-facing website.

Country Risk

WRM captures the merchant's website IP address every time the URL is scanned and uses an extensive database to identify the country where the website is being hosted. WRM maintains a Country Risk matrix, which provides a risk level based on the location of where the website is hosted.

Website Additional Information

Every website scan that WRM performs not only looks for illegal activities, but also gathers important information that may be used during merchant onboarding and on-going merchant monitoring.

WRM captures the following information:

- Contact information pages
- Terms and conditions pages
- Shipping and delivery pages
- Privacy pages

Client may analyze each of these items during the onboarding phase to ensure that the merchant provides accurate and trustworthy information on its website.

Website Pricing

WRM's scan attempts to capture any price points it finds on a website. Each scan stores the highest, lowest, and average price of goods found; WRM tracks the trends for product pricing for any website. Any significant change in the site's pricing could indicate that a merchant has changed its business model.

Password Protected Sites

WRM can detect websites that have a password protected area accessible only with login credentials. These sites will be highlighted under the website security areas within the Portal, including the dashboard and site scan results.

WHOIS and IP Analysis

WHOIS analysis helps the Client validate that the domain registered for the merchant's website is registered to the merchant. WRM alerts Client to any website that has set its WHOIS information as private, as this could be a sign that merchant is trying to hide its true identity.

WRM also searches for other websites hosted on the same IP address as the merchant's website and determines whether any such website has been reported for illegal activities in WRM.

This service is dependent on the availability of Registration Directory Services (formerly WHOIS) information allowed by the Internet Corporation for Assigned Names and Numbers (ICANN) policies as set by the ICANN board of directors. See https://whois.icann.org/en/policies and

https://whois.icann.org/en/implementation for current policies. Client acknowledges that this service may be interrupted or stopped without warning if this information is no longer available to SecureTrust due to policy changes made by a 3rd party and/or government regulation.

Automatic Third-Party Detection

Merchant Intelligence will attempt to identify all the third parties involved in the processing of transactions that originate from a merchant's website. These third parties may include, but are not limited to:

- Internet Service Providers and web hosting providers
- Shopping carts
- Payment service providers

Merchant Intelligence will evaluate this information during each merchant website scan and detail the potential PCI compliance of each third party. This information helps to manage the risk a merchant's transaction processing workflow and website infrastructure may pose to the Client.

The card brands require that the Client register all third-party service providers used by the Client's merchants and ensure that its merchants are only using PCI compliant service providers. Merchant Intelligence helps to identify these third-party service providers for registration. However, Client is responsible for registering with the card brands.

Scan results of all detected third parties will be made available through the Portal.

Malware Monitoring

Malware Detection

Malware Monitoring will use industry leading third-party malware detection and scanning technologies to detect both traditional and advanced dynamic web-based malware on a merchant's website.

Malware Monitoring can be performed on all scan types and identifies merchants that are affected by malware prior to their acceptance, routinely tracks the presence of malware across an online merchant portfolio, and performs on-demand malware checks of any merchant.

Malware Monitoring does not require an installation of software on the merchant's webserver. The results of malware monitoring will be available in the Portal.

Secure Checkout Validation

Any check-out page capturing personally identifiable information data and card holder data must have a valid SSL certificate installed in order to encrypt the data being sent during the transaction process according to various security schemes. If there is no certificate, or the certificate is not valid, the data sent could potentially be observed by a third party.

WRM's process detects the following:

- Whether a website has an SSL certificate installed
- Whether a certificate has expired or is still valid
- The type of SSL certificate
- The supported SSL protocols of the web server

Custom Monitoring

The Custom Monitoring service scans for content that is deemed objectionable by Client and/or prohibited beyond card brand program restrictions. It searches for the specific Client-defined requirements or terms of service violations. An alert is provided when such specified activity has been identified and confirmed by a SecureTrust auditor.

Client may provide a merchant policy statement to SecureTrust to configure the Custom Monitoring profile in WRM. The profile may be modified from time to time in accordance with changes in the Client's.

Custom Monitoring can be performed for all scan types.

Transaction Laundering Detection (TLD)

Transaction Laundering Detection (TLD) is a process to locate and associate card brand damaging websites to merchants within Client's portfolio that may have been previously unobserved by Client.

SecureTrust analyzes a growing comprehensive database of card brand damaging websites ("Damaging Websites") to identify the services provides by such websites. SecureTrust will attempt to a purchase on the Damaging Websites using a card number from a list that has been shared with Client exclusively for use with the TLD service. Client will be responsible for adding these card numbers to Client's fraud prevention system as fraudulent card numbers. When Client detects that a transaction has been attempted with one of these card numbers, Client will be responsible for reporting such attempt to SecureTrust via the Portal. Additionally, SecureTrust may attempt TLD transactions against the website that Client has submitted as the merchant's website to confirm that the merchant is processing as expected. These transactions should also be reported to SecureTrust in the Portal to confirm the process is working normally.

Client is presented with a workflow to respond to TLD alerts within the Portal. This workflow includes report details and declares the action that Client has taken with the merchant to remediate the card brand damaging activity or other laundering activity. The results of this workflow are automatically aggregated into a report that meets card brand specifications for reporting Client efforts to mitigate risk in the form of merchant transaction laundering of a card brand damaging nature. Client may also report transaction laundering that is not of a card brand damaging nature.

Client is responsible for reporting to the card brands any instances of suspected transaction laundering and working with the card brands and law enforcement during any investigation. SecureTrust will provide information to Client from the TLD process as needed during investigation.

Merchant MCC Code Matching

Merchant Category Code (MCC) Matching is a service to help confirm the accuracy of a merchant's MCC code as assigned by Client. An MCC code is a four-digit number listed in ISO 18245 for retail financial services. SecureTrust will use the ISO 18245 standard when performing the MCC Matching service. MCC Matching may also be used to initially define a merchant's appropriate MCC at the time the service is performed by SecureTrust.

Client must submit a list of merchants, including each merchant's company name and website, in order to proceed with the MCC Matching service. SecureTrust will perform the MCC Matching process and provide reports to Client in the Portal indicating the following:

- Confirmed MCC matches for merchants

- Merchants that SecureTrust has determined did not match SecureTrust's analysis, along with a SecureTrust assigned MCC code

Client is responsible for determining the final MCC code of the merchant and may update MCC assignments within the WCM application in the Portal via a bulk merchant operation or by individual manual adjustments.

The MCC Matching service can assign MCCs to merchants if Client has not done so. To perform this assignment, Client must submit the information for these merchants via the SecureTrust Portal individually or by bulk upload. The MCC Matching service may be performed again on a previously submitted list. In order to do so, Client must re-submit the list to SecureTrust via the SecureTrust Portal.

WRM Additional Paid Services

Additional services may be added to the Client's WRM program. These additional services allow Client to receive benefits including delivering services directly to the merchant, increasing analysis frequency for high risk merchant portfolios, and locating websites previously unknown to Client for addition to a WRM program.

Merchant Discovery & Dead Site Review

In some cases, Client may not know the correct URLs or domain names of all merchants in their portfolio, or the URL provided by the merchant may be invalid, dead, or otherwise unavailable to be monitored by the WRM service. In these circumstances, SecureTrust will attempt, on a best-effort basis, to determine the website domain names of merchants based on other business contact information which Client provides.

Client may also request that SecureTrust analyze merchant sites marked as a "dead site" by WRM to determine if the site is a valid site. If the site is valid, Client may request that the scan be resubmitted. If the site is not valid, Client may request Merchant Discovery on this merchant to determine the correct URL or domain name. This service is provided as part of Merchant Discovery and will be billed as Merchant Discovery.

High Frequency Monitoring

The standard frequency for Content Monitoring, Custom Monitoring, Malware Monitoring, and Merchant Intelligence scans is once per month. For an additional service fee and upon Client's written request, this frequency may be increased to a daily or weekly basis.

DELIVERY AND IMPLEMENTATION

Service Initiation

The SecureTrust team facilitates the successful delivery of the service, which includes scheduling and conducting a remote kickoff meeting to define and agree to a high-level project plan consisting of key steps, estimates for duration, deliverables, resource requirements, and escalation procedures.

Phase I: Merchant Onboarding

The first step is to load merchants into the Portal, either via manual entry or bulk upload. Once the merchants have been loaded into the Portal, SecureTrust will execute the onboarding scans, the results of which will be available in the Portal. Client is responsible for reviewing these scans and indicating to if each

merchant will be onboarded or cancelled. Only merchants that Client indicates will be onboarded, or are automatically onboarded, will be included in future monitoring activities. Any merchant that is cancelled by Client manually or via the bulk upload tool will not be monitored further and will not count towards services rendered for billing purposes in future invoicing, unless reopened again.

Phase 1a: Card brand service provider registration

Client will be responsible for registering SecureTrust as Client's Merchant Monitoring Service Provider (MMSP) with the Mastercard Business Risk and Mitigation (BRAM) program for content monitoring and Transaction Laundering (TL) detection if Client is subscribed. Client is also responsible for registering SecureTrust as Client's service provider with all card brand programs where Client is required to register any provider, such as: Visa Global Brand Protection Policy (GBPP). If Client does not have a direct relationship with MasterCard or Visa, Client is responsible for notifying their acquiring bank that Client is using SecureTrust WRM for BRAM and GBPP compliance to allow acquirer to register SecureTrust as providing BRAM and GBPP services for Client's merchants.

Phase II: Transaction Laundering Preparation

The Client is responsible for all configuration and/or custom development necessary to prepare for TLD monitoring. SecureTrust will provide the Client with a list of randomly generated, non-active credit card Primary Account Numbers (PAN) that will be used by SecureTrust during TLD monitoring. Client will be responsible for enabling automatic detection and blocking of transactions attempted using these PANs. Client will work with SecureTrust to perform test transactions to confirm that the process works before SecureTrust begins the TLD monitoring process by attempting transactions.

Phase IIIa: Merchant Monitoring

Once merchants have been onboarded, SecureTrust will begin the monitoring process. Results for all monitoring scans will be available through the SecureTrust portal. Client is responsible for accessing, reviewing, and acting upon these results in the SecureTrust Portal.

Phase IIIb: Transaction Laundering Detection Monitoring

Once TLD monitoring preparation is complete, SecureTrust will begin the TLD monitoring process. This will include SecureTrust research, discovery, and analysis of potential laundering sites. Once potential sites have been identified, SecureTrust will attempt transactions using the shared list of PANs. Client will be responsible for monitoring Client's process system for potential detections of these transactions.

When these transactions are detected, Client will be responsible for tracking and reporting the following to SecureTrust:

- MID of merchant
- Date and time
- Response
- Transaction amount
- Credit card PAN

Client is responsible for informing SecureTrust if it detects a transaction attempt using a PAN from the shared list provided by SecureTrust. These transactions may be attempted against the merchant's registered website or against other websites that SecureTrust believe may be associated with illegal activity or are potentially using merchant's MID for other forms of laundering.

Phase IV: Merchant cancellation

When Client no longer wishes to monitor a specific merchant, Client will request cancellation of monitoring for that merchant via the Portal manually or using the bulk upload tool. SecureTrust will cease monitoring when a bulk operation has completed successfully and confirmed with Client, or when Client manually cancels the merchant via the Portal.

Phase V: Card Brand Violation Notifications

Client is responsible for responding to all card brand notifications that a merchant has been found in violation of a card brand's rules, policies, or regulations. SecureTrust will assist Client in determining the following:

- Whether SecureTrust has performed any WRM services in reference to the merchant that the card brand has reported in violation
- When SecureTrust was provided information from Client regarding merchant
- What services have been performed
- When the services were performed
- The outcome of those services

This information can be provided on SecureTrust letterhead to Client for response to a card brand, but will always be immediately available in the Portal for the Client to investigate and report to the card brand on the Client's letterhead. SecureTrust will make every reasonable effort to respond quickly to any violation reports submitted by the Client using the ticket tracking system and email, but SecureTrust makes no warranty to the timeliness of responses to these requests. It is the Client's responsibility to respond in a timely manner to the card brand. The Client is responsible for any fees incurred due to the timeliness of the response to a card brand violation letter, or the results of any investigation by the card brand or law enforcement.

Merchant Discovery Process

SecureTrust's Merchant Discovery process requires the following information:

- Merchant ID (or another unique identifier)
- Merchant Doing Business As (DBA) Name
- Merchant Registered Company Name
- Physical Address of Retail Location (if any)
- Point of Contact Email Address
- Suspected URL or domain name (if available)

Client must provide this information to SecureTrust in an Excel spreadsheet. SecureTrust will provide a template of a preferred spreadsheet format.

Once Client has provided the required information to SecureTrust, and requested Merchant Discovery, SecureTrust will begin the Merchant Discovery process. Once this process has been completed, the results will be made available in the Portal. Client will then be responsible for completing the onboarding process for the merchants that Client wishes to onboard or cancelling any merchants that Client does not wish to onboard. Merchant monitoring will not begin for each new merchant and/or site until Client completes the onboarding process for each new merchant. SecureTrust will work with Client to discuss how to address merchants where no URL was found.

Invoice Calculation

SecureTrust will calculate an invoice for Client's usage of the SecureTrust WRM service according to the terms of the executed agreement and based on the number of successfully completed website scans during the invoice period.

- The standard service for WRM is one scan per month per URL
- Overage fees are calculated by dividing the monthly price by the number of URLs included in the monthly scan price
- SecureTrust will calculate the number of enrolled URLs during the invoice period.
    - An enrolled URL is any URL that is configured in the SecureTrust portal for an active merchant during the invoice period
- SecureTrust will calculate the number of completed scans (across all scan types) on a per URL basis during the invoice period.
    - A completed scan is any scan that does not result in an error as reported in the SecureTrust portal
- Any URL added by the automated system due to a website redirect is automatically considered an enrolled URL if it is not removed by the Client before the end of the invoice period.
- SecureTrust will calculate the number of merchants enrolled in the merchant discovery service during the invoice period.
- SecureTrust will create the invoice using the terms of the Client agreement for all enrolled services and submit to Client for payment as per the terms of the Client agreement.
- Any other fees or charges will be included as per the Client agreement.

SECURETRUST RESPONSIBILITIES

- Establish and maintain contact with Client.
- Establish communication and escalation plans.
- Schedule and conduct kickoff meeting.
- Provide Client Portal account credentials.
- Respond to Client support requests via the Portal ticketing system, email, or telephone.
- Provide monitoring services as detailed in this document.
- Provide access to result data and reporting as detailed in this document.
- Calculating a monthly or quarterly invoice.
- Submitting the monthly or quarterly invoice to Client for payment.

CLIENT RESPONSIBILITIES

- Establish and maintain contact with SecureTrust.
- Establish communication and escalation plans.
- Agree to high-level project plan key steps, estimates for duration, deliverables, and resource requirements.
- Forward all notices from card brands, including updates to the card brand monitoring programs
- Participate in and understand materials explained during calls, meetings, and discussions
- Client acknowledges:
    - This product is delivered as a remote service on computer systems owned and operated by SecureTrust.

- SecureTrust will be performing remote website crawls, scans, vulnerability scans, and collecting information about Client's merchants from third parties after the merchant completes onboarding.
- Client is responsible for providing SecureTrust with the merchant information required to begin the onboarding or merchant discovery processes.
- Client is responsible for onboarding merchants, or allowing merchants to be automatically onboarded before services commence for each merchant loaded either manually or by bulk loading via spreadsheet.
- Client is responsible for disabling any merchant or site URL Client does not want to be scanned before the scheduled scan starts. If the merchant or site is not disabled before the scheduled scan, Client will be billed for the scan and all URLs are considered as enrolled for that invoicing period.
- The WRM system will automatically enroll any URL that the system receives as a website redirect.
- Client is responsible for reviewing all URLs that the system adds as a redirect and reports as a dead site.
- Client is responsible for adding and/or removing URLs for enrolled and active merchants within the Portal.
- Client is responsible for acquiring and maintaining consent from Client's merchants and service providers for all activities, including, but not limited to:
  - Remote web site crawling
  - Vulnerability scans
  - 3rd party information gathering
  - TLD transaction attempts
- SecureTrust will perform the service in the English language.
- SecureTrust will not create or modify Client documentation.
- SecureTrust will not provide remediation services.
- Client authorizes SecureTrust to respond to requests from MasterCard, Visa, or other card brands to verify Client's enrollment in SecureTrust's WRM service.
- SecureTrust will provide support services from 0900 to 1700 US Central time Monday through Friday in English only.
- Client is responsible for communicating and working with the card brands.
- Client is responsible for completing any required service provider registration process with the card brands that Client works with. SecureTrust will not register as Client's service provider with any card brand.
- Client is solely responsible for responding to card brand violation notifications from all card brands.