First Data

Fraud FlexDetect℠ FAQs

Understanding Fraud

How do I understand my total impact of fraud today?
As a merchant, you should take into account chargebacks (including fees and fines), the danger of losing your merchant account, the limits on international growth, the customer insults felt by rejected transactions, the overhead cost of other third-party interactions, the manual review training and staffing efforts, and cost of lost goods. This will give an overall idea of the true cost of fraud and help calculate a return on investment for enabling Fraud FlexDetect℠.

How will Fraud FlexDetect help protect my business against fraud?

The FlexDetect solution evaluates all of the transaction data elements that you send to First Data in your authorization message and uses a real-time data engine to provide a numerical score, indicating relative risk on a transaction. The score is then referenced against your Fraud Settings Wizard. The transaction is processed based on your wizard preferences, and the processing action will be stored for future reference and analysis. This workflow is objective and comprehensive, yet easy to manage, and has been recognized as one of the best solutions in the industry to identify and avoid fraud.

Will this service help me if I don't have chargebacks?
Fraud FlexDetect gathers and evaluates details about the shopper's behavior and interaction on your site, to help you prevent future fraud losses, even if you are not incurring any today. It is a proactive solution that can identify patterns of shoppers' habits and preferences—leading to improved sales growth, fewer customer insults and overall streamlined order operations.

Is there any kind of guarantee that I am not liable for fraud?
This solution can be used in conjunction with Verified by Visa® and MasterCard® SecureCode™ programs, which offer relief from the burden of fraud liability. Outside of those services, the merchant is still responsible should a chargeback occur.

Setting Up Fraud FlexDetect

What is required for me to begin using Fraud FlexDetect?
You must be using the First Data Global Gateway – Virtual Terminal, Connect 2.0, or Web Service API entry points. Contact your account representative to activate the service quickly and easily.

How can I set up and control my fraud preferences?
You can adjust your preferences on handling risky transactions through the Fraud Settings Wizard at any time, which can be found within the Virtual Terminal Administration section. Adjusting your fraud settings too often may not be optimal for consistent analysis of fraud patterns, but there is no restriction on changes made to the settings at any time. It will take less than 30 minutes for your new fraud settings to go into effect.

How can I test the system before I launch it?
You may log in to the customer test environment (CTE) system to test how score and disposition responses from Fraud FlexDetect will look. Please reference the Fraud FlexDetect User Guide for more details.

How will the system work with or against my current fraud settings or services?
Fraud FlexDetect can complement other First Data services such as Verified by Visa and MasterCard SecureCode. It may also be used in conjunction with the basic fraud blocking and limiting details that exist within the Virtual Terminal Administration page. However, if you currently use a third-party system, it may not fit well with the Fraud FlexDetect system, and you should consult your account representative before moving forward with two separate fraud systems rather than a consolidated, streamlined solution.

First Data

Fraud FlexDetect℠ FAQs

Which transactions will be scored through Fraud FlexDetect?
Any Issuer-approved payment card "sale" transaction will be scored when Fraud FlexDetect℠ is activated. At this time, check transactions, recurring billing transactions and alternative payments will not be scored.

Who creates my scoring profile?
You configure your profile within the Fraud Settings Wizard. You input information about your typical business model and your preferences for handling risky transactions. Behind the scenes, the Fraud FlexDetect system calculates the logic and rule set for you. There are no IT resources required to build that logic into your Web site.

Other Fraud FlexDetect Questions

How will this solution affect my PCI compliance?
If you change the user permission setting (within Virtual Terminal Manage Users) for yourself or your staff to view full credit card data (also known as the full PAN), then that may change your Payment Card Industry (PCI) requirements. For more details, visit https://www.pcisecuritystandards.org/saq/index.shtml.

Who else will be viewing my data if I participate in the shared database information?
It is highly recommended that you participate in the shared database for Fraud FlexDetect. Each transaction score will be more accurate because the system will be able to reference that shopper's behavior across multiple merchants. Your site will not be identified by name. No confidential identifiable information about your business or your shoppers can be shared within this database.

What is "Accertify" and/or "Interceptas"? I see these terms in some of my documentation and in the Fraud FlexDetect interface.
First Data has partnered with Accertify as our chosen vendor for this fraud detection solution. Their technology has been built into the First Data Global Gateway℠ solution so that you do not need to establish a connection to them directly. Accertify's product platform is called "Interceptas," and this terminology may still be found in some legal documentation, technical manuals and on the Web browser interface. All connectivity with Accertify's technology is secure and confidential.

What if I don't notice a difference in my fraud levels after I launch the service?
Results may come over time as the cardholder has up to six months to dispute a purchase. We recommend monitoring fraud and chargeback reduction quarterly and annually to compare with historical results. If you believe a change in your Fraud Settings Wizard is required after monitoring, and need assistance, contact your support representative.

How does the Web Importer system work?
The Web Importer tool enables you to load existing credit card, product SKU, shipping method and country data into the Fraud FlexDetect reference tables. For example, if you know that Nigeria and Russia are high-risk countries for you, adding them through the Web Importer will allow the Fraud FlexDetect system to score them higher and help avoid transactions from those areas, if needed. For more information, please reference your Fraud FlexDetect User Guide.

What is the DeviceID and how does it work for me?
DeviceID, also known as Device Fingerprinting, is a key element in the Fraud FlexDetect scoring solution. This technology looks at the computer that the shopper is using to make a certain purchase, and it checks to see if that computer has ever been associated with fraud, or has characteristics that may indicate higher transaction risk. For merchants using Virtual Terminal for credit card authorization, this feature does not apply.

For other questions or additional information, contact support at 888-467-3611 or e-mail globalgateway.support@firstdata.com.

301-880