## 1.0 Processing Fraud Prevention

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.

## FraudDetector Compatible Methods

The following ProPay API Methods are compatible with the FraudDetectors object

- 4.3.2 Credit Card Authorization Transaction
- 4.3.4 Process a Credit Card Transaction
- 4.3.5 Process an ACH Transaction
- 4.3.7 Refund an ACH Transaction
- 4.4.3 ProPay SplitPay Transaction

The following ProtectPay API Methods are compatible with the FraudDetector object

- 4.4.1 Authorize a PaymentMethodId
- 4.4.2 Authorize a PaymentMethodId (Recurring)
- 4.4.3 Authorize a PaymentMethodId with Encrypted Block Data
- 4.5.1 Process a PaymentMethodId
- 4.5.2 Process a PaymentMethodId (Recurring)
- 4.5.3 Process a PaymentMethodId with Encrypted Block Data
- 4.6.3 Process a Credit Transaction
- 4.9.1 ProPay SplitPay Transaction
- 4.9.2 ProPay SplitPay Transaction with Encrypted Block Data
- 4.10.1 Authorize External Transaction
- 4.10.2 Process External Transaction
- 4.10.3 Process External ProPay SplitPay Transaction
- 4.10.4 Process a Credit Card

## FraudDetectors Base Object

| Request Object | Inherited Elements |
|---|---|
| **FraudDetectors** | FraudDetectorProviderName |
| | InputIpAddress |
| | ShippingPhoneNumber |
| | ShippingAddress1 |
| | ShippingAddress2 |
| | ShippingCity |
| | ShippingState |
| | ShippingZip |
| | ShippingCountry |
| | * Specific Attributes for Fraud System Provider |

## Using multiple fraud detection providers

When using multiple providers, a FraudDetector array must be created with each element of the array being a FraudDetector object of the specific namespace used to reference the correct elements for the provider.

- If submitting multiple Fraud Providers the order of precedence is
    1. ThreatMetrix
    2. Amex Enhanced Auth
    3. ProPay Fraud Detection

## Interface: ProPay Legacy XML

The FraudDetectors object is passed as the namespace of a new `<ArrayOfFraudDetector>` child element of the `<FraudDetector>` Element of the `<XMLTrans>` object of a ProPay Legacy XML Request. Each provider has its own required namespace as seen below.

### Sample XML Request Structure:

```
<XMLTrans>
        <-- Specific Elements for the ProPay API Request -->
        <FraudDetector>
                <ArrayOfFraudDetector xmlns="FraudDetectors">
                        <FraudDetector xsi:type="ThreatMetrixFraudDetection">
                                <FraudDetectorProviderName>ThreatMetrix</FraudDetectorProviderName>
                                <-- Specific Elements for the Fraud System Provider -->
                        </FraudDetector>
                                <FraudDetector xsi:type="PropayFraudDetection">
                                <FraudDetectorProviderName>PropayFraudDetection</FraudDetectorProviderName>
                                <-- Specific Elements for the Fraud System Provider -->
                        </FraudDetector>
                </ArrayOfFraudDetector>
        </FraudDetector>
</XMLTrans>
```

## Interface: ProtectPay REST

The FraudDetectors object is passed in the parent object for REST methods.

```
"FraudDetectors":[
        {
                "ThreatMetrixFraudDetection":{
                        "FraudDetectorProviderName":"ThreatMetrix",
                        /* Specific Elements for Fraud System Provider */
                },
                "AmexEnhancedAuth":{
                        "FraudDetectorProviderName":"AmexEnhancedAuth",
                        /* Specific Elements for Fraud System Provider */
                },
                "PropayFraudDetection":{
                        "FraudDetectorProviderName":"PropayFraudDetection",
                        /* Specific Elements for Fraud System Provider */
                }
        }
],
```

## Interface: ProtectPay SOAP

The FraudDetectors Object itself is added to the following:

- For PaymentMethodId methods it is added to the Transaction object:

```
<con:Transaction>
    <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>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers"
    i:type="amex:AmexEnhancedAuth">
                    <fraud:FraudDetectorProviderName>AmexEnhancedAuth</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers" i:type="
    propayfraud:PropayFraudDetection">
                    <fraud:FraudDetectorProviderName>PropayFraudDetection</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
    </typ:FraudDetectors>
</con:Transaction>
```

- For EncryptedBlockData methods it is added to the AuthorizeAndCapture object:

```
<con: AuthorizeAndCapture>
    <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>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers"
    i:type="amex:AmexEnhancedAuth">
                    <fraud:FraudDetectorProviderName>AmexEnhancedAuth</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers" i:type="
    propayfraud:PropayFraudDetection">
                    <fraud:FraudDetectorProviderName>PropayFraudDetection</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
    </typ:FraudDetectors>
</con: AuthorizeAndCapture >
```

- For Create HostedTransactionIdentifier method it is added to the HostedTransaction object.

```
<con:hostedTransaction>
    <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>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers"
    i:type="amex:AmexEnhancedAuth">
                    <fraud:FraudDetectorProviderName>AmexEnhancedAuth</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers" i:type="
    propayfraud:PropayFraudDetection">
                    <fraud:FraudDetectorProviderName>PropayFraudDetection</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
    </typ:FraudDetectors>
</con: hostedTransaction >
```

- For ProPay SplitPay Transaction method it is added to the request object :

```
<con: request>
    <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>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers"
    i:type="amex:AmexEnhancedAuth">
                    <fraud:FraudDetectorProviderName>AmexEnhancedAuth</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers" i:type="
    propayfraud:PropayFraudDetection">
                    <fraud:FraudDetectorProviderName>PropayFraudDetection</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
    </typ:FraudDetectors>
```

```
</con: request>
```

- For ProPay SplitPay Transaction with Encrypted Block Data method it is added to the ProcessSplitPayTransactionWithEncryptedTrackData object :

```
<con: ProcessSplitPayTransactionWithEncryptedTrackData>
    <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>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers"
    i:type="amex:AmexEnhancedAuth">
                    <fraud:FraudDetectorProviderName>AmexEnhancedAuth</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers" i:type="
    propayfraud:PropayFraudDetection">
                    <fraud:FraudDetectorProviderName>PropayFraudDetection</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
    </typ:FraudDetectors>
</con: ProcessSplitPayTransactionWithEncryptedTrackData>
```

- For External Transaction methods it is added to the ExternalPaymentMethodTransaction object :

```
<con: externalPaymentMethodTransaction>
    <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>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers"
    i:type="amex:AmexEnhancedAuth">
                    <fraud:FraudDetectorProviderName>AmexEnhancedAuth</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers" i:type="
    propayfraud:PropayFraudDetection">
                    <fraud:FraudDetectorProviderName>PropayFraudDetection</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
    </typ:FraudDetectors>
</con: externalPaymentMethodTransaction>
```

- For External SplitPay Transaction method it is added to the ExternalPaymentMethodSplitPayTransaction object :

```
<con: externalPaymentMethodSplitPayTransaction>
    <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>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers"
    i:type="amex:AmexEnhancedAuth">
                    <fraud:FraudDetectorProviderName>AmexEnhancedAuth</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
```

```
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers" i:type="
    propayfraud:PropayFraudDetection">
                    <fraud:FraudDetectorProviderName>PropayFraudDetection</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
    </typ:FraudDetectors>
</con: externalPaymentMethodSplitPayTransaction>
```

- For Process a Credit Card method it is added to the ProcessCard object :

```
<con: ProcessCard>
    <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>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers"
    i:type="amex:AmexEnhancedAuth">
                    <fraud:FraudDetectorProviderName>AmexEnhancedAuth</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
            <fraud:FraudDetector
    xmlns:amex="http://schemas.datacontract.org/2004/07/Propay.Contracts.FraudDetection.Providers" i:type="
    propayfraud:PropayFraudDetection">
                    <fraud:FraudDetectorProviderName>PropayFraudDetection</fraud:FraudDetectorProviderName>
                    <!-- Specific Attributes for Fraud System Provider -->
            </fraud:FraudDetector>
    </typ:FraudDetectors>
</con: ProcessCard>
```

### Interface: ProtectPay WSDL

In order to properly use the FraudDetectors object by extrapolating the WSDL the specific Fraud System Provider Object must be created and set to the value of the FraudDetector.

This can be done in the following manner:

| Request Element: | Object | Attributes |
|---|---|---|
| FraudDetectors | Specific Fraud Detector Provider Obje | FraudDetectorProviderName |
| | | Attribute1 |
| | | Attribute2 |
| | | Attribute3 |
| | | … |

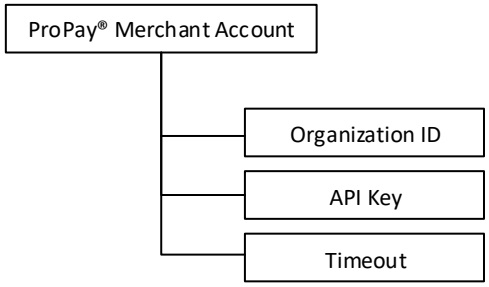
- ❖ See supported FraudDetector Providers for specific examples

## 1.1 ThreatMetrix

### ThreatMetrix Account Setup

ProPay must set up a ProPay merchant account to use ThreatMetrix. This cannot be done through the Application Programming Interface. The ThreatMetrix credentials are tied directly to the ProPay Account for ProPay's non-tokenized solution or to the ProtectPay Biller Id for ProPay's tokenized solution. Please refer requests to obtain ThreatMetrix account information to: riskescalation@propay.com

If a client has access to multiple ProPay Accounts or Biller Id's, they will have multiple ThreatMetrix Credentials




The Organization ID is the value assigned by ThreatMetrix to represent the client. It must be used to create a ThreatMetrix Session ID.

The API Key is the client's ThreatMetrix API credential that ProPay will use when sending a request to ThreatMetrix.

The Timeout value (in milliseconds) is the value the ProPay system will wait for a response from ThreatMetrix before automatically passing the transaction along to the processor. The default value set by ProPay at 2000ms, and can be adjusted by the client by request to a ProPay relationship manager. If the timeout period elapses, the transaction is passed to the processor which can create a case where a transaction was actually determined to be fraudulent, but the ThreatMetrix API responded after the timeout period elapsed.

Please work with the ProPay risk department to mitigate such occurrences and develop an appropriate resolution.

ProPay will supply the client a ThreatMetrix username and password. The client must then sign into the ThreatMetrix Portal and set up their risk profiles that are used to determine whether or not a transaction will be considered fraudulent by the client. The ProPay risk department can assist a client in determining which attributes should be set in a risk profile however it is the responsibility of the client to determine what will be considered a fraudulent transaction and what will not.

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 SessionId Creation

Prior to sending a transaction request to the ProPay or the ProtectPay API the merchant must create and send to ThreatMetrix a unique SessionId. ThreatMetrix hosts a download of an invisible iFrame that must be placed on the merchant's website prior to the checkout page. ProPay recommends the use of an order confirmation page to accomplish this prior to navigation to the final checkout page.

The ThreatMetrix iFrame requires that the appropriate organization ID be sent. The ThreatMetrix iFrame gathers information from the payer's browser and associates with the SessionId that must be passed to ThreatMetrix. It is important that this SessionId is persisted in the browser session to the final checkout page as it must be passed to ProPay in the API call.

## ThreatMetrix Processing flow

1. Merchant system creates ThreatMetrix Session ID and submits the Input IP Address of a payer's web browser.
2. Merchant system submits a ProPay API request including the related Fraud Detector tags.
    a. See Object attributes below
    b. 60 second ProPay timeout timer begins
3. ProPay submits user details to ThreatMetrix including Session ID, Input IP Address and Filter Requirements.
4. ThreatMetrix responds with score and the following messages
    a. Accept
    b. Refer

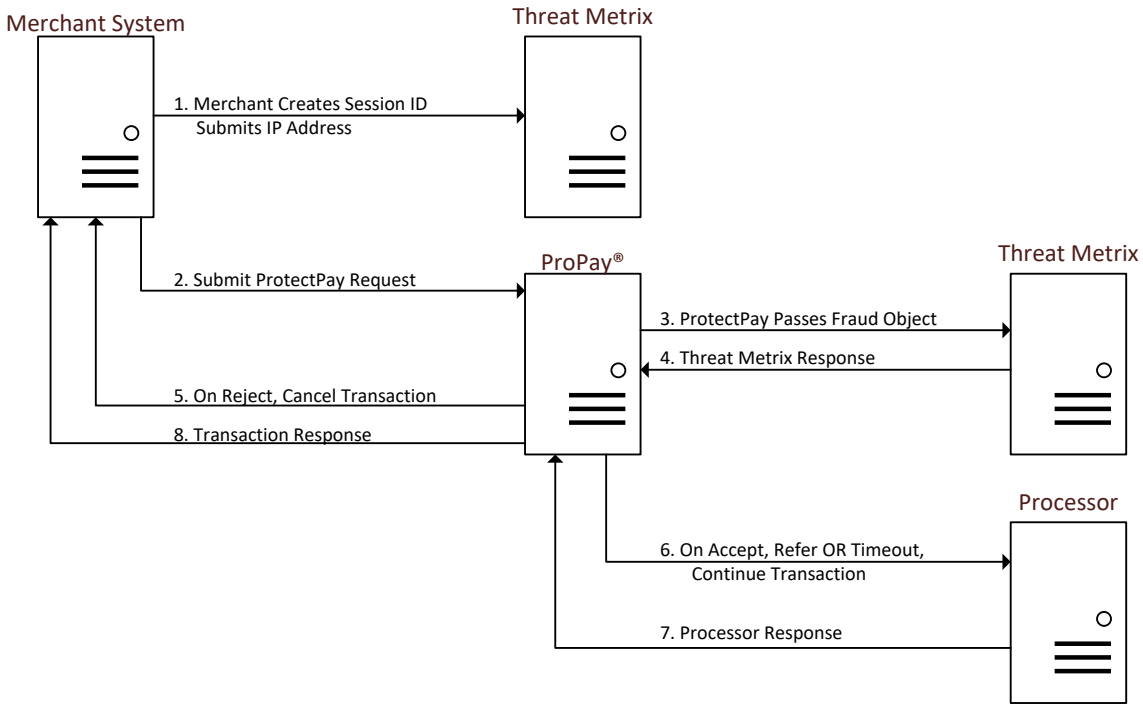
c. Reject
d. Error

5. On Reject or Error the transaction is cancelled and reported back to the Merchant with appropriate response code.
    a. See Appendix A.10 Fraud Solutions Response Codes: ThreatMetrix.
    b. The Actual Score is not returned. Please log into the ThreatMetrix Portal to view scores.
6. On Accept, Refer or at timeout the Transaction is passed to the Processor.
    a. The ThreatMetrix timeout period is part of the ProtectPay 60 second timeout and does not extend it.
    b. If ThreatMetrix responds with a "Refer" and the transaction request is successful the transaction response will be 00 with a <Response> text of "Risk Review" to indicate that the client may want to review it.
7. The Processor responds to the transaction request.
8. ProPay responds to the merchant with the transaction response.

❖ Both the SessionId and IP Address must be passed in the method, otherwise the ThreatMetrix process is ignored.

❖ **ProPay recommends as a Best Practice all ThreatMetrix transaction requests also contain a Unique Invoice be passed along with the transaction request**

## ThreatMetrix Process flow diagram




## ThreatMetrix Specific Elements

| 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 |

## Interface: ProPay Legacy XML

```
<ArrayOfFraudDetector xmlns="FraudDetectors">
        <FraudDetector xsi:type="ThreatMetrixFraudDetection">
                <FraudDetectorProviderName>ThreatMetrix</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>
                <ACHAccountHash></ACHAccountHash>
                <ConditionalAttribute1></ConditionalAttribute1>
```

```
            <ConditionalAttribute10></ConditionalAttribute10>
            <ConditionalAttribute11></ConditionalAttribute11>
            <ConditionalAttribute12></ConditionalAttribute12>
            <ConditionalAttribute13></ConditionalAttribute13>
            <ConditionalAttribute14></ConditionalAttribute14>
            <ConditionalAttribute15></ConditionalAttribute15>
            <ConditionalAttribute16></ConditionalAttribute16>
            <ConditionalAttribute17></ConditionalAttribute17>
            <ConditionalAttribute18></ConditionalAttribute18>
            <ConditionalAttribute19></ConditionalAttribute19>
            <ConditionalAttribute2></ConditionalAttribute2>
            <ConditionalAttribute20></ConditionalAttribute20>
            <ConditionalAttribute3></ConditionalAttribute3>
            <ConditionalAttribute4></ConditionalAttribute4>
            <ConditionalAttribute5></ConditionalAttribute5>
            <ConditionalAttribute6></ConditionalAttribute6>
            <ConditionalAttribute7></ConditionalAttribute7>
            <ConditionalAttribute8></ConditionalAttribute8>
            <ConditionalAttribute9></ConditionalAttribute9>
            <CreditCardNumberHash></CreditCardNumberHash>
            <CustomAttribute1></CustomAttribute1>
            <CustomAttribute10></CustomAttribute10>
            <CustomAttribute2></CustomAttribute2>
            <CustomAttribute3></CustomAttribute3>
            <CustomAttribute4></CustomAttribute4>
            <CustomAttribute5></CustomAttribute5>
            <CustomAttribute6></CustomAttribute6>
            <CustomAttribute7></CustomAttribute7>
            <CustomAttribute8></CustomAttribute8>
            <CustomAttribute9></CustomAttribute9>
            <DriversLicenseHash></DriversLicenseHash>
            <SessionId>08a3958c-f2f5-43ad-b171-9de35633ff68e</SessionId>
            <SocialSecurityNumberHash></SocialSecurityNumberHash>
        </FraudDetector>
</ArrayOfFraudDetector>
```

```
"FraudDetectors":[
        {
                "ThreatMetrixFraudDetection":{
                        "FraudDetectorProviderName":"ThreatMetrix",
                        "SessionId":"08a3958c-f2f5-43ad-b171-9de35633ff68",
                        "InputIpAddress":"8.8.8.8",
                        "ShippingAddress1":"",
                        "ShippingAddress2":"",
                        "ShippingCity":"",
                        "ShippingState":"",
                        "ShippingZip":"",
                        "ShippingCountry":"",
                        "ShippingPhoneNumber":"",
                        "ConditionalAttribute1":"",
                        "ConditionalAttribute2":"",
                        "ConditionalAttribute3":"",
                        "ConditionalAttribute4":"",
                        "ConditionalAttribute5":"",
                        "ConditionalAttribute6":"",
                        "ConditionalAttribute7":"",
                        "ConditionalAttribute8":"",
                        "ConditionalAttribute9":"",
                        "ConditionalAttribute10":"",
                        "ConditionalAttribute11":"",
                        "ConditionalAttribute12":"",
                        "ConditionalAttribute13":"",
                        "ConditionalAttribute14":"",
                        "ConditionalAttribute15":"",
                        "ConditionalAttribute16":"",
                        "ConditionalAttribute17":"",
                        "ConditionalAttribute18":"",
                        "ConditionalAttribute19":"",
                        "ConditionalAttribute20":"",
                        "CustomAttribute1":"",
                        "CustomAttribute2":"",
                        "CustomAttribute3":"",
                        "CustomAttribute4":"",
                        "CustomAttribute5":"",
                        "CustomAttribute6":"",
                        "CustomAttribute7":"",
                        "CustomAttribute8":"",
                        "CustomAttribute9":"",
                        "CustomAttribute10":"",
                        "ACHAccountHash":"",
                        "CreditCardNumberHash":"",
                        "DriversLicenseHash":"",
                        "SocialSecurityNumberHash":""
                }
        }
]
```

## Interface: 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>
                <fraud:ShippingAddress1></fraud:ShippingAddress1>
                <fraud:ShippingAddress2 />
                <fraud:ShippingCity></fraud:ShippingCity>
                <fraud:ShippingCountry></fraud:ShippingCountry>
                <fraud:ShippingFirstName i:nil="true" />
                <fraud:ShippingLastName i:nil="true" />
                <fraud:ShippingPhoneNumber i:nil="true" />
                <fraud:ShippingState></fraud:ShippingState>
                <fraud:ShippingZip></fraud:ShippingZip>
                <threatmetrix:ACHAccountHash i:nil="true" />
                <threatmetrix:ConditionalAttribute1 i:nil="true" />
                <threatmetrix:ConditionalAttribute10 i:nil="true" />
                <threatmetrix:ConditionalAttribute11 i:nil="true" />
                <threatmetrix:ConditionalAttribute12 i:nil="true" />
                <threatmetrix:ConditionalAttribute13 i:nil="true" />
                <threatmetrix:ConditionalAttribute14 i:nil="true" />
                <threatmetrix:ConditionalAttribute15 i:nil="true" />
                <threatmetrix:ConditionalAttribute16 i:nil="true" />
                <threatmetrix:ConditionalAttribute17 i:nil="true" />
                <threatmetrix:ConditionalAttribute18 i:nil="true" />
                <threatmetrix:ConditionalAttribute19 i:nil="true" />
                <threatmetrix:ConditionalAttribute2 i:nil="true" />
                <threatmetrix:ConditionalAttribute20 i:nil="true" />
                <threatmetrix:ConditionalAttribute3 i:nil="true" />
                <threatmetrix:ConditionalAttribute4 i:nil="true" />
                <threatmetrix:ConditionalAttribute5 i:nil="true" />
                <threatmetrix:ConditionalAttribute6 i:nil="true" />
                <threatmetrix:ConditionalAttribute7 i:nil="true" />
                <threatmetrix:ConditionalAttribute8 i:nil="true" />
                <threatmetrix:ConditionalAttribute9 i:nil="true" />
                <threatmetrix:CreditCardNumberHash i:nil="true" />
                <threatmetrix:CustomAttribute1 i:nil="true" />
                <threatmetrix:CustomAttribute10 i:nil="true" />
                <threatmetrix:CustomAttribute2 i:nil="true" />
                <threatmetrix:CustomAttribute3 i:nil="true" />
                <threatmetrix:CustomAttribute4 i:nil="true" />
                <threatmetrix:CustomAttribute5 i:nil="true" />
                <threatmetrix:CustomAttribute6 i:nil="true" />
                <threatmetrix:CustomAttribute7 i:nil="true" />
                <threatmetrix:CustomAttribute8 i:nil="true" />
                <threatmetrix:CustomAttribute9 i:nil="true" />
                <threatmetrix:DriversLicenseHash i:nil="true" />
                <threatmetrix:SessionId>08a3958c-f2f5-43ad-b171-9de35633ff68</threatmetrix:SessionId>
                <threatmetrix:SocialSecurityNumberHash i:nil="true" />
        </fraud:FraudDetector>
</typ:FraudDetectors>
```

# 1.2 Amex Enhanced Auth

## American Express Enhanced Authorization Setup

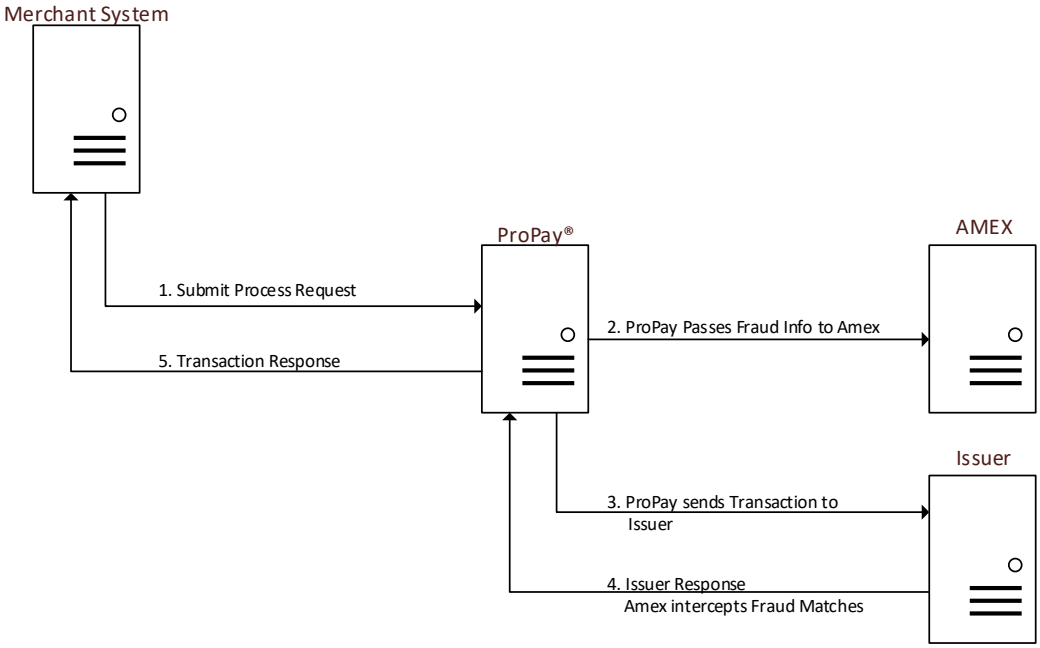
A client must provide to ProPay their Amex SE Number. ProPay will then setup the ProPay Merchant Account to use Amex Enhanced Auth. If a client does not have a relationship with Amex, it may use the ProPay Amex Aggregated SE number with approval from the ProPay Risk Department.

Please refer requests to setup a ProPay Merchant Account for Amex Enhanced Auth to: riskescalation@propay.com

## Amex Enhanced Auth Processing flow

1. Merchant System Submits ProPay API Request including Fraud Object.
    a. See Object attributes below
    b. 60 second ProtectPay timeout timer begins
2. ProPay Submits Fraud Object Data asynchronously to American Express and continues transaction process
3. Transaction is submitted along the American Express network and declined by American Express if submitted data matches criteria for fraud
4. On a decline from American Express or Error the transaction is completed and reported back to the Merchant with appropriate response code.
    a. See Appendix A.7 Fraud System Response Codes: Amex Enhanced Auth
    b. On an approval from American Express the transaction is completed and reported back to the Merchant with the appropriate response code and transaction response.
5. ProPay responds to the merchant with the transaction response.

## Amex Enhanced Auth Process flow diagram




## 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 | |

## Interface: ProPay Legacy XML

```
<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>
```

## Interface: ProtectPayREST

```
"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>
```

### Interface: ProtectPay WSDL

#### FraudDetectorProviderName: AmexEnhancedAuth

| Request Object | Fraud Provider Object | Attributes |
|---|---|---|
| FraudDetectors | **AmexEnhancedAuth** | FraudDetectorProviderName |
| | | ShippingMethod |
| | | InputIpAddress |
| | | ShippingAddress1 |
| | | ShippingAddress2 |
| | | ShippingCity |
| | | ShippingState |
| | | ShippingZip |
| | | ShippingCountry |
| | | ShippingPhoneNumber |

## 1.3 ProPay Fraud Detection

### ProPay Fraud Detection Setup

A client must provide their Merchant Account Number to ProPay. ProPay will then setup the ProPay Merchant Account to use ProPay Fraud Detection at Tier and merchant level to use ProPay Fraud Detection.

Please refer requests to setup a ProPay Merchant Account to: riskescalation@propay.com

### ProPay Fraud Detection Attributes

| Attribute | Type | Max | Required | Notes |
|---|---|---|---|---|
| FraudDetectorProviderName | String | | Required | Set to: `PropayFraudDetection` |
| InputIpAddress | String | | Optional | |
| ShippingAddress1 | String | | Optional | |
| ShippingAddress2 | String | | Optional | |
| ShippingCity | String | | Optional | |
| ShippingState | String | | Optional | |
| ShippingZip | String | | Optional | |
| ShippingCountry | String | | Optional | |

### Interface: ProPay Legacy XML

```
<ArrayOfFraudDetector xmlns="FraudDetectors">
        <FraudDetector xsi:type="PropayFraudDetection">
                <FraudDetectorProviderName>PropayFraudDetection</FraudDetectorProviderName>
                <InputIpAddress>8.8.8.8</InputIpAddress>
                <ShippingAddress1>123 Main Street</ShippingAddress1>
                <ShippingAddress2> </ShippingAddress2>
                <ShippingCity>Lehi</ShippingCity>
                <ShippingState>UT</ShippingState>
                <ShippingZip>84043</ShippingZip>
                <ShippingCountry>USA</ShippingCountry>
        </FraudDetector>
</ArrayOfFraudDetector>
```

### Interface: ProtectPayREST

```
"FraudDetectors":[
        {
                "PropayFraudDetection":{
```

```
                        "FraudDetectorProviderName":"PropayFraudDetection",
                        "InputIpAddress":"8.8.8.8",
                        "ShippingAddress1":"",
                        "ShippingAddress2":"",
                        "ShippingCity":"Lehi",
                        "ShippingState":"UT",
                        "ShippingZip":"84043",
                        "ShippingCountry":"USA"
                }
        }
]
```

### 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="propayfraud:PropayFraudDetection">
                <fraud:FraudDetectorProviderName>PropayFraudDetection</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:ShippingState i:nil="true" />
                <fraud:ShippingZip i:nil="true" />
        </fraud:FraudDetector>
</typ:FraudDetectors>
```

### Interface: ProtectPay WSDL

#### FraudDetectorProviderName: PropayFraudDetection

| Request Object | Fraud Provider Object | Attributes |
|---|---|---|
| FraudDetectors | **PropayFraudDetection** | FraudDetectorProviderName |
| | | InputIpAddress |
| | | ShippingAddress1 |
| | | ShippingAddress2 |
| | | ShippingCity |
| | | ShippingState |
| | | ShippingZip |
| | | ShippingCountry |

## 1.4 Fraud System Response Code

The following response codes are returned in the [RequestResult] object. They are generated by ProtectPay in response to the Fraud System and returned as the status of the API Request. They are unique to each Fraud System.

### 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 threat metrix 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 |