Product Sheet

FraudNet

Comprehensive and frictionless online fraud detection

To catch a criminal, you have to think like one. Based on this premise, FraudNet was specifically designed to deliver a comprehensive, frictionless fraud management solution that protects the customer experience in the midst of rising fraud threats. FraudNet's multi-layered approach deploys quickly and can be easily tailored to view suspect events, make informed decisions, and perform link analysis to quickly recognise multiple events with common themes. Designed to detect fraud as well as fast-track trusted customers, FraudNet helps grow and enable digital business.

Benefits of fraudnet

Lower fraud losses

Fraud capture rates are pivotal to determining the effectiveness of your fraud solution provider and are measured in various industry reports on an annual basis. FraudNet provides a comprehensive solution with fraud capture rates that exceed industry averages.

Protect the customer experience

FraudNet provides a covert, frictionless solution that reduces outsorts and false positives, thus speeding good customers along and growing your business. card company for the declination, while nearly one in three pointed to the merchant

Frustrate fraudsters

The FraudNet solution has consistently demonstrated reduced long-term attack rates for our clients, as frustrated fraudsters move on to more vulnerable targets.

Improve operational efficiency

The FraudNet solution provides efficiencies that help reduce waste and improve operations.

FraudNet Components

Device intelligence DeviceInsight

This real-time technology is tagless and cookieless, empowering businesses to stay one step ahead of the fraudster while allowing for an unimpeded customer journey. Device information and collectors are internally controlled, guaranteeing a DeviceInsight ID for every event, without the need for call outs, pop-ups, or a separate relationship from the fraud solution provider.

Covert and privacy-friendly, the device collector gathers over 100 different attributes from each page, combines them with HTTP headers, and then generates a 40-character hash. In addition to DeviceInsight, patented Time-Differential Linking (TDL) values provide even more granularity and insight into the device that has been used.

Mobile SDKS

Mobile devices and mobile apps are synonymous with digital events. Mobile SDKs have been built for use in native apps to provide even more granularity with device identification. Experian researchers have tested hundreds of different devices and continue to make improvements on the collectors for both iOS and Android devices. In addition to testing many devices, the team regularly makes changes to keep up with the latest software updates, usually in advance of software releases.

Risking

Risk engine

FraudNet's real-time risk engine is a highly configurable, strategy-driven risk model with over 600 out of the box rules. In addition to the standard rules available to every client, custom rules can be created to target the specific fraud patterns that occur within specific industries. The combination of contextual data, behavioral data, and device data enables FraudNet to identify more fraud with fewer false positives than others.

Model management

FraudNet allows managers the added flexibility of being able to control all of their models within the UI, eliminating dependence on a helpdesk member. Managers can add, remove, and modify a rule, rule score, or rule action at any time. Any changes made to a model are effective immediately. Risk strategy. To truly be effective, the risk strategy must work in tandem with the technology. That is why FraudNet's risk management team works directly with customers to develop fraud prevention strategies, actively tune risk models, and share cross-vertical fraud intelligence. This high-touch approach best leverages the risk team's expertise and the needs of the business for the most effective fraud prevention strategy.

Velocity

FraudNet administrators can create custom threshold windows to identify fraudsters who are re-using data or accessing multiple accounts from the same device. This information can be used to detect BOT activity, card testing, bust-out accounts, and free-trial abuse.

Malware

Though the presence of malware does not always indicate a specific event is fraudulent, it does indicate that a user's credentials have been compromised and that extra precaution should be taken with their account going forward.

User Interface

Case management

This workbench provides all of the information an investigator needs in one intuitive, configurable GUI. Investigators can search for a specific event or work from a queue of outsorted events, and make notations, take different actions, or conduct further research as needed. Confirming an event as fraud can automatically add pre-defined data points to the negative list so that future fraud is automatically captured. Within the event page, an Investigator can take advantage of the different data enrichments and links that populate an event with even more information.

DataSpider

Investigators can be bogged down with post-forensic analysis when looking for fraud related to a confirmed bad event. DataSpider takes the manual work out of doing this, and recursively searches for linked events based on name, email, phone, address, User ID, and encrypted credit card number within a user-based timeframe. Once the query is run, the results come back color coded to show the different links within the different events. DataSpider can locate complex fraud patterns even when the fraudsters are tumbling information and trying to evade existing logic.

SketchMatch

While DataSpider links events based on user-entered data, SketchMatch does the same thing with device data. Device data is hard to circumvent and change, and fraudsters are often not aware of what is being collected. By using link analysis, an investigator can find linked events based on device attributes, and uncover fraud rings.

Configurable lists

Although FraudNet provides basic positive and negative lists to white and black list key data points including email address, DeviceInsight ID, address, and many others, different industries have different needs and patterns of risk that might not be applicable to another. Because of this, multiple industry specific lists have been created in order to provide an added layer of defense.

Analytics

Standard reporting

Six standard, out of box reports provide all the basic metrics necessary for measuring the effectiveness of FraudNet and the associated risk team. Each report focuses on a different aspect of fraud management within a risk organisation.

Feedback by Payment Type and Feedback by Reason Code

These two reports address chargeback rate, the most common fraud metric used by ecommerce and travel merchants. Losses are measured through feedback submitted via chargeback or feedback submitted by an analyst that indicated an event was found to be fraudulent.

System Level Summary

Provides a snapshot of how the entire organisation is performing overall, with total sales and loss numbers.

Outsort Summary

Provides a view of what is in current outsort queues.

Investigator Productivity

Measures investigator performance, including how many events were reviewed, and what actions were taken. Additional metrics include how many investigators approved reviews were later deemed to be fraudulent **Rule Level Hit Rate.** This report allows administrators to measure the effectiveness of each rule in their system, on an individual model basis. Each rule code, its current settings, and a host of metrics are provided. One of the key metrics provided is the lift, which is a numerical quantification of effectiveness.

Custom reporting

In addition to the standard reports that are available to every customer, FraudNet allows for custom reports to be created as well. These reports can be run ad-hoc or scheduled as recurring jobs, and can be saved or exported for review. Almost every field that is available in the UI is also available for reporting purposes.

Enhanced analytic response

This add-on analytics feature is a compilation of event data, device data, enrichment data, and advanced risk data made available for machine- to-machine consumption. This reporting feature can be used to combine the data from online and offline businesses, into existing data warehouse for analysis by internal business intelligence tools. The combination of this information can be used in identifying meta-trends and providing a full 360-degree picture of all customers.

Data enrichment

Third party data enrichment

FraudNet uses third party data enrichment to provide investigators with added context to create a clearer picture. Obtaining information like an IP address or BIN number is good protocol, but individually, neither of those elements help to make informed decisions. Knowing that the BIN indicates a foreign issued account or that the IP is in the same city as the billing address does provide more context and help the investigator piece together the puzzle.

Product Sheet

FraudNet

Behavioral context

Fraudsters are opportunistic and attempt to get as many events completed as possible in the shorted period allowed and often exhibit the same habits and patterns in an attempt to get through the process as quickly as possible without being detected. Risk analysts continuously work to identify the specific attributes of new fraud trends and rings to create new rules that trap the fraudsters while keeping false positives and queue outsorts low.

About Experian Decision Analytics, Fraud and Identity Solutions

The fraud and identity business line of Experian Decision Analytics enables organisations to drive growth and profits by identifying legitimate customers and detecting fraud at every point of contact while maintaining a positive customer experience. Through our unique combination of consumer and business information, analytics, decisions, and execution, we help organisations implement a comprehensive, layered defense strategy where protection is commensurate with risk and value.

Our expertise in risk-based decisioning has made us a global leader in fraud and identity solutions including new account opening, account takeover, bust-out fraud, online and mobile fraud, and card-not-present fraud across a range of industries and customer channels. Experian enables organisations to realise increased revenue, controlled risk, enhanced operational efficiency, and superior compliance for competitive advantage.

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
T: 1 888 414 1120
www.experian.com

03/17 • 2000/1238 • 1044-DA