Product Sheet

FraudNet

Powerful fraud detection and a positive customer experience. Can you really have it all?

To catch a criminal, you have to think like one. Based on this premise, FraudNet was designed to make fraud inroads hard and the customer journey easy. FraudNet's multi-layered approach can be tailored to view suspicious events and make informed decisions. Link analysis done behind the scenes allows you to quickly spot multiple events with common themes. If your fraud systems challenge, block or deny too many good transactions, your good customers will get frustrated. With FraudNet, you'll know the difference between a fraudster and a customer, so you can protect your online channel without disrupting the customer experience.

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.

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 risk 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 to 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.

Product sheet

FraudNet

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 your own risk team to develop fraud prevention strategies, actively tune risk models, and share cross-vertical fraud intelligence. This high-touch approach best leverages our experience and your needs 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. FraudNet detects the presence of malware, and although 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. The FraudNet 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 potentially 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-the-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 organization.

Feedback by payment type and feedback by reason code reporting. 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. This report provides a snapshot of how the entire organization is performing overall, with total sales and loss numbers.

Outsort summary. This report provides a view of what is in current outsort queues.

Investigator productivity. This report 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, 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 provides more context and helps the investigator piece together the puzzle.

Behavioral context. Fraudsters are opportunistic and attempt to get as many events completed as possible in the short 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 the behaviors of fraud rings to create new rules that trap the fraudsters while keeping false positives and queue outsorts low.

Effective fraud prevention does more than stop fraud

Without a doubt, your fraud prevention efforts are aimed at stopping fraud and reducing losses. But, an effective program also makes it easier for your good customers to do business with you. So how do you achieve both? It starts with moving away from a one-size-fits all approach. Instead, you should apply the right level of protection needed for each and every transaction.

Our fraud team – nearly 300 experts around the world – works with businesses to do exactly that. We're proud of the fact that we helped our clients screen more than 15 billion fraud events this past year. That's over 3,300 events per second. Most consumers aren't aware of what's happening behind the scenes to keep them safe as they do everyday things...like shop online or check bank balances from a mobile device. We call that hassle-free, and that's how it should be. Our solutions are built using data, technology and analytics to stop fraudsters without stopping good customers. Now, fraud prevention contributes to growth and a positive experience.

United Arab Emirates
Dubai Islamic Bank Building 01
Office 102, First Floor
Dubai Internet City
www.experian.ae