

Merchant
User Guide

Safetech Fraud Tools – Getting Started

May 30, 2013

|

Version 1

CHASE ™
Paymentech

CHASE ™
Paymentech

4 Northeastern Blvd.
Salem, NH 03079-1952
603.896.6000

www.chasepaymentech.com

Getting Started with Safetech Fraud Tools

A Merchant Reference Guide



© Chase Paymentech Solutions, LLC – 2013 – All Rights Reserved

14221 Dallas Parkway
Dallas, TX 75254
www.chasepaymentech.com

This document contains confidential and proprietary information of Chase Paymentech Solutions, LLC and Paymentech, LLC (collectively referred to as "Chase Paymentech"). No disclosure or duplication of any portion of these materials may be made without the express written consent of Chase Paymentech. These materials must be used solely for the operation of Chase Paymentech programs and for no other use.

Revision History

Date	Revision Summary	Page(s)
05.30.13	Reference Manual Created	All

Table of Contents

- Revision History* i
- Introduction**..... 4
 - Why Do You Need A Fraud Management Solution?*..... 4
- Safetech Fraud Tools Components**..... 6
 - Multi-Layer Device Fingerprinting*..... 6
 - Proxy Piercing*..... 7
 - Persona Technology* 7
 - Dynamic Scoring and Rescoring* 8
 - Safetech Fraud Score*..... 9
 - Manual Review AutoAgent*..... 9
 - Business Intelligence Reporting*..... 10
 - Third Party Callouts* 11
 - Agent Management* 11
 - Mobile Device Analysis* 12
 - Workflow Management*..... 12
 - VIP Lists* 13
 - Chargeback Data (VISA and MasterCard)* 14
- Safetech Connections** 15
 - Required* 15
 - Orbital Gateway, Stratus or via Spectrum SDK 15
 - Kaptcha (Data Collector) 16
 - Web Console User Interface 16
 - Optional*..... 17
 - Event Notification System..... 17
 - Application Programming Interfaces (API's) 18
 - Mobile SDK..... 18
- Process Maps**..... 19
 - Safetech Score Coupled with Authorization* 19
 - Stand Alone Safetech Score Request Followed by Authorization* 20
 - Stand Alone Authorization Request Followed by Safetech Score* 21
- FAQs** 22
 - Who Do I Call?*..... 22
 - Frequently Asked Questions* 23
 - What if I lose my Password? 23
 - What if my login isn't working? 23
 - What is GEOX? 23

Why did an order receive the score it did?.....	23
How is the score created?.....	23
How do I add a value to one of the VIP Lists?.....	24
Why was Kaptcha/Data Collector data missing on an order?.....	24
What happens when there’s no Kaptcha/Data Collector data?	24
What is a persona?	24
What is a device fingerprint?	25
How can I see Linked Orders?.....	25
How can I tell why orders were linked?.....	25
Why is an order no longer showing as linked?	25
How can I tell if this order was placed from a mobile or handheld device?.....	25
What does the time zone represent?	25
What is the HTTP Country?.....	26
What are Extended Variables?.....	26
How can I see which rules or thresholds triggered on an order?	26
Can a customer edit information on an order and re-submit and receive a new score?	26
Why didn’t my rule updates get saved?	26
How do I edit a rule?.....	27
Can I have more than one rule set active?	27
How do I activate another rule set?.....	27
How can I see a report of transactions processed?	27
What does it mean when some scores are highlighted orange?.....	27
Where can I see the most current score of an order?	28
How do I assign orders to Agents?.....	28
Can I add a note to an order?	28
What is “Re-evaluate” Button?.....	28
Do you validate email addresses?.....	28
What is a proxy server?	29
What is a Website ID?.....	29
What is Shopping Cart data?.....	29
What is a User Defined Field (UDF)?.....	29
What is Melissa Data?.....	29
How do I receive scoring on my Phone Orders from my Call Center or Customer Service teams?.....	30
How does Kaptcha/Data Collector work on phone orders?	30
<i>Risk Evaluation Field Definitions.....</i>	<i>30</i>
<i>Description of Delivered Data.....</i>	<i>31</i>
Basic Device and Network Variables:.....	31
Multi-Merchant Variables and Other Variables:.....	33

Introduction

Why Do You Need A Fraud Management Solution?

So, what does a card-not-present (CNP) merchant look for when searching for a fraud management solution? Today's technology is complicated, compared to the simplistic Address Verification Service (AVS). The key attributes of a state-of-the art fraud management offering are identified below – along with a statement about the specific purpose or value to the CNP merchant.

Some of the most desirable traits of a fraud management offering include:

- The ability to identify repeat transactions from the same point-of-sale device
- The ability to pinpoint the location of a transaction's origin
- The use of a sophisticated and proven statistical scoring model
- The ability to detect fraud globally
- The ability to link orders that share little or no common elements
- The use of continuous transaction monitoring
- The availability of a custom rules engine
- The availability to customize workflow management
- The ability to interface with third party verification sources accomplishes all of the above. The use of TargusInfo; Lexis Nexis Instant ID or Chargeback Defender; or 192.com will provide the merchant with additional resources to utilize in fraud review.

The Safetech Fraud Tools Web Console uses multiple, proven fraud-fighting technologies designed to maximize a merchant's revenue while minimizing fraud exposure. This solution is designed to apply to virtually any level of the market from small business through strategic markets. The fraud detection capability is much more technologically advanced than traditional fraud prevention offerings such as Verified by Visa™ and MasterCard SecureCode™. When used correctly, this solution will be the only fraud prevention solution the merchant will need to minimize their fraud exposure while maximizing their revenue.

Fraudsters are intelligent, well-funded and more importantly, resilient in their efforts to make money from fraudulent practices. They spend a great deal of time researching the vulnerabilities of various merchants. They look for gaps in fraud detection capabilities, order response information used to validate or reject orders, call center response questions, changing/seasonal fraud strategies as well as weekend/after hours support. Their sole purpose is to discover any possible weakness in a merchant's order process and exploit it to the fullest extent possible.

But that's not the worst part of it! Sophisticated fraudsters are patient as well. They recycle identities and may hold compromised cards "in reserve" so they can slowly cash in on the rewards over time rather than attempt a full-scale assault on a merchant site that may raise red flags.

Continued on next page

Why Do You Need A Fraud Management Solution?, Continued

Safetech Fraud Tools uses a combination of detectors including:

1. Real-time order analysis and comparison across all merchants participating in the program
2. Geolocation technologies to fingerprint the device used to make the purchase and the physical geographic location of the device at the time of the purchase
3. The ability to create “personas” of both good and bad transaction details over time so that fraud rings can be identified and linked together in real time. In short, the solution was designed to detect all forms of CNP fraud operating across the globe in real time. It is the single most advanced, merchant-facing fraud detection suite integrated with an acquirer today.
4. Custom Rules Engine / Management

The use of a scoring methodology to compare variables (such as order elements, device fingerprints, proxy locations, etc.) in real time, coupled with the ability to continuously monitor these transactions for connections to future fraudulent activity, is a major differentiator. Scoring can be applied to any type of CNP sales channel including web, call center and Internet voice recognition.

Example: Let's consider a merchant who is selling laptop computers. They may decide, via the use of this solution, that an order placed at 8 a.m. EST is legitimate. So, orders placed at 8 a.m. are accepted and processed as usual. However, during the picking and packing process, the system may reassess the order using new order elements coming in from multiple merchant sources. New information indicates that the order is fraudulent. The picking and packing process is halted and the order is rejected. Information that was not available at the time the order was placed has now prevented the merchant from shipping the product to the fraudulent purchaser. The web console will provide constant score updates on prior orders every 30 minutes for a 2-week period to ensure maximum fraud detection effectiveness.

Safetech Fraud Tools Components

Multi-Layer Device Fingerprinting

This feature collects a complete set of data that will identify a device in real time (fixed or mobile). The key is the ability to analyze customer behavior associated with the device and to collect additional parameters that are not typically accessible by other device technologies. Chase Paymentech's process does this without retrieving the user's personally identifiable information (PII).

Multi-Layer Device Fingerprinting is a part of Chase Paymentech's complete solution. It examines any device via numerous attributes – computer, tablet PC, SmartPhone, etc. While the device type may vary, the following characteristics are typically examined:

- Network
- SSL
- JavaScript
- Browser
- Operating System
- Flash
- HTTP

There are other variables analyzed as well: time zone, country/region, proxy use, cookies enabled, language, remote control of device, wireless application protocols and associations to other devices with histories of fraudulent activity.

It is through the examination of all of these different layers within a device (in as little as 300 milliseconds) that Multi-Layer Device Fingerprinting establishes and maintains a distinct device ID. This helps even when fraudsters try to modify system settings to disguise their true identities.

Merchants can associate certain device anomalies with fraud patterns, making it easy to create specific rules to optimize fraud detection, regardless of the device being used.

So basically this detector operates under the assumption that all devices capable of executing a payment transaction have a unique fingerprint, just like the human hand. Any merchant who sells a good or a service via a website can utilize this technology to attach a unique ID to each device used to make a purchase. It's an incredibly powerful detector of many types of fraudulent activity, especially when combined with proxy-piercing technology (see below). Fraudsters must literally change the majority of the device variables associated with the "source" computer to alter the device fingerprint itself. This fact is further proof that no single tool can effectively block all forms of fraud. Device fingerprinting is not applicable to any sales channel outside of web commerce as it requires direct interaction with the consumer's web browser at the time of checkout.

Proxy Piercing

This feature is designed to combat fraudsters who try to hide their activity behind proxy servers (thus hiding their actual location). Proxy servers are intermediary devices that disguise the geographical location that is associated with high fraud activity. For example, a fraudster may use a proxy server to appear as though they are using a stolen credit card from the same location as the owner of the stolen card.

The Proxy Piercing feature determines if the purchasing transaction is being relayed through a proxy and if so, it can determine:

- The true geolocation of the purchase request
- The type of network being used by the person attempting to make the transaction.

Certain locations are considered high risk of fraud such as:

- Prisons, schools, library, anonymous proxies

The Proxy Piercing feature can also detect “botnets”. Botnets are networks made up of remotely-controlled computers that have been compromised without the owner’s knowledge or consent. These are used to relay fraudulent purchase requests in an attempt to again hide the true source of the order. The Proxy Piercer can detect these botnets and provide the true geolocation of the fraudster.

This detection occurs in real-time thus it returns the result while the transaction is still in the merchant system and can be passed to the merchant’s risk assessment department before an approval is given on the transaction. Due to this, the merchant can either conduct additional risk evaluation activity or decline the purchase request as they deem appropriate.

Persona Technology

The Persona feature determines the key characteristics and identified qualities and attributes associate with a transaction. Persona constructs a definitive link to online purchase behavior (directly or indirectly) to help reveal fraudulent activity. The process itself takes less than one second to provide merchants with highly accurate fraud assessments in real-time.

A Persona is built as the Safetech Fraud Tools system collects information from the purchases made across all merchants within the network and links that data throughout the fraud database.

The process starts with technologies like Dynamic Scoring, Multi-Layer Device Fingerprinting, and Proxy Piercing assessing over 200 variables and reporting in real-time on potential risks on the transaction. When these variables are compiled and evaluated, a Persona is created.

Continued on next page

Persona Technology, Continued

Examples of attributes that make up a Persona are:

- The number of credit cards linked to the Persona. A single Persona may be associated with dozens of credit card numbers issued to different individuals that have been used to make purchases within a short time span.
- The number of email addresses associated with a Persona making a purchase.
- The actual location of the individual making the purchase as determined through the Proxy Piercer.
- Discrepancies in the customers self-divulged information and actual information as determined by Multi-layer Device Fingerprinting information.

Dynamic Scoring and Rescoring

This dynamic feature monitors credit cards for signs of fraudulent activity even after a transaction has been approved so it can retroactively tie suspicious activity to previous purchases. This process is “Post-Authorization” and has proven highly successful at identifying suspicious activity and alerting the merchant that a previously-approved order now looks to have connections to fraudulent activity. The merchant can then re-evaluate the order and decline to ship – avoiding the loss of goods while preventing the expense of a chargeback or return.

This feature is based on the fact that stolen credit cards and/or account numbers quickly start to exhibit patterns that identify them as involved in fraud. For example, stolen cards often incur a high number of big ticket purchases in a short amount of time, spawn multiple device identities in rapid succession, and give changing email addresses across multiple transactions.

Dynamic Scoring will continually monitor all account numbers involved in an approved transaction and provide real-time updates when the risk status changes. This is done by identifying and grouping transactions that are directly or indirectly linked through a set of attributes or variables such as Device IDs, Account Numbers, and emails. Based on the updated status, the merchant can determine if there is sufficient threat of fraud to retroactively decline the purchase request or take other necessary action.

This feature is a continual real-time process. As information changes across all merchants in the Safetech Fraud Tool system, the “fraud risk” score for any transaction currently in each merchant’s queue will also change.

Safetech Fraud Score

The Safetech Fraud Score provides a more predictive control and customization in the way merchants manage fraud risk. The score is a highly accurate prediction of fraudulent activity using information from over two billion purchase attempts. The Risk Inquiry System (RIS) generates a numeric Fraud Score (between 1 and 99) in real-time for every transaction. The higher the score, the greater the risk of fraud.

Unlike other scoring systems that may use only a few variables to calculate risk, the Safetech Fraud Tool's Predictive Modeling reviews over 200 variables that cross-reference the transaction with millions of data points looking for association with risky behavior.

Included in a Safetech Fraud Score calculation:

- Multi-merchant order linking
- Customer credit cards, email addresses and shipping addresses
- Highest risk country within the past 14 days, using the Proxy Piercer
- Multilayer Device Fingerprinting Analysis
- Machine setting and configurations
- Network type, such as prison, school, library, or satellite
- Use of anonymous and proxy services
- Time zone and device time differences
- Persona Fraud Identification technology

Since a fraudster's organization or botnet usually attempts multiple fraudulent purchases while any single merchant is evaluating an individual purchase, Safetech Fraud Tools allows you to dynamically re-score a potential purchase on-the-fly, so you can detect a fraudulent purchase that may have initially appeared legitimate.

Manual Review AutoAgent

Please note that this section does NOT apply to Safetech Express Users.

The AutoAgent feature is a powerful rules engine that enables administrators and risk assessment managers to create custom rules for orders with specific characteristics. When an order is entered into the merchant's system that has one or more of these characteristics, it's automatically routed for the AutoAgent review and disposition. The Auto Agent can then apply additional tests, processes, and/or profiles and reach a decision to approve, review, decline, or escalate without the need for intervention by a human risk assessment agent.

The AutoAgent has its own rules engine that is separate from the Primary rules engine. This makes it possible to automate additional review processes for certain types of suspect orders.

An example of how this might work could be if an order triggers a certain rule, the AutoAgent can be instructed to automatically perform a look-up using third party vendors, such as TARGUSinfo, LexisNexis, or 192.com. Once this additional step is complete, the order is profiled for risk based on the new data.

Continued on next page

Manual Review AutoAgent, Continued

Because the AutoAgent lets merchants create rules and rule actions for the system to determine without involving a human agent, the efficiency of the risk assessment team is greatly enhanced. Fewer agents can handle higher overall transaction volumes without increasing a merchant's fraud exposure.

The merchant can also use this feature to maintain control over how rules are written and applied for both the Primary Rules engine and the AutoAgent rules engine. Only those suspect orders deemed appropriate to be auto-decided by the AutoAgent. Any orders the merchant requires to be manually reviewed are still routed to the risk assessment team.

Business Intelligence Reporting

Please note that this section does NOT apply to Safetech Express Users.

Datamart is Safetech Fraud Tool's Business Intelligence application suite. This feature uses an integrated dashboard, data mining, reporting, and workflow tools to structure raw data into a comprehensive presentation. These reports can help merchants plan and manage risk management, staff workload, transaction queues, rule effectiveness, organization and more. This feature makes it easy to maximize functionality and productivity while ensuring system integrity and security.

Datamart helps administrators discover trends, summarize results, and analyze historical information of transactions drawing from over 100 variables. This feature assists in validating rule effectiveness, preparing agent and workflow management results, evaluating shopping cart details, and preparing custom dashboards with simple, drag-and-drop functionality.

Datamart includes over twenty-nine standard reports and dashboards such as agent, workflow, analysis, operational, planning, and trending reports. It also includes over 100 variables and drag-and-drop features making the creation of custom reports virtually unlimited. Reports can be viewed in table or chart formats and easily be exported.

Administrators can also track any configuration changes to the management console, rules engine and workflow to verify that an authorized individual made each change and that the changes match the approved policies. User Login Reporting tracks user login attempts (successful and unsuccessful). This report can help determine if a party is attempting to gain unauthorized access to the system.

Third Party Callouts

The Safetech Fraud Tools Complete solution integrates data services from leading providers to facilitate smooth, seamless operations – without having to leave the Safetech Fraud Tools interface.

To aid risk assessment agents and to support automated functions and capabilities, Chase Paymentech has integrated a number of key data services into this solution.

This integration of third-party evaluation and assessment services within Safetech provides merchants with a superior level of fraud detection within a single, on-screen view. When necessary, merchants may choose to use one or more of these third-party services to enhance their ability to quickly review and validate transactions. These services are directly accessible through the Web Console for easy access and can be used as a part of the rules engine and the AutoAgent feature.

Agent Management

The Agent Workflow Console helps increase efficiency and reduces the cost of manual reviews. This feature addresses one of the largest fraud prevention costs for merchants: the training and maintenance of human risk assessment agents to manually review orders. Using a pattern-based rules engine and auto-decision routines, the Agent Workflow Console feature enables superior operational efficiencies when reviewing transaction activities, evaluating risk, and managing human assets.

This feature uses a number of tools that automate routine risk assessment tasks. For example, if Safetech Fraud Tools detects attributes in a transaction that indicate possible fraud, the Agent Workflow Console feature can invoke one or more rules which in turn can trigger the “auto-decision” feature to take actions based on pre-defined merchant specifications.

Features like this help risk assessment agents more quickly determine whether an order is valid or if a manual review would be necessary.

Merchants can also add third-party risk assessment functionality to the Agent Workflow Console, such as including real-time web links to data verification sources like TARGUSinfo, LexisNexis, and 192.com, enabling agents to seamlessly gather customer information through on-demand address and telephone verification.

The interface provides a number of risk assessment agent management tools – such as Workflow Metrics, which generates a detailed report on the departments’ workflow and Agent Metrics, which provides an analysis of any given agent’s activities – to help merchants better manage the risk assessment department by allocating resources more efficiently.

Mobile Device Analysis

While mobile commerce is an exciting way to allow customers a choice when purchasing services and products, it has also opened the door for fraudsters to have more ways to access goods and services as well. Unlike other forms of payment, mobile devices introduce many elements that complicate the user verification process. Stolen mobile devices are as vulnerable as stolen credit cards and other forms of identification.

Safetech looks at fraud as fraud without regard to where or with which device or payment method it is being committed. While mobile devices have a different set of criteria for merchants to identify, validate, and authorize purchases as quickly as possible, The Safetech Fraud Tools all-in-one solution makes it easy to monitor transactions coming from mobile devices and make any necessary adjustments.

The Risk Decision Rules engine gives merchants the flexibility to approve, decline, or review orders from any type of device (including mobile) automatically, based on established business rules.

With mobile devices, speed and accuracy are critical to keep the checkout process friction-free and still catch fraud in real-time and meet customer expectations. The Safetech Fraud Tools platform already has mobile protection technology integrated in as a part of the overall fraud solution to protect merchants from fraudsters using mobile devices.

The Safetech Fraud Tools platform looks at each transaction individually, reviews hundreds of data elements and gives merchants an assessment in less than one second, regardless of device. This single platform approach simplifies fraud management and maximizes effectiveness.

Workflow Management

Please note that this section does NOT apply to Safetech Express Users.

Workflow management is an important factor that ensures the efficient and effective processing of orders flagged for review. Based on established rules, the Workflow Queue Manager quickly sends suspect transactions to the most appropriate review agent for a convenient and appropriate resolution. The Workflow Queue Manager recognizes each rule's assigned priority based on other factors including "time in queue" and many others.

Continued on next page

Workflow Management, Continued

Resolving suspicious transactions quickly helps increase sales and maintains a high level of customer satisfaction. The Workflow Management feature allows the freedom to process manual reviews quickly and efficiently using the Workflow Queue Manager. Any number of filters, or rules, can be used to flow transactions to the most appropriate review agent whether on premises, working from home, or anywhere in the world – thus maximizing efficiency and operational control.

When manual reviews are required, Safetech makes it easy to manage order flow and maintain established business processes.

VIP Lists

The VIP list is an important feature of the Safetech Fraud Tools platform. Merchants can set up lists based on certain criteria and then create rule actions for each VIP List in the system. Some different options for VIP Lists include Email lists, Shipping Address Lists, Device ID lists, UDFs and even Card Number Lists. If a transaction comes through and hits a category on one of these VIP lists, it will automatically be forwarded to review that transaction regardless of any other triggers that transaction may have cleared or the transaction may be triggered to automatic denial based on the settings of the specific VIP List.

VIP lists can have actions set such as Review, Escalate, Decline, or Approve. They can also be set to forward a transaction on to the AutoAgent.

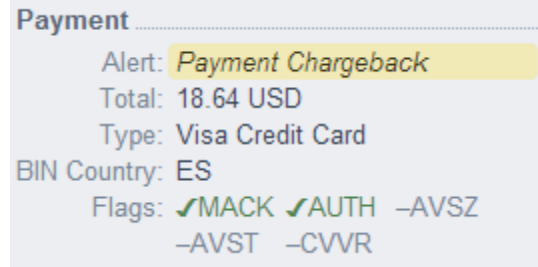
We recommend adding items such as Credit Card, Device, Email and Shipping address to the VIP review or decline list for any confirmed or suspected fraud orders including Chargebacks.

Chargeback Data (VISA and MasterCard)

By providing Safetech Fraud Tools with chargeback data and history, the information can be utilized for analysis of submitted transactions. Rules can flag current orders if their data relates to a previous chargeback and historical data analysis can be used to determine if there is a pattern.

Chargeback information for a merchant account will display in the Transaction Details page in the Payment Section.

If a chargeback has been entered against a particular transaction, the yellow band will display along with the words "Alert: Payment Chargeback".



The screenshot shows a payment summary with the following details:

- Payment** (Section Header)
- Alert:** *Payment Chargeback* (highlighted in a yellow band)
- Total:** 18.64 USD
- Type:** Visa Credit Card
- BIN Country:** ES
- Flags:** ✓MACK ✓AUTH -AVSZ
-AVST -CVVR

Merchants can also run reports showing Chargeback data from the Adhoc Reports and Datamart options in the Reports Tab.

Safetech Connections

Required

In order to connect with Safetech, merchants need to utilize the listed connection points. This section reviews the connection points to Safetech that are required and why a merchant would want to include or exclude each feature.

Orbital Gateway, Stratus or via Spectrum SDK

The Safetech Fraud Tools service is fully integrated with Orbital Gateway processing, through the transaction submission server, called Stratus, or via the Spectrum SDK. Whether including additional information in an authorization request, or sending a stand-alone request, the basic process remains the same: A consumer navigates to the payment page to complete a purchase or bill payment. The Safetech Fraud Tools seamlessly capture location and device data from the consumer. The merchant sends an authorization request or standalone Fraud Analysis request, the Safetech service then returns fraud score information in the response message to the request.

All data elements submitted in the transaction are included in the fraud scoring process performed by the Safetech service, so the overall value of the fraud score result is directly related to the transaction data included in the request.

The Fraud Score is a numerical representation of the relative risk of each transaction that is screened. The information returned can be used to enhance any current risk program, or to develop a customized approach to risk management.

The Orbital Gateway, Stratus, and Spectrum SDK both provide the response information provided by the Safetech service; however it is the merchant's decision to proceed or not to proceed with a transaction.

When a transaction receives a fraud score a merchant deems unacceptable, the merchant should submit a corresponding Void or Reversal request to prevent the transaction from going out in settlement.

Continued on next page

Required, Continued

Kaptcha (Data Collector)

The Kaptcha/Device Data Collector collects and analyzes data from the customer's browser. Each time a customer views the merchant order screen, a Kaptcha/Device Data Collector image is loaded. The Kaptcha /Data Collector specification details the requirements for implementing the Kaptcha/Device Data Collector. Generally, when detecting fraud, not all of a customer's information is required. However, every piece of data has potential value and a customer providing additional data is always better for fraud detection purposes.

The customer's browser is required to interact with the Kaptcha/Device Data Collector servers, although in an indirect manner. This enables Chase Paymentech to perform an automated risk analysis of the customer.

Web Console User Interface

The Web Console is the host-based web application interface between merchants and Safetech Fraud Console. It provides an area where merchants can set up fraud detection rules and VIP lists, disposition orders in a job-order queue, use reporting tools to gather information on customer orders.

Optional

Event Notification System

When you are using the Safetech Fraud Tools system to process purchasing requests going through your business, events are almost constantly occurring. Transaction risks are being calculated and recalculated, transactions are being assigned to agents, and DMC rule values are being changed. Each one of these events is registered in Safetech Fraud Tools and the event information can be sent to you at any website your company hosts. This allows you to monitor Safetech Fraud Tools events related to your business “under the hood”, rather than using the Reporting features in the AWC.

There are four general classifications of events.

- **DMC Events:** Events that are typically set in the DMC such as changes to email, credit card, or postal address lists.
- **Workflow Events:** Events that are typically associated with changes in the workflow queue such as assigning a transaction to an agent.
- **Risk Change Events:** Events that are typically associated with some change in transaction risk such as a change detected in the buyer’s network type.
- **Special Alert Events:** There is only a single event in this class; the change in score of a transaction previously approved to a score below the approve threshold.

These events are either generated by an **Agent** or **API** action¹ or by a **System** action. Agent actions are specific activities conducted by your company’s **Risk Department** staff as they perform their tasks in the Safetech Fraud Tools AWC. System actions are activities automatically performed by Safetech Fraud Tools itself as it analyzes and processes transaction information submitted to the system.

If you so request, you can have notices of each event sent directly to a website at your company. You must provide us with the URL of that site and once you do, the events described are queued by Safetech Fraud Tools and sent to your website.

Actual events occur in real time; however the event information is queued and transmitted to your URL every 30 seconds by default. Event information is sent in **XML** format.

It is highly recommended to use Event Notification for any merchants that want to utilize Safetech Fraud Tools to hold orders for manual review.

Event Notification is the communication process that Safetech uses to update orders on the back end.

One of the benefits of Event Notification is that manual review staff can make notes and update held orders within the Safetech Web Console.

Event Notification can be used to update the Order Management system and release or cancel orders. This reduces the time staff spend manually processing orders.

Continued on next page

Optional, Continued

Application Programming Interfaces (API's)

APIs allow you to send information to Safetech Fraud Tools, such as adding a large number of email addresses to a VIP list, adding chargebacks and receive a response stating if your change was successfully accomplished.

Mobile SDK

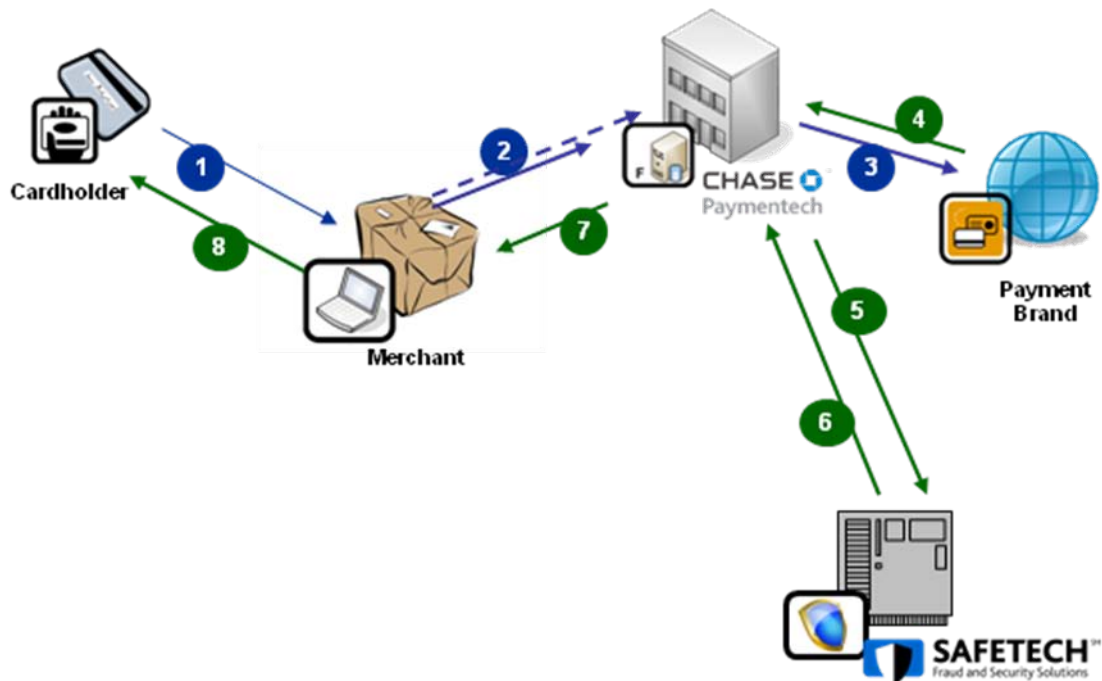
A Software Development Kit, also called a “devkit” or SDK, is a set of development tools that allows software engineers to create customized applications for a particular software package, software framework, hardware platform, or operating system. This allows developers to create applications specific to their business needs that will interact with the product or products developed by the SDK creators. In order to take advantage of our Android and iOS Mobile SDK, merchants must have their own mobile application that they can embed this SDK code into in order for mobile device interrogation to occur.

The Android Device Collector SDK provides a java jar file which can be used to perform Device Collection interaction with Chase Paymentech for native Android applications. The SDK includes a collection of development tools that allow you to build your own customized applications in order to submit information to the Risk Inquiry System (RIS) server.

The Chase Paymentech iOS Device Collector SDK provides a static library which can be linked with an iOS application to perform Device Collection interaction with Chase Paymentech for native iOS applications on Apple's iPhone and iPad platforms. The SDK includes a collection of development tools that allow you to build your own customized applications in order to submit information to the Risk Inquiry System (RIS) server.

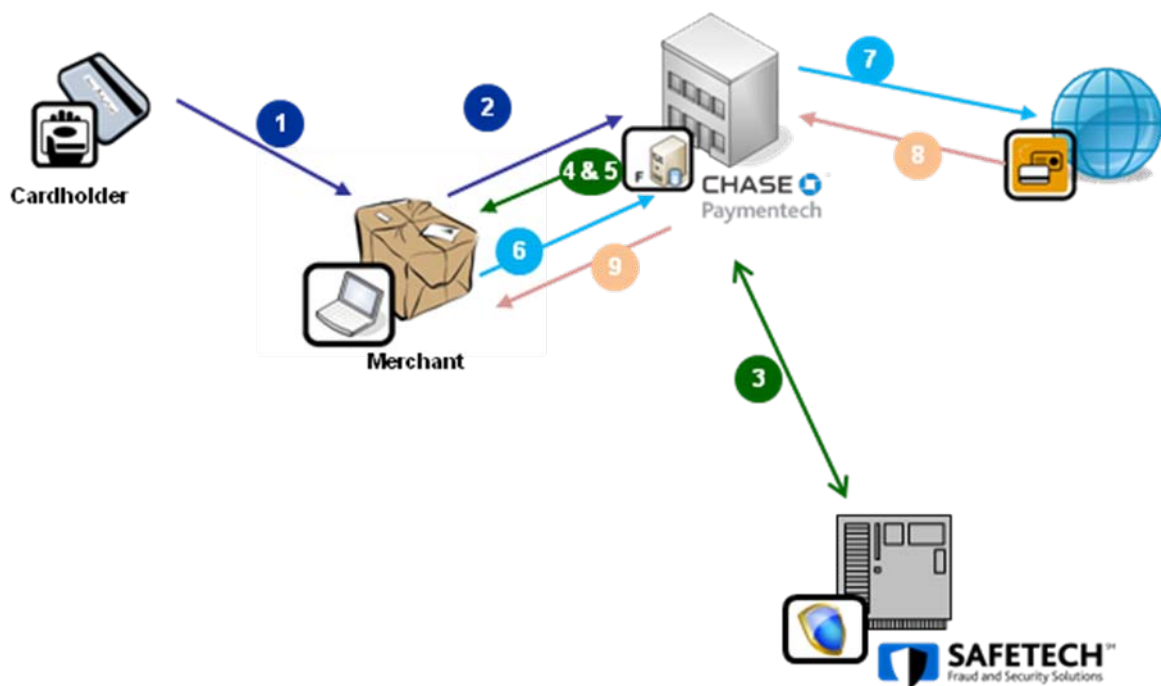
Process Maps

Safetech Score Coupled with Authorization



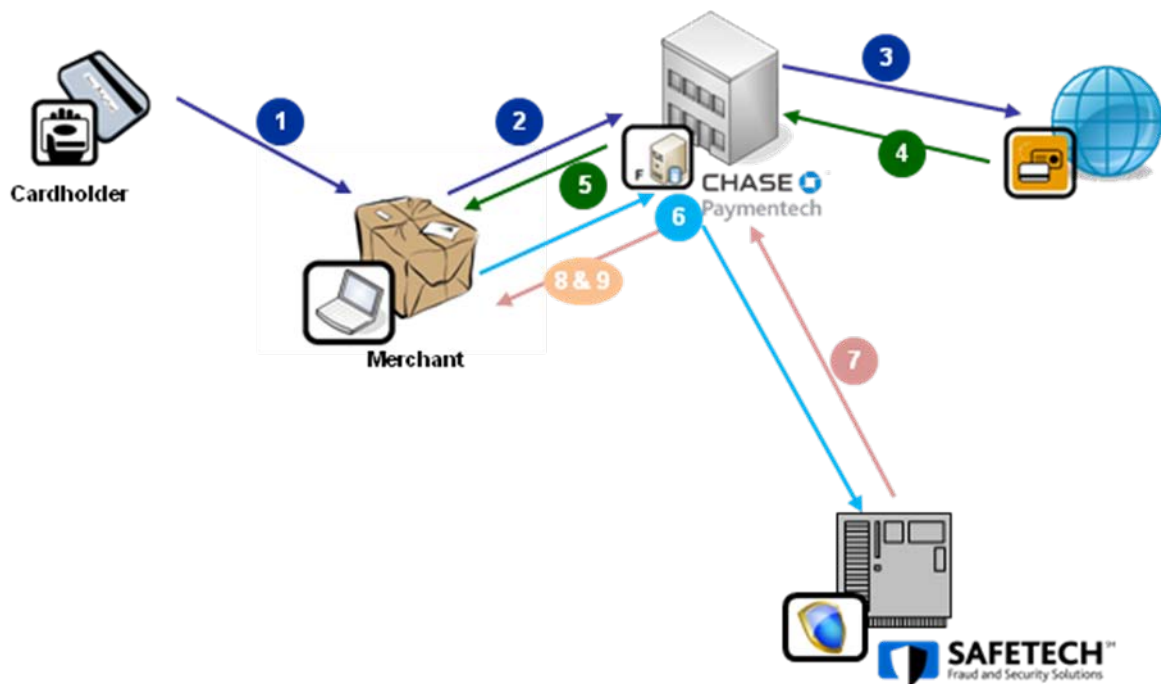
1. Customer makes a purchase at merchant's website or call center
2. The merchant requests an Authorization coupled with a Fraud Score
3. CPS will send the transaction to the issuing bank for an Authorization and AVS/CVV response
4. Once the bank responds with an Authorization or Decline the order is automatically sent to Safetech for scoring
5. Safetech analyzes any device details with the transaction information, provides a Score and runs the transactions through the Rules Engine
6. CPS responds to the merchant with both the credit card response as well as the Safetech score and recommended action
7. The merchant determines whether or not to accept the order or decline the order
8. If the merchant declines the order, they need to submit an authorization reversal on the credit card

Stand Alone Safetech Score Request Followed by Authorization



1. Customer makes a purchase at merchant's website or call center
2. The merchant requests a standalone Fraud Score Request (this request will be missing the AVS and CVV response codes)
3. Safetech analyzes any device details with the transaction information, provides a Score and runs the transactions through the Rules Engine
4. CPS sends the merchant the Safetech details
5. Since no credit card authorization was requested, the merchant can determine if they want to send the transaction through for a credit card authorization or simply cancel the order based on the response from Safetech
6. If the transaction is Approved by Safetech the merchant can request a standalone authorization request
7. CPS will send the transaction to the issuing bank for an Authorization and AVS/CVV response
8. The bank provides an Authorization or Decline along with AVS and CVV response code
9. CPS sends the merchant the credit card details. The merchant determines whether or not to accept the order or decline the order. If the merchant declines the order, they need to submit an authorization reversal on the credit card

Stand Alone Authorization Request Followed by Safetech Score



1. Customer makes a purchase at merchant's website or call center
2. The merchant requests a standalone credit card authorization request
3. CPS will send the transaction to the issuing bank for an Authorization and AVS/CVV response
4. The bank provides an Authorization or Decline along with AVS and CVV response codes
5. If the card is Approved by the issuing bank
6. The merchant then sends a standalone fraud request (the merchant will need to send the AVS and CVV responses as well, using a User Defined Field)
7. Safetech analyzes any device details with the transaction information, provides a Score and runs the transactions through the Rules Engine
8. CPS sends the merchant the Safetech details
9. The merchant determines whether or not to accept the order or decline the order

FAQs

Who Do I Call?

During Certification and Testing:

- For questions regarding Chase Paymentech message specifications prior to certification call:
 - Technical Consulting (Tech C)
 - Your Assigned Technical Consulting Representative
- For questions and issues during the message certification process call:
 - Merchant Certification (MCert)
 - Your Assigned Integration Consultant
- For questions and issues related to the Web Console; Fraud Rule Definition; and Monitoring and Reporting call:
 - Your Safetech Fraud Tools Advisor

In Production, within 60 days of going “live” with Safetech Fraud Tools (30 days for Safetech Express Users):

- For technical questions and urgent after-hours support:
 - If using the Orbital Gateway or Spectrum SDK, contact Advanced Product Support (APS) at 1.866.645.1314
 - If sending transactions direct to the Stratus Mainframe contact Salem Operations at 1.800.228.7782
- For AWC and rule-related questions during business hours:
 - Contact your Assigned Safetech Fraud Advisor
- For AWC and rule-related questions after business hours:
 - Contact the Safetech Fraud Tools Advisory Department via email at PTI-SafetechFraud@ChasePaymentech.com

In Production, after 60 days of going “live” with Safetech Fraud Tools (30 days for Safetech Express Users):

- For technical questions and urgent after-hours support:
 - If using the Orbital Gateway or Spectrum SDK, contact Advanced Product Support (APS) at 1.866.645.1314
 - If sending transactions direct to the Stratus Mainframe, contact Salem Operations at 1.800.228.7782
- For AWC and rule-related questions during and after business hours:
 - Contact the Safetech Fraud Tools Advisory Department via email at PTI-SafetechFraud@ChasePaymentech.com

Continued on next page

Frequently Asked Questions

What if I lose my Password?

If you've misplaced your password for the Product instance of the web console, please visit <https://safetech.chasepaymentech.com/login.html> and click **Lost Password**. You will then be prompted to input the email address used when your account was created. This email address is your login name. After submitting, you will receive an email from Safetech with a link and instructions to re-set your password.

For the Test instance of the web console please visit <https://safetechtest.chasepaymentech.com/login.html> and click Lost Password.

What if my login isn't working?

If you've misplaced your login credentials or are locked out, please see your direct manager. They can unlock your account within the web console.

What is GEOX?

The GEOX indicator is an ISO Country Code that represents the country with the highest level of known e-commerce risk (as determined by the U.S. State Dept.) that has been **associated** to a particular **persona** within the last 14 days. The GEOX is not the same as the physical device location, but rather an indication of where the associated persona has been seen.

Why did an order receive the score it did?

The score is based upon over 200 criteria associated to the order (payment implement, email address, order info) as well as the attributes and settings of the physical device placing the order. The score is derived during an analysis of these elements through a proprietary mathematical algorithm and is our indication of the risk level for a particular transaction from 1-99, with 99 being the most risk. Please see additional information above under the Safetech Fraud Score section.

How is the score created?

The score is based upon multiple criteria associated to the order (payment implement, email address, order info) as well as the attributes and settings of the physical device placing the order. The score is derived during an analysis of these elements through a proprietary mathematical algorithm and is our indication of the risk level for a particular transaction from 1-99 with 99 being the most risk. Please see additional information above under the Safetech Fraud Score section.

Continued on next page

Frequently Asked Questions, Continued

How do I add a value to one of the VIP Lists?

There are two methods in which values can be added to the VIP List based upon a user's permissions.

1. The first and simplest method is to add the value while reviewing a Suspect Order in the Transaction Details page of the Web Console in the Workflow. The Email Address; Credit Card; Billing/Shipping Address each have two small icons on their respective header rows. By enabling either of these icons, the data value will be placed upon the corresponding VIP list for either the "Review" or "Decline" action. To switch a value for a different action, simply select the icon desired. To remove an item from the VIP List, select the icon highlighted once again and the value will be removed.
2. If your personal permissions allow, you may access the Fraud Tab of the Web Console and select the VIP Lists Options. You will see the options listed for Email; Card; Addresses. Each category has its own input page and upon accessing the respective page, you will input the data value, select the appropriate action and save.

Why was Kaptcha/Data Collector data missing on an order?

From time to time, Kaptcha/Data Collector data may not be received on an order due to either a time-out related issue or browser settings of a user. Kaptcha/Data Collector is not gathered on Phone or Customer Service Orders

What happens when there's no Kaptcha/Data Collector data?

Orders without associated Kaptcha/Data Collector data may impact which rules trigger as without Kaptcha data, device-related information will not be determinable and the score will also be impacted. The order may still be reviewed and depending upon the nature of the order, additional validation steps may be warranted.

What is a persona?

A persona is created when the details of an order and device are evaluated together. By creating this persona, we will determine attributes which are the same and begin linking orders across the entire database even if multiple emails, names or credit cards are in use.

Continued on next page

Frequently Asked Questions, Continued

What is a device fingerprint?

The device fingerprint is a calculated value derived from the variations device layers associated to the physical device. The mathematical equation used to create the fingerprint analyzes each layer and calculates the fingerprint, which can then be utilized with persona technology and order linking.

How can I see Linked Orders?

When orders within your merchant account have been linked to the same device fingerprint or persona, the **Persona Orders** button will appear on the transaction details page of the order you're viewing. By selecting this button, a listing of any linked orders will appear for your review/action/investigation. Orders will remain linked for up to 14 days.

How can I tell why orders were linked?

Oftentimes the reason for order linking may be obvious as the consumer used the details (email, credit card, name, etc.) for all of the linked orders. But in many cases, it will not be obvious and you may want to look at the device fingerprint associated to the multiple orders. Remember to review the Link Analysis section located on the Transaction Details page to find related orders.

Why is an order no longer showing as linked?

Orders will remain linked for 14 days maximum. At that time, they are de-coupled.

How can I tell if this order was placed from a mobile or handheld device?

Within the Extended Variables section of the Risk Evaluation on the Transaction Details page, there will be listings for whether or not a device was of a mobile nature (Apple – Ipad; Iphone; Droid).

What does the time zone represent?

The time zone represents the number of minutes from Greenwich Meantime that the physical devices time zone setting is configured for. By dividing the number listed by 60, you can determine the number of hours from GMT and then review to see if it seems reasonable based upon the addresses, device location, etc.

Continued on next page

Frequently Asked Questions, Continued

What is the HTTP Country?

The HTTP country is the country designated in the device's control panel configuration. This is not the same as the Device Location country that represents the actual physical location.

What are Extended Variables?

Extended Variables are elements of the persona and physical device and can often be helpful when evaluating an order. The Extended Variables are found in the Risk Evaluation section of the Transaction Details page.

How can I see which rules or thresholds triggered on an order?

You will find the Rules Triggered in the Rules Triggered gadget on the Transaction Details page of the order.

Can a customer edit information on an order and re-submit and receive a new score?

Unfortunately, an order cannot be re-submitted by the consumer if they've input incorrect data. A new order would be required for processing. However, you can re-evaluate an order within a 14-day window should you wish to get an update/immediate re-score.

Why didn't my rule updates get saved?

Please note that this question does NOT apply to Safetech Express Users.

When creating or editing a rule, you must save your work on the specific rule and then when you return to the master rules list, you must save the updated rules list as well in order for your updates to be maintained. At that time, you'll have the option to Activate the newly saved rule set. You must Save the Rule, Save the Rule Set and Active the Rule Set for the rule to be active on any new transactions.

Continued on next page

Frequently Asked Questions, Continued

How do I edit a rule?

Please note that this question does NOT apply to Safetech Express Users.

Once you've accessed the current rule set, you simply click on the 'conditions' of the rule as displayed. This action will take you to the rules engine page where you can make any edits, etc. as needed. Remember to save your edits as well as the updated rule set and Active the rule set too. Some edits to rules (enable, disable, delete) can occur from the main rule set page.

Can I have more than one rule set active?

Please note that this question does NOT apply to Safetech Express Users.

There can only be one active rule set at any given time.

How do I activate another rule set?

Please note that this question does NOT apply to Safetech Express Users.

To activate a new rule set, simple access the Fraud Control Tab and select the **Rule Sets List** option from the dropdown menu. You will be presented with the library of Rule sets to select from. Select the rule set desired and follow the prompts to Activate.

How can I see a report of transactions processed?

Please note that this question does NOT apply to Safetech Express Users.

Depending upon your level of access and permission, you may be able to create an AdHoc or utilize the Datamart reporting feature. If you do not have access, please see your manager.

What does it mean when some scores are highlighted orange?

Scores which are highlighted in orange are indicating that the original reply SCORE has changed. By accessing an order which shows a highlighted score, refer to the History section at the bottom of the transaction details page. Here you will see the history of any score changes and other actions taken or processed on an order.

Continued on next page

Frequently Asked Questions, Continued

Where can I see the most current score of an order?

The score displayed on the Suspect Orders queue page will always be the most current score. When reviewing an order and from the Transactions Details page, the most current score will appear in the History section at the bottom portion of the page.

How do I assign orders to Agents?

If your personal access allows, you may assign orders to specific individuals or agents to work and appear in their specific workflow queue. In order to assign orders in bulk, from the Suspect Orders page, filter the results to your liking, then select the orders you wish to assign. From the drop down menu at the bottom of the page, select the agent's initials, input a note (optional), and then click "Apply Changes" (Note: Do not make any selection/changes to the "STATUS" drop down). Those orders will now appear in that agent's queue upon their next login.

Can I add a note to an order?

To add a note to an order, from the Transaction Details page, access the Notes Section at the bottom of the page. Input your note (it will be public for all to see) and then select Save.

What is "Re-evaluate" Button?

Re-evaluate button will allow a user to process the order again to see if any additional rules have triggered and also return a most current score. The use of Re-evaluate risk is infrequent, but can be useful to determine if new rules have been triggered. There is an additional fee for each re-evaluation.

Do you validate email addresses?

Due to anti-spam laws, we are unable to validate that an email address has been issued validly and can verify the data or string submitted conforms with standard email protocol structure.

Continued on next page

Frequently Asked Questions, Continued

What is a proxy server?

A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server requesting some service (such as a file, connection, web page, or other resource) available from a different server. The proxy server evaluates the request according to its filtering rules. Proxies can be used by legitimate consumers as well as fraudsters alike. This software package allows any user to select random IP addresses for specified ZIP codes or regions of their choosing. Fraudsters can utilize over-the-counter proxy server technologies or create custom applications designed to hide their true location from detection. It's not uncommon for fraudsters to use schools, prisons, hospitals, airports or other anonymous locations as the focal point for their transactions.

What is a Website ID?

Please note that this question does NOT apply to Safetech Express Users.

Merchant created site identifier allowing merchant to segregate and identify orders based upon such things as site, type, location, etc. Also can be used in rule creation and qualifying your line of business. An example is a website id for your US business, UK, Canada or B2B or B2C.

What is Shopping Cart data?

Merchant product, sku, quantity and amount of items purchased on the transaction. You can send through this data which will allow you the ability to create rules around high risk product.

What is a User Defined Field (UDF)?

Please note that this question does NOT apply to Safetech Express Users.

Merchant created custom datafields. You can use these data fields to send through additional information. These fields will be available on the Transaction Details page as well as allow you the ability to create rules with these elements.

What is Melissa Data?

This is a service from the USPS for address normalization and validation. On the Transaction Details page you will see the normalized address along with Melissa Data Reason Codes if the address was modified during the normalization process. These reason codes can be used to create custom rules.

Continued on next page

Frequently Asked Questions, Continued

How do I receive scoring on my Phone Orders from my Call Center or Customer Service teams?

Be sure to include data in the CustomerANI field with each transaction or you may pass a default value of 01233456789

How does Kaptcha/Data Collector work on phone orders?

Does your customer service or sales team use the same online site to place orders? If yes.....be sure you do NOT send Kaptcha/Data Collector on those phone orders. Please refer to the Kaptcha/Data Collector specifications for additional details.

Risk Evaluation Field Definitions

Field	Definition
GEOX	The country with the highest level of e-commerce risk associated to this persona in the last 14 days
NETW	The riskiest network type associated to the persona in the last 14 days. (Normal, Proxy, Satellite, Anonymous, Library, Prison, High School)
SCOR	The result of the evaluation of the order which will range from 1 – 99, with 99 being considered very high risk.
VELO	The quantity of unique orders seen from this persona in the last 14 days.
VMAX	The quantity of unique orders seen from this persona in the most recent 6-hour period.

Description of Delivered Data

Basic Device and Network Variables:

Key	Description
DEVICE_LAYERS	<p>Each layer is ten characters long and may be absent if a specific layer could not be gathered. The five device layers in this field, separated by periods, represent five general queries from Chase Paymentech to the device that identify different properties or characteristics of the device. While each layer contains a number of attributes, in general, you can consider them as follows:</p> <ol style="list-style-type: none">1. Network/OS/SSL - Network, OS, and SSL layers return very definite information.2. Flash - Flash layer queries the device to determine if it is Flash capable and if so, gathers device data via Flash.3. JavaScript - The JavaScript layer queries the device to determine if it is JavaScript capable and if so, gathers device data via JavaScript.4. HTTP - HTTP layer queries HTTP headers for a number of device associated data.5. Browser - The Browser layer queries the high-level web browser to collect information about the browser such as the user-agent string and type of browser.
FINGERPRINT	<p>A 32-character hash that represents numerous system identifiers. This value is considered a constant for a particular device, despite user attempts to change values in any particular device layer.</p>
TIMEZONE	<p>Time zone of the customer as a 4 digit number indicating the offset in minutes from GMT</p>

Continued on next page

Description of Delivered Data, Continued

Basic Device and Network Variables, continued:

Key	Description																																	
LOCALTIME	The format YYYY-MM-DD HH:MM is used for local time on the device																																	
REGION	Returns the estimated region of the customer in USPS format for the U.S. and Canada and FIPS 10-4 region code for all other countries																																	
COUNTRY	A two-character code such as US indicating the country where the computer user is operating																																	
PROXY	Is the end device using a proxy? (Y/N)																																	
JAVASCRIPT	Does the end device's browser allow JavaScript? (Y/N)																																	
FLASH	Does the end device's browser allow Flash? (Y/N)																																	
COOKIES	Does the end device's browser allow cookies? (Y/N)																																	
HTTP_COUNTRY	A two-character country code such as US set by the user for the device.																																	
LANGUAGE	A two-character code such as EN indicating the language preference of the computer's user.																																	
MOBILE_DEVICE	Is the end device a mobile device? (Y/N)																																	
MOBILE_TYPE	Identifies the specific type of mobile device: <table border="0" style="margin-left: 40px;"> <tr> <td>Android</td> <td>MMP</td> <td>Pocket</td> </tr> <tr> <td>AvantGo</td> <td>MOT_RAZR</td> <td>SonyEricsson</td> </tr> <tr> <td>BlackBerry</td> <td>MobilePhone</td> <td>Symbian</td> </tr> <tr> <td>ELNK-TA-WIN</td> <td>Motorola</td> <td>Treo</td> </tr> <tr> <td>Hiptop</td> <td>NetFront</td> <td>UP.BROWSER</td> </tr> <tr> <td>iPad</td> <td>Nokia</td> <td>UP.LINK</td> </tr> <tr> <td>iPhone</td> <td>Opera Mini</td> <td>Vodafone</td> </tr> <tr> <td>iPod</td> <td>PDA</td> <td>WAP2.0</td> </tr> <tr> <td>Kindle</td> <td>Palm</td> <td>Windows CE</td> </tr> <tr> <td>LG-LG/</td> <td>PlayStation Portable</td> <td></td> </tr> <tr> <td>MIDP</td> <td>Pluckerm</td> <td></td> </tr> </table>	Android	MMP	Pocket	AvantGo	MOT_RAZR	SonyEricsson	BlackBerry	MobilePhone	Symbian	ELNK-TA-WIN	Motorola	Treo	Hiptop	NetFront	UP.BROWSER	iPad	Nokia	UP.LINK	iPhone	Opera Mini	Vodafone	iPod	PDA	WAP2.0	Kindle	Palm	Windows CE	LG-LG/	PlayStation Portable		MIDP	Pluckerm	
Android	MMP	Pocket																																
AvantGo	MOT_RAZR	SonyEricsson																																
BlackBerry	MobilePhone	Symbian																																
ELNK-TA-WIN	Motorola	Treo																																
Hiptop	NetFront	UP.BROWSER																																
iPad	Nokia	UP.LINK																																
iPhone	Opera Mini	Vodafone																																
iPod	PDA	WAP2.0																																
Kindle	Palm	Windows CE																																
LG-LG/	PlayStation Portable																																	
MIDP	Pluckerm																																	
MOBILE_FORWARDER	Does the mobile device's wireless application protocol indicate the use of mobile forwarding? (Y/N)																																	
VOICE_DEVICE	Is the device voice controlled? (Y/N)																																	
PC_REMOTE	Is the device a remotely controlled computer? (Y/N)																																	

Continued on next page

Description of Delivered Data, Continued

Multi-Merchant Variables and Other Variables:

Key	Description
SCOR*	Risk Score (1-99).
GEOX*	The worst (highest risk) country associated with the customer in the last 14 days.
REGN*	The worst (highest risk) estimated region associated with the customer in the last 14 days. USPS format for the U.S. and Canada and FIPS 10-4 region code for all other countries.
DEVICES*	Number of devices associated with the customer in the last 14 days.
CARDS*	Number of cards associated with the customer in the last 14 days.
EMAILS*	Number of emails associated with the customer in the last 14 days.
VELO	Total number of prior sales by this customer in the last 14 days.
VMAX	Total number of prior sales by this customer in any 6-hour window over the last 14 days.
NETW*	The worst (highest risk) Network Type associated with this customer in the past 14 days: N - Normal L - Library H - High School P - Prison O - Open Proxy A - Anonymous S - Satellite
KAPT	Indicates if a RIS record has a corresponding Kaptcha record, (Y/N) a value of "N" may be a sign of deception.
BRND	Payment Method Brand: AMEX - American Express DNRS - Diners Club GDMP - GreenDotMoneyPak MSRO - Maestro SOLO - Solo VISA - Visa AUBC - Australian Bankcard CHEK - Check CHIN - China Pay DISC - Discover JCB - JCB International MSTR - MasterCard SWCH - Switch VISE - Visa Electron PYPL - Paypal UNKN - Other

() Indicates the value is a Multi-Merchant variable calculated across the entire Chase Paymentech client base. For example, a CARDS value of 12 means Chase Paymentech has observed this customer attempting to use 12 different cards across all merchants in the last 14 days.*