vantiv® | PayFac™

Fraud Toolkit FAQ

Q **What problems does Fraud Toolkit solve?**

A Fraudsters are sophisticated, well-funded and persistent. The impact of an individual fraud attack can depend on how quickly it can be detected and managed. Early and accurate prevention at the time of authorization can help reduce downstream expenses including loss of goods, refunds, chargebacks, representments and the intangible reputational damage.

Fraud Toolkit helps merchants mitigate these costs, losses, and expenses with a set of fraud detection tools that can be mixed and matched to counter particular fraud attacks.

Q **How does Fraud Toolkit identify fraudulent transactions?**

A Each individual tool works a bit differently. Below is a brief overview.

Basic Tools

The Fraud Toolkit offers 7 basic tools (aka "fraud filters") that employ common fraud detection techniques in the form of configurable rules. For instance, a PayFac may tell us "I want to filter out any transactions that fail security (i.e. CVV, CVC, CID) validation." These filters identify risky transactions simply by evaluating the PayFac's pre-configured rules. Two of the filters (AVS and Security Code) rely on responses from the issuing bank at the time of authorization. The other five, however, are based on data we maintain in-house.

Advanced Tools

Our advanced tools are powered by ThreatMetrix and rely on a different set of fraud detection techniques than our basic tools. ThreatMetrix gathers data in two ways: 1) device data directly via the merchant's checkout/payment page; and 2) transactional data that Vantiv sends at the time of authorization. ThreatMetrix's fraud scoring engine will then run all of these data points through that merchant's pre-configured fraud policy—which yields an overall risk score (i.e. -100, riskiest, to +100, safest). The merchant's fraud policy specifies the ranges along that spectrum that determine when a transaction should be passed, reviewed, or failed.

Q **What does Fraud Toolkit do when it finds a risky transaction?**

A For Basic Tools, any transaction that triggers any of pre-configured rules (e.g. Filter out when AVS checking yields a mismatched address and/or zip code) will be declined automatically on behalf of the merchant. Any successful authorizations (i.e. funds reserved by issuer) will be automatically reversed to preclude any misuse-of-authorization fees. The response reason code sent back to the merchant via XML will indicate the decline. The level of granularity as to messaging is dependent on the XML version to which the PayFac has coded.

With Advanced Tools, PayFacs have more control over how Vantiv will act upon finding risky transactions. They have two options: Auto Decline and Information Only. If they choose Auto Decline, we will decline the transaction on behalf of the merchant just as we do for Basic Tools. If the PayFac opted for Information Only, Vantiv will return the detailed fraud results from ThreatMetrix, but will not act on it at all. The PayFac is then responsible to reverse any approved authorizations.

Q **Who configures the Fraud Toolkit?**

A Each individual tool is configured differently. Below is a brief overview for each tier.

Basic Tools

The rule-set for each merchant is configured via MPM with the help of the implementation analyst.

Advanced Tools

PayFacs can either use the Vantiv pre-configured default fraud policy (i.e. rule set) or manage their own via the Self Service option. With the default option, PayFacs will not be able to tweak their rule set nor manage their own black/white lists. They will simply be assigned that policy by their implementation analyst via MPM. Self Service allows merchants who need more control direct access to the ThreatMetrix portal to manage their own rule set in real-time. In this case, there is still minor configuration in MPM from Implementation but the PayFac will do rule management.