PROPAY® FRAUD SOLUTIONS

Instructions for Guardian Cyber Shield

PROPAY®
A TSYS® Company

1.0 Guardian Cyber Shield General Information

ProPay offers integration opportunities to various fraud prevention solutions to help prevent Merchants from accepting fraudulent credit cards and/or known fraudulent bank accounts. A special FraudDetectors object is used to pass along credentials and additional provider-specific information to the fraud prevention provider. Please note that improperly configured credentials or invalidly-formatted request objects can result in transactions not being completed at all. It is important to have properly tested the solution and confirmed your credentials or account have been enabled for a specific provider before attempting live transactions.

Fraud Detector Compatible Methods

The following ProPay API Methods are compatible with the FraudDetectors object

- Credit Card Authorization Transaction
- Process a Credit Card Transaction
- Process an ACH Transaction
- Refund an ACH Transaction
- ProPay SplitPay Transaction

The following ProtectPay API Methods are compatible with the FraudDetector object

- Authorize a Payment Method
- Authorize a Payment Method (Recurring)
- Authorize a Payment Method with Encrypted Block Data
- Process a Payment Method
- Process a Payment Method (Recurring)
- Process a Payment Method with Encrypted Block Data
- Process a Credit Transaction
- ProPay SplitPay Transaction
- ProPay SplitPay Transaction with Encrypted Block Data
- Authorize External Transaction
- Process External Transaction
- Process External ProPay SplitPay Transaction
- Process a Credit Card

1.1 ThreatMetrix

ThreatMetrix profile setup

In order for a customer to use the ThreatMetrix component of ProPay's Guardian Cyber Shield solution, they must first be set up By ProPay for its use. Once a contract has been established for this feature, ProPay will supply you with a ThreatMetrix username and password. You may then log into the ThreatMetrix Portal and set up a profiles used to govern the settings that decide when a transaction is to be considered fraudulent. (Don't worry, a default profile is created for you.)

ThreatMetrix Portal URI: https://portal2.threatmetrix.com
For additional information on setting up risk profiles please see:
https://kb.threatmetrix.com/index.php?View=login&Msg=_index

ThreatMetrix Widget inclusion

The ThreatMetrix website provides access to a hidden JavaScript widget that you are expected to place on your website. This widget will gather information about the computer accessing your website and send it to ThreatMetrix. Your own page should pass a couple of data points into the JavaScript:

- Organization ID: This is a generic value provided to you by ProPay
- Session ID: This is your own unique identifier. You will also pass this value into the ProPay boarding API.

```
<head>
    <script type="text/javascript"
        src="https://h.online-metrix.net/fp/tags.js?org_id=4uw65rkp&session_id=01f50c4d1430a620a3b50005ffe98541">
    </script>
</head>In the body of your page, you should include the following:
</body>
  <noscript>
    <iframe style="width: 100px; height: 100px; border: 0; position: absolute; top: -5000px;"
      src="https://h.online-metrix.net/fp/tags?org_id=abcd1234&session_id=01f50c4d1430a620a3b50005ffe98541">
    </iframe>
  </noscript>
</body> org_id will usually be '4uw65rkp' (However, in some special cases, ProPay may elect to provide partners with their own org_id.)
```

** session_id should be a value that you generate to uniquely identify an individual transaction. It should consist of: Upper and lowercase English letters (a-z, A-Z), Digits (0-9), Underscore (_), and Hyphen (-)

ThreatMetrix – passing the same data to ProPay

Then, in your processing request to ProPay, you should pass data that acts as a "callback" to what you originally passed into the ThreatMetrix widget. ProPay will check the ThreatMetrix system, and block what ThreatMetrix describes (according to your profile) it considers fraudulent.

ThreatMetrix Additional Elements

Only the required elements are necessary when you use the default ThreatMetrix profile. If you decide that you want to establish controls using some of these other elements, feel free.

Element	Type	Max	Required	Notes
FraudDetectorProvider	String		Required	Set to: ThreatMetrix
SessionId	String		Required	Created by merchant and sent to ThreatMetrix prior to transaction
InputIpAddress	String		Required	Sent by merchant to ThreatMetrix prior to transaction
ShippingAddress1	String		Optional	
ShippingAddress2	String		Optional	
ShippingCity	String		Optional	
ShippingState	String		Optional	
ShippingZip	String		Optional	
ShippingCountry	String		Optional	

CustomAttribute1	String		Optional	Must exist as part of the Organization Id prior to being passed
CustomAttribute2	String		Optional	Must exist as part of the Organization Id prior to being passed
CustomAttribute3	String		Optional	Must exist as part of the Organization Id prior to being passed
CustomAttribute4	String		Optional	Must exist as part of the Organization Id prior to being passed
CustomAttribute5	String		Optional	Must exist as part of the Organization Id prior to being passed
CustomAttribute6	String		Optional	Must exist as part of the Organization Id prior to being passed
CustomAttribute7	String		Optional	Must exist as part of the Organization Id prior to being passed
CustomAttribute8	String		Optional	Must exist as part of the Organization Id prior to being passed
CustomAttribute9	String		Optional	Must exist as part of the Organization Id prior to being passed
CustomAttribute10	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute1	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute2	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute3	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute4	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute5	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute6	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute7	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute8	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute9	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute10	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute11	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute12	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute13	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute14	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute15	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute16	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute17	String		Optional	Must exist as part of the Organization Id prior to being passed

ConditionalAttribute18	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute19	String		Optional	Must exist as part of the Organization Id prior to being passed
ConditionalAttribute20	String		Optional	Must exist as part of the Organization Id prior to being passed
ACHAccountHash	String		Optional	Do not use at this time
CreditCardNumberHash	String		Optional	Do not use at this time
DriversLicenseHash	String		Optional	Do not use at this time
SocialSecurityNumberHash	String		Optional	Do not use at this time

Sample: ProPay API

<ArrayOfFraudDetector xmlns="FraudDetectors">
<FraudDetector xsi:type="ThreatMetrixFraudDetection">
<FraudDetectorProviderName>ThreatMetrix</FraudDetectorProviderName>
<InputIpAddress>8.8.8.8</InputIpAddress>
<SessionId>08a3958c-f2f5-43ad-b171-9de35633ff68e</SessionId>
</FraudDetector>
</ArrayOfFraudDetector>

Sample: ProtectPay REST

"FraudDetectors":[{
"ThreatMetrixFraudDetection":{
"FraudDetectorProviderName":"ThreatMetrix",
"SessionId":"08a3958c-f2f5-43ad-b171-9de35633ff68",
"InputIpAddress":"8.8.8.8",
}}]

Sample: ProtectPay SOAP

<typ:FraudDetectors xmlns:fraud="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection">
<fraud:FraudDetector xmlns:threatmetrix="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers"
i:type="threatmetrix:ThreatMetrixFraudDetection">
<fraud:FraudDetectorProviderName>ThreatMetrix</fraud:FraudDetectorProviderName>
<fraud:InputIpAddress>8.8.8.8</fraud:InputIpAddress>
<threatmetrix:SessionId>08a3958c-f2f5-43ad-b171-9de35633ff68</threatmetrix:SessionId>
</fraud:FraudDetector>
</typ:FraudDetectors>

1.2 Amex Enhanced Auth

American Express Enhanced Authorization Setup

ProPay must enable merchants who wish to use American Express Enhanced Authorization using one of our provided merchant accounts. Please refer requests to setup a ProPay Merchant Account for Amex Enhanced Auth to: riskescalation@propay.com

Amex Enhanced Auth Processing flow

You should send as much of the data that Enhanced authorization accepts that is feasible for you to collect. The value provided by this solution is dependent, almost entirely, on how much information you can provide to it. While many of the fields listed below are described as optional. Forgoing their collection will cause that this feature provides you with diminished value.

Enhanced auth causes the ProPay system to send an extra message to American Express during a "normal processing flow", and you don't need to change the way your system works beyond the gathering of additional data that you provide to ProPay. Any fraud caught using the Enhanced Auth steps that will simply result in a decline by the processing system. There are a few extra response codes specific to Enhanced auth, and those are listed in this document's appendix.

American Express Enhanced Authorization only works for American Express cards.

Amex Enhanced Auth Specific Attributes

Attribute	Type	Max	Required	Notes
FraudDetectorProviderName	String		Required	Set to: AmexEnhancedAuth
InputIpAddress	String		Optional	
ShippingMethod	String		Optional	
ShippingPhoneNumber	String		Optional	
ShippingAddress1	String		Optional	
ShippingAddress2	String		Optional	
ShippingCity	String		Optional	
ShippingState	String		Optional	
ShippingZip	String		Optional	
ShippingCountry	String		Optional	

Sample: ProPay API

```
<ArrayOfFraudDetector xmlns="FraudDetectors">
        <FraudDetector xsi:type="AmexEnhancedAuth">
                <FraudDetectorProviderName>AmexEnhancedAuth</FraudDetectorProviderName>
                  <InputIpAddress>8.8.8.8</InputIpAddress>
                  <ShippingAddress1>123 Main Street</ShippingAddress1>
                 <ShippingAddress2> </ShippingAddress2>
                 <ShippingCity></ShippingCity>
                 <ShippingState></ShippingState>
                 <ShippingZip></ShippingZip>
                <ShippingCountry></ShippingCountry>
                 <ShippingFirstName></ShippingFirstName>
               <ShippingLastName></ShippingLastName>
              <ShippingPhoneNumber></ShippingPhoneNumber>
             <ShippingMethod>02</ShippingMethod>
        </FraudDetector>
</ArrayOfFraudDetector>
```

Sample: ProtectPay REST

```
"FraudDetectors":[ {
                        "AmexEnhancedAuth":{
                                    "FraudDetectorProviderName":"AmexEnhancedAuth",
                                    "ShippingMethod":"1",
                                       "InputIpAddress":"8.8.8.8",
                                     "ShippingAddress1":"",
                                     "ShippingAddress2":"",
                                     "ShippingCity":"",
                                     "ShippingState":"",
                                     "ShippingZip":"",
                                     "ShippingCountry":"",
                                   "ShippingPhoneNumber":""
                        } } ]
```

Interface: ProtectPay SOAP

```
<typ:FraudDetectors xmlns:fraud="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection">
            <fraud:FraudDetector
xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers" i:type="amex:AmexEnhancedAuth">
                        <fraud:FraudDetectorProviderName>AmexEnhancedAuth</fraud:FraudDetectorProviderName>
                           <fraud:InputIpAddress i:nil="true" />
                           <fraud:ShippingAddress1 i:nil="true" />
                           <fraud:ShippingAddress2 i:nil="true" />
                           <fraud:ShippingCity i:nil="true" />
                           <fraud:ShippingCountry i:nil="true" />
                           <fraud:ShippingFirstName i:nil="true" />
                          <fraud:ShippingLastName i:nil="true" />
                         <fraud:ShippingPhoneNumber i:nil="true" />
                           <fraud:ShippingState i:nil="true" />
                           <fraud:ShippingZip i:nil="true" />
                      <amex:ShippingMethod>02<amex:ShippingMethod>
            </fraud:FraudDetector>
</typ:FraudDetectors>
```

Appendix: Guardian Cyber Shield-specific Response Codes

The following response codes are returned as either the ProPay API's <status> value or in ProtectPay's [RequestResult] object.

Threat Metrix Status Codes Returned by Fraud Systems

Code	Message	Transaction Status
00	Success	Processed
133	Threat Metrix Score Threshold Met	Decline
353	Session Id is an invalid it should only contain upper and lowercase characters, digits, underscores and hyphens.	Failure
354	Nonexistent account configured for ThreatMetrix on our system.	Failure

Amex Enhanced Auth Status Codes Returned by Fraud Systems

Code	Message	Transaction Status
00	Success	Processed
355	Amex fraud solution invalid account configuration	Failure