

MULTI-LAYER DEVICE FINGERPRINTING™

Overview

Kount's Multi-Layer Device Fingerprinting™ collects a comprehensive set of data that positively identifies a device in real time—whether fixed or mobile. The key to maintaining a device's ID, regardless of hardware and software configurations, is the ability to **analyze customer behavior associated with the device** and collect additional device parameters not typically accessible by other device ID technologies. Most importantly, Multi-Layer Device Fingerprinting™ does all this without retrieving the user's Personally Identifiable Information (PII).



The Solution

As part of the Kount Complete™ solution, Multi-Layer Device Fingerprinting™ thoroughly examines any device via numerous attributes—computer, tablet PC, SmartPhone, etc. While device type may vary, the following characteristics are typically examined:

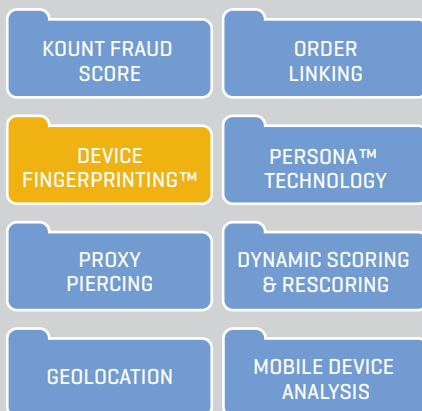
- > Network
- > SSL
- > JavaScript
- > Browser
- > Operating System
- > Flash
- > HTTP

In addition to this basic information, other variables are analyzed: 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. By examining all these different layers within a device—in a mere 300 milliseconds—Multi-Layer Device Fingerprinting™ establishes and maintains a distinct device ID—even when fraudsters try to modify system settings to disguise their true identities.

The advanced nature of Kount Multi-Layer Device Fingerprinting™ enables merchants to associate certain device anomalies with fraud patterns, making it easy to construct very specific rules to optimize fraud detection...no matter the device. We call this “moving beyond the device.”

FRAUD DETECTION

Kount's core technology analyzes hundreds of variables to detect fraud and risky behavior.



Kount's Fraud Platform consists of the three main pillars of an overall fraud strategy, Fraud Detection, Strategy Management and Operational Management. Multi-layer Device Fingerprinting™ is just one of the many features in Kount's comprehensive solution. See reverse for more detail.

PROXY PIERCING

Overview

The Proxy Piercer® feature combats fraudsters who use proxy servers to hide their actual location. Typically, the location of anyone accessing the Internet can be identified via the IP address assigned to their computer by their Internet Service Provider. A proxy server is used as an intermediary device to disguise a geographic location that is associated with high fraud activity. Proxy servers are used because a fraudster conducting a stolen credit card transaction wants to appear to be in the same location as the owner of the stolen card.



The Solution

Kount uses patented Proxy Piercer® Geolocation technologies to determine in real time if the purchase transaction request is being relayed through a proxy and if so, to determine:

- > True geolocation of the purchase request
- > Type of network being used by the person attempting to make the transaction [certain types of networks, such as prisons, schools, and libraries, as well as anonymous proxies, can indicate an increased risk of fraud]

The Proxy Piercer feature also has the ability to detect the use of “botnets.” Botnets are networks made up of remotely-controlled computers that have been compromised without the owner’s knowledge or consent. Fraudsters use botnets to relay fraudulent purchase requests in attempt to hide the true source of their order. As with proxy servers, the Proxy Piercer feature can determine if a botnet is in use and provide the true geolocation of the fraudster accessing the botnet.

Because the Proxy Piercer feature can detect proxy server or botnet use in real-time—returning a result while the transaction is within the merchant’s system—information is passed on to the merchant’s risk assessment department before an approval is given, so that the merchant can either conduct further risk evaluation activity or if deemed necessary, decline the purchase request.

FRAUD DETECTION

Kount’s core technology analyzes hundreds of variables to detect fraud and risky behavior.

KOUNT FRAUD SCORE	ORDER LINKING
DEVICE FINGERPRINTING™	PERSONA™ TECHNOLOGY
PROXY PIERCING	DYNAMIC SCORING & RESCORING
GEOLOCATION	MOBILE DEVICE ANALYSIS

Kount’s Fraud Platform consist of the three main pillars of an overall fraud strategy, Fraud Detection, Strategy Management and Operational Management. Multi-layer Device Fingerprinting™ is just one of the many features in Kount’s comprehensive solution. See reverse for more detail.

PERSONA™ TECHNOLOGY

Overview

The Persona™ feature is a method of determining key characteristics and identified qualities/attributes associated with a transaction. Persona uses hundreds of variables to construct a definitive link to online purchase behavior—either directly or indirectly—to help reveal fraudulent activity. This process takes less than one second to provide merchants with highly accurate fraud assessments in real-time.



The Solution

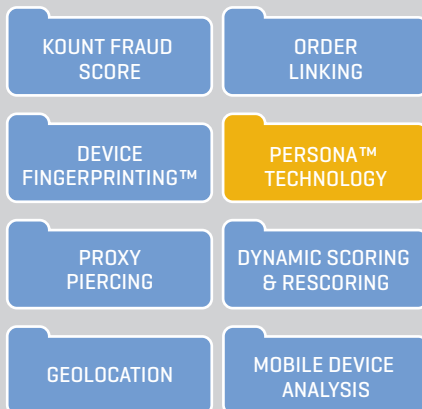
The Kount Persona™ feature provides a time-saving “shortcut” for predicting the likelihood of fraud. A Persona is built as the Kount system collects information from the purchases made across all merchants within the Kount’s network.

First, other Kount technologies such as Dynamic Scoring™, Multi-Layer Device Fingerprinting™, and Proxy Piercer assess over 200 variables and report in real-time (under one second) on potential risks. When these variables are compiled and evaluated, a Persona is created. Examples of attributes that make up a Kount 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 device making the purchase as determined through Proxy Piercer technology.
- > Discrepancies in the customers self-divulged information and actual information as determined by Multi-layer Device Fingerprinting information.

FRAUD DETECTION

Kount’s core technology analyzes hundreds of variables to detect fraud and risky behavior.



Kount’s Fraud Platform consist of the three main pillars of an overall fraud strategy, Fraud Detection, Strategy Management and Operational Management. Multi-layer Device Fingerprinting™ is just one of the many features in Kount’s comprehensive solution. See reverse for more detail.

DYNAMIC SCORING & RESCORING

Overview

The Dynamic Scoring™ feature monitors a credit card for signs of fraudulent activity even after a transaction has been approved. This “post-authorization” process has proven highly successful at spotting suspicious activity and retroactively tying that activity to previous purchases. The Kount Complete™ system then alerts the merchant that a previously-approved order now looks to have relevant connections to fraudulent activity. The merchant can re-evaluate the order and decline to ship—avoiding the loss of the goods while also preventing the expense of a chargeback.



The Solution

The Dynamic Scoring™ feature capitalizes on the fact that stolen credit cards 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 continually monitors all credit cards involved in approved transactions and provides real-time updates to the merchant when the card’s risk status changes. Dynamic Scoring does this by identifying and grouping transactions that are either directly or indirectly linked through a set of attributes or variables such as device IDs, credit card numbers, and emails. Based on this updated status, the merchant can determine if there is sufficient threat of fraud to retroactively decline the purchase request or to take other necessary action [for example, manual review by a human agent].

Dynamic Scoring is a continual, real-time process. As the information associated with an original order changes across all Kount merchants, the “fraud risk” score for any transaction currently in a merchant’s queue also changes, providing additional real-time updates on the transaction’s risk.

Note: Kount does not disclose which merchants were affected by the fraudulent activity, but will tell them that certain attributes, like the number of credit cards used, associated with the transaction have changed. This gives merchants an opportunity to assess the orders and verify the identity of the person placing the order. Kount Dynamic Scoring is continually searching for fraudulent connections and updates scores every 30 minutes. Since this is all happening in real-time, merchants can easily cancel orders, retain product and prevent a possible charge.

FRAUD DETECTION

Kount’s core technology analyzes hundreds of variables to detect fraud and risky behavior.

KOUNT FRAUD SCORE	ORDER LINKING
DEVICE FINGERPRINTING™	PERSONA™ TECHNOLOGY
PROXY PIERCING	DYNAMIC SCORING & RESCORING
GEOLOCATION	MOBILE DEVICE ANALYSIS

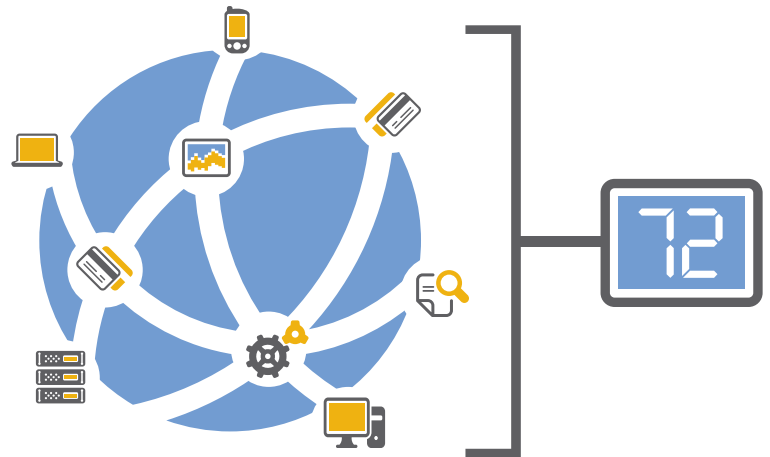
Kount’s Fraud Platform consist of the three main pillars of an overall fraud strategy, Fraud Detection, Strategy Management and Operational Management. Multi-layer Device Fingerprinting™ is just one of the many features in Kount’s comprehensive solution. See reverse for more detail.

KOUNT FRAUD SCORE

Overview

The Kount Score feature provides merchants with more predictive control and customization in the way they manage their fraud risk. This feature meets a key requirement identified in Gartner’s 2010 Magic Quadrant for Web Fraud Detection:

“Users want...a mathematically predictive scoring system that runs in parallel with the rules. Users can more easily set thresholds with predictive model scoring systems than they can with rules-based systems alone to enable them to better adjust their false-positive and transaction review rates.”



The Solution

The Kount Score is a highly accurate prediction of fraudulent activity using information from over two billion purchase attempts. The Kount Risk Inquiry System [RIS] generates a numeric Kount Score—between 1 and 99—in real-time for every transaction. The higher the “risk” score, the greater the risk of fraud.

Unlike other scoring systems that may only use a few variables to calculate a risk evaluation, Kount Predictive Modeling reviews over 200 variables that cross reference the transaction with millions of data points looking for any association with risky behavior.

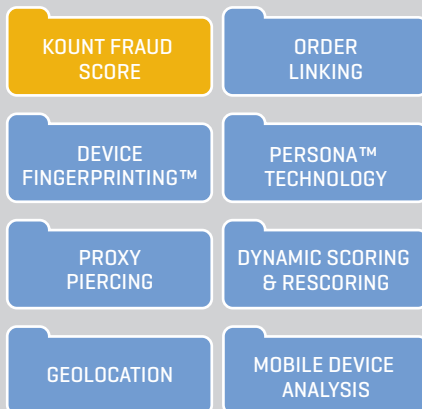
Included in a Kount Score calculation:

- > Multi-merchant order linking
- > Customer credit cards, email addresses and shipping addresses
- > Highest risk country within the past 14 days, using Kount’s 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
- > Kount’s 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, Kount allows you to dynamically re-score a potential purchase on-the-fly, so you can detect a fraudulent purchase that may initially have appeared to be legitimate.

FRAUD DETECTION

Kount’s core technology analyzes hundreds of variables to detect fraud and risky behavior.

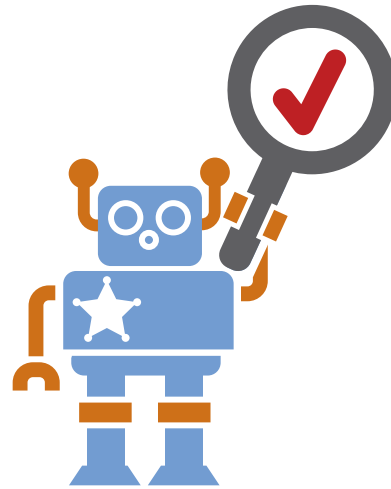


Kount’s Fraud Platform consist of the three main pillars of an overall fraud strategy, Fraud Detection, Strategy Management and Operational Management. Kount Fraud Score is just one of the many features in Kount’s comprehensive solution. See reverse for more detail.

MANUAL REVIEW AUTO AGENT

Overview

The AutoAgent feature in the Kount Complete™ solution features a powerful rules engine that enables administrators and risk assessment managers to create custom rules for orders with specific characteristics. When an order enters the merchant’s system that has one or more of these characteristics, it is automatically routed for AutoAgent review and disposition. AutoAgent can then apply additional tests, processes and/or profiles and reach a decision—without the need for intervention by a human risk assessment agent.



The Solution

The Kount AutoAgent feature employs its own rules engine that is separate from the Primary rules engine, making it possible to automate additional review processes for certain types of suspect orders.

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

Because AutoAgent allows merchants to create rules and rule actions for the system to make an “auto-decision” on suspect orders (approve, review, decline, or escalate) 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 exposure to fraud.

Most importantly, the merchant maintains total 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-decisioned are assessed by the AutoAgent. Any orders the merchant requires to be manually reviewed are still routed to the risk assessment team.

OPERATIONAL MANAGEMENT

Comprehensive support and best practices to maximize operational efficiency.

MANUAL REVIEW
AUTO AGENT

3RD PARTY
DATA CALLOUTS

CASE
MANAGEMENT

AGENT MANAGEMENT
TOOLS

BANK
INFORMATION

VERIFICATION &
AUTHENTICATION

REPORTING

ENTERPRISE WEB
SERVICES

Kount’s Fraud Platform consist of the three main pillars of an overall fraud strategy, Fraud Detection, Strategy Management and Operational Management. Manual Review Auto Agent is just one of the many features in Kount’s comprehensive solution. See reverse for more detail.

BUSINESS INTELLIGENCE REPORTING

Overview

Kount Datamart™ is a business intelligence application suite that uses integrated dashboard, data mining, reporting and workflow tools to re-structure raw data into a comprehensive presentation of relevant information. Datamart reports can help businesses plan and manage risk management, staff workload, transaction queue, rule effectiveness, organization and many other aspects of analyzing data gathered in the Kount Agent Web Console. The reporting features make it easy to establish the perfect view of your data to maximize functionality and productivity while ensuring system integrity and security.



OPERATIONAL MANAGEMENT

Comprehensive support and best practices to maximize operational efficiency.

MANUAL REVIEW
AUTO AGENT

3RD PARTY
DATA CALLOUTS

CASE
MANAGEMENT

AGENT MANAGEMENT
TOOLS

BANK
INFORMATION

VERIFICATION &
AUTHENTICATION

REPORTING

ENTERPRISE WEB
SERVICES

Kount's Fraud Platform consist of the three main pillars of an overall fraud strategy, Fraud Detection, Strategy Management and Operational Management. Business Intelligence Reporting is just one of the many features in Kount's comprehensive solution. See reverse for more detail.

The Solution

- > **Kount Datamart™.** Helps administrators discover trends, summarize results and analyze historical information of transactions drawing from over 100 variables.
- > **Easy To Use.** The robust Datamart tool assists in validating rule effectiveness, preparing agent and workflow management results, evaluating shopping cart details and preparing custom dashboards with simple, easy to use drag-and-drop functionality.
- > **Standard and Custom Reports.** Kount Datamart™ includes over twenty-nine standard reports and dashboards such as agent, workflow, analysis, operational, planning and trending reports. In addition, with over 100 variables and drag-and-drop features, creating custom reports is virtually unlimited. Reports can be viewed in table or chart formats and can be easily exported for distribution.
- > **Security.** Administrators can track any configuration changes to the management console, rules engine and workflow to verify that an authorized individual made each change and that changes match approved policies. User Login Reporting tracks user login attempts, both successful and unsuccessful. This report can help determine if a party is attempting to gain unauthorized access to your Kount system.

THIRD PARTY DATA CALLOUTS

Overview

The Kount Complete™ solution integrates data services from leading providers to facilitate smooth, seamless operations—without having to leave the Kount interface.



OPERATIONAL MANAGEMENT

Comprehensive support and best practices to maximize operational efficiency.

MANUAL REVIEW
AUTO AGENT

3RD PARTY
DATA CALLOUTS

CASE
MANAGEMENT

AGENT MANAGEMENT
TOOLS

BANK
INFORMATION

VERIFICATION &
AUTHENTICATION

REPORTING

ENTERPRISE WEB
SERVICES

Kount's Fraud Platform consist of the three main pillars of an overall fraud strategy, Fraud Detection, Strategy Management and Operational Management. Third Party Data Integration is just one of the many features in Kount's comprehensive solution. See reverse for more detail.

The Solution

To aid risk assessment agents in their review process—and to support automated functions and capabilities—Kount has integrated a number of key data services into the Kount Complete™ solution.

This Integration of third-party evaluation and assessment services within Kount 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 more quickly review and validate transactions. These services are directly accessible through the Agent Web Console for easy access and can be used as part of the Kount rules engine and Kount AutoAgent features.

ENTERPRISE WEB SERVICES

Overview

Kount Enterprise Web Services provide the maximum protection for the merchant while minimizing the impact of managing fraud prevention. These services provide merchants with external resources that help them maintain and enhance their Kount Complete™ solution. Kount's risk analysis department works with the merchant's risk managers, augmenting the merchant's experience to develop effective anti-fraud strategies that optimize the Kount Complete anti-fraud solution.



OPERATIONAL MANAGEMENT

Comprehensive support and best practices to maximize operational efficiency.

MANUAL REVIEW AUTO AGENT	3RD PARTY DATA CALLOUTS
CASE MANAGEMENT	AGENT MANAGEMENT TOOLS
BANK INFORMATION	VERIFICATION & AUTHENTICATION
REPORTING	ENTERPRISE WEB SERVICES

Kount's Fraud Platform consist of the three main pillars of an overall fraud strategy, Fraud Detection, Strategy Management and Operational Management. Enterprise Web Services is just one of the many features in Kount's comprehensive solution. See reverse for more detail.

The Solution

Merchants can capitalize on Kount's expertise to secure critical benefits: enhanced protection, lower cost of goods sold, and improved operational efficiency...without impacting the customer experience.

Kount Enterprise Web Services provides a comprehensive set of support and development services, including:

- > Boarding and certifying new merchants
- > In-depth training on Kount features and best practices
- > Customized rules development and review
- > Global analysis of a merchant's risk environment
- > Optimization of rules and configuration specific to a merchant's needs

Most importantly, Kount Enterprise Web Services enables merchants to confidently scale transaction volume and revenue while holding down staff growth, sustaining overall profitability.

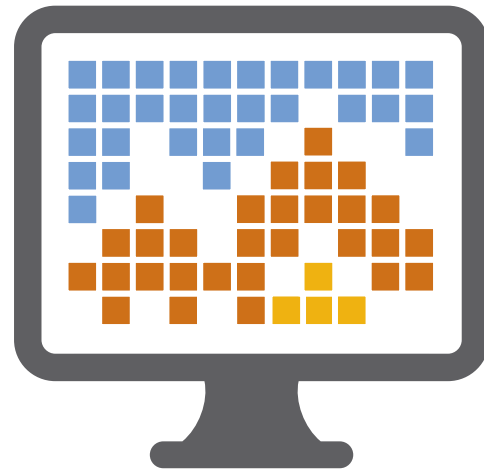
Kount Enterprise Web Services allows merchants to minimize the impact of hiring and training internal staff to:

- 1) Support and administer the Kount application
- 2) Manage the complexity of ever-changing fraud attacks, payment regulations, and emerging fraud and anti-fraud technologies

AGENT MANAGEMENT

Overview

The Agent Workflow Console helps increase operational 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.



OPERATIONAL MANAGEMENT

Comprehensive support and best practices to maximize operational efficiency.

MANUAL REVIEW
AUTO AGENT

3RD PARTY
DATA CALLOUTS

CASE
MANAGEMENT

AGENT MANAGEMENT
TOOLS

BANK
INFORMATION

VERIFICATION &
AUTHENTICATION

REPORTING

ENTERPRISE WEB
SERVICES

Kount's Fraud Platform consists of the three main pillars of an overall fraud strategy, Fraud Detection, Strategy Management and Operational Management. Agent Management Integration is just one of the many features in Kount's comprehensive solution. See reverse for more detail.

The Solution

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

Features like "auto-decision" help risk assessment agents more quickly determine whether an order is valid, or if a manual review is even 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 such as TARGUSinfo, LexisNexis and 192.com, enabling agents to seamlessly gather customer information through on-demand address and telephone verification.

The Kount web 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.

AFFILIATE MONITORING

Overview

Merchants often use affiliates and affiliate networks for marketing products and services. Unfortunately, affiliates can engage in fraudulent activity in order to “earn” commissions from the merchant without actually fulfilling their responsibility to direct valid customer traffic to the merchant’s website and the desired product page. Sites that offer “free trials,” or that require an application to be completed before the transaction can be submitted, are especially vulnerable to fraud due to the delay in the actual sale.



The Solution

There are multiple methods by which an affiliate can commit fraud against a merchant. The two most common include:

- > Affiliates use automated programs [“click bots”] to generate a large number of fraudulent clicks to collect illegitimate “pay-per-click” commissions.
- > Affiliates use stolen credit cards to illegitimately “buy” products from the merchant—not with the idea of receiving the product but to collect fraudulent “pay-per-sale” commissions.

Kount’s Affiliate Monitoring feature allows merchants to quickly identify fraudulent affiliate behavior prior to paying the commission for a “click” or “sale.” The same technology that identifies when stolen credit cards are used by external customers can be used to detect an affiliate using a stolen credit card for a fraudulent “purchase.” Since this occurs in real-time, the order can be rejected and the merchant can avoid paying a fraudulent commission to the affiliate.

If certain affiliates are deemed higher risks (but not found to have committed fraud), Kount allows a merchant to flag any orders associated with these suspected affiliates. These flagged transactions can then be routed for manual review by the merchant’s risk assessment team.

If affiliates are identified as fraudsters, they can be banned from the affiliate network and Kount can subsequently identify any order activity generated by a banned affiliate to prevent fraudulent orders.

STRATEGY MANAGEMENT

Create and manage a fraud strategy based on your specific business needs.

CREATE RULES

SHOPPING CART DATA

MANAGE RULES

CUSTOM SCORES

AFFILIATE MONITORING

AUTO DECISIONING

VELOCITY LIMITS

MULTI-CHANNEL STRATEGIES

Kount’s Fraud Platform consist of the three main pillars of an overall fraud strategy, Fraud Detection, Strategy Management and Operational Management. Affiliate Monitoring is just one of the many features in Kount’s comprehensive solution. See reverse for more detail.

MOBILE DEVICE ANALYSIS

Overview

Most merchants look at mobile commerce as a new and exciting way to allow customers to buy products without sitting in front of a PC. Rapid growth of mobile devices globally though, has opened new doors for fraudsters. Fraudsters now have more ways to access goods and services, mask themselves, and attempt to steal from merchants. Unlike other forms of payment, mobile devices introduce many new elements that complicate the user verification process. Stolen mobile devices are as vulnerable as stolen credit cards and other forms of identification.



The Solution

At Kount, we look at fraud as fraud, no matter where it is being committed or with which device or payment method. Mobile devices have a different set of criteria, which require merchants to employ technology to identify, validate, and authorize purchases as quickly as possible. Kount's all-in-one solution makes it easy to monitor transactions coming from mobile devices and make any necessary adjustments.

- > Kount's Risk Decision Rules engine gives merchants the flexibility to approve, decline, or review orders from any type of device (including mobile devices) automatically, based on established business rules.
- > With mobile devices, speed and accuracy are critical to maintain a friction-free checkout, catch fraud in real-time, and meet customer expectations. Kount provides merchants with real-time analysis of mobile devices, helping reduce fraudulent transactions, increase sales, and maintain customer satisfaction.
- > The Kount platform already has mobile protection technology integrated in as part of the overall fraud solution, to protect merchants from fraudsters using mobile devices.

The Kount 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.

FRAUD DETECTION

Kount's core technology analyzes hundreds of variables to detect fraud and risky behavior.

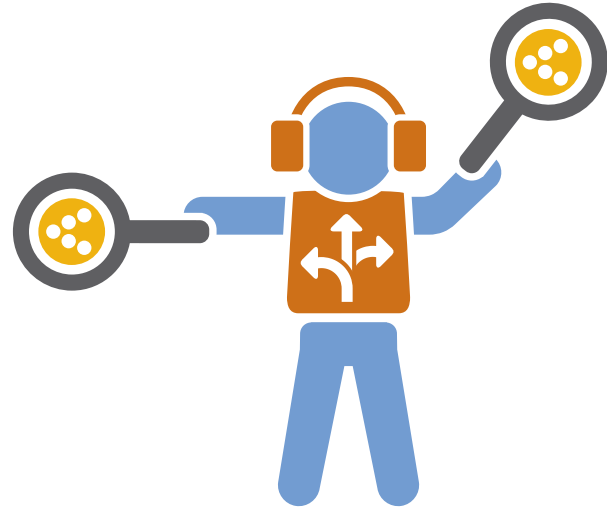
KOUNT FRAUD SCORE	ORDER LINKING
DEVICE FINGERPRINTING™	PERSONA™ TECHNOLOGY
PROXY PIERCING	DYNAMIC SCORING & RESCORING
GEOLOCATION	MOBILE DEVICE ANALYSIS

Kount's Fraud Platform consist of the three main pillars of an overall fraud strategy, Fraud Detection, Strategy Management and Operational Management. Kount's Mobile Device Analysis is just one of the many features in Kount's comprehensive solution. See reverse for more detail.

WORKFLOW MANAGEMENT

Overview

Workflow management is an important factor that ensures the efficient and effective processing of orders flagged for review. Based on established rules, Kount’s 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 so that the most important transactions are processed first. Transactions waiting to be resolved can also be escalated to top priority based on other factors including “time in queue” and many others.



The Solution

Resolving suspicious transactions quickly helps merchants increase sales and maintain a high level of customer satisfaction. Kount’s workflow management features allow 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, maximizing efficiency and operational control.

- > **Example:** During an initial screening of a transaction, Kount determines the consumer’s browser is set to Spanish as the primary language. If that transaction needs review, the Workflow Queue Manager forwards the transaction details to a Spanish-speaking review agent automatically.
- > **Example:** Kount flags a high-value transaction because the merchant’s established rules are triggered and details of the order are suspicious. Because the order is above a certain dollar amount, Kount automatically sends transaction details to a senior review agent for resolution.
- > **Example:** An order is placed from a customer in London and has been identified because of some questionable payment details. Kount’s Workflow Queue Manager sends the transaction details to the merchant’s London-based review staff for processing.

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

OPERATIONAL MANAGEMENT

Comprehensive support and best practices to maximize operational efficiency.

MANUAL REVIEW AUTO AGENT	3RD PARTY DATA CALLOUTS
CASE MANAGEMENT	AGENT MANAGEMENT TOOLS
BANK INFORMATION	VERIFICATION & AUTHENTICATION
REPORTING	ENTERPRISE WEB SERVICES

Kount’s Fraud Platform consist of the three main pillars of an overall fraud strategy, Fraud Detection, Strategy Management and Operational Management. Business Intelligence Reporting is just one of the many features in Kount’s comprehensive solution. See reverse for more detail.

A STRATEGIC APPROACH TO FRAUD/RISK MANAGEMENT

Kount provides an all-in-one fraud management solution to help you prevent fraud before it occurs.

FRAUD DETECTION

The layered integration of Kount’s core technology makes it possible to more quickly and accurately detect fraud. Our proprietary techniques analyze hundreds of variables resulting in a highly predictive Kount Risk Score.

STRATEGY MANAGEMENT

Kount’s tools create and manage a fraud strategy that dovetails with your business needs. Customize how Kount processes transactions based on your specific business rules.

OPERATIONAL MANAGEMENT

Comprehensive support and best practices to maximize operational efficiency. A simple way to manage the flow of transactions through the system, interact with risk managers and critical business systems such as logistics, accounting, etc.

KOUNT FRAUD SCORE	ORDER LINKING	CREATE RULES	SHOPPING CART DATA	MANUAL REVIEW AUTO AGENT	3RD PARTY DATA CALLOUTS
DEVICE FINGERPRINTING™	PERSONA™ TECHNOLOGY	MANAGE RULES	CUSTOM SCORES	CASE MANAGEMENT	AGENT MANAGEMENT TOOLS
PROXY PIERCING	DYNAMIC SCORING & RESCORING	AFFILIATE MONITORING	AUTO DECISIONING	BANK INFORMATION	VERIFICATION & AUTHENTICATION
GEOLOCATION	MOBILE DEVICE ANALYSIS	VELOCITY LIMITS	MULTI-CHANNEL STRATEGIES	REPORTING	ENTERPRISE WEB SERVICES

Kount

Kount delivers an all-in-one fraud and risk management solution for companies that have card-not-present environments looking to simplify their fraud/risk operations while dramatically improving bottom line results. Kount provides a single, turnkey fraud solution that is easy-to-implement and easy-to-use. Kount’s proprietary technology has

reviewed hundreds of millions of transactions and provides maximum protection for some of the world’s best-known brands. Kount’s solution is feature rich and technology proven. Regardless of the industry, Kount responds with accurate information in milliseconds, thereby enhancing the overall consumer experience.