Fraud Scoring

Definition/Description

Fraud scoring is used by merchants, issuers, and/or their processors to assess the level of risk in taking a CNP order. A fraud score indicates whether an order should be rejected, accepted, or further reviewed. The fraud scoring engine arrives at the score using techniques discussed elsewhere (e.g., velocity checks, blacklists, geolocation). Fraud scoring can be seen as the "calculator" that uses data from multiple techniques to arrive at a score that can be used to determine which action can be taken.

Fraud scoring is usually done by a vendor, which will bring more information to the scoring than a home-built single merchant solution. Solution results can be pass/fail or provide a score in a range. Consortium models are typically used by issuers to score transactions for authorizations. A score can also be used in an EMV 3-D Secure (3DS) or other authentication process to identify high-risk authentication requests that require stepped-up authentication.

Methods used for scoring vary, and can include heuristics, neural nets, or external scores. Some services may also provide tools to help with items needing manual review.

Applicability

Channel	Applicable?	Use Case	Applicable?	Stakeholder	Applicable?
In-app [merchant app]	Yes	Customer onboarding	NA	Merchants	Yes: internal
Mobile browser	Yes	Authentication (onboarding)	Yes	Issuers	Yes: internal
Desktop/laptop computer	Yes	Authentication (transaction)	Yes	Issuer processors	Yes: for clients
Phone	NA	Authorization	Yes	Wallet/online payment providers	Yes: for clients
		Post-authorization review	Yes	Acquirer processors	Yes: for clients

Technical Features/How the Technique Works

Fraud scoring can be used at various points in the CNP transaction process. During pre-authorization, a score can be employed in an authentication procedure (e.g., EMV 3DS). During authorization, a fraud score can be used to approve or deny a purchase. During post-authorization, the score can be used to queue a transaction for manual review, often prior to fulfillment.

Fraud engines differ among vendors. In a typical case, various data elements are checked against any internal fraud lists for matches. If nothing is found, rules for velocity of use and change are often applied, followed by items that could include geolocation, address, phone number or other factors. All of these then produce a pass/fail result or numerical score, on which the client can then take action.

Risks Associated with Technique

The effectiveness of fraud scoring depends on the strength of the model. Because of this, internally built systems are generally weaker than third-party services because the data on which internal models operate is more limited.

Since fraudster tactics change frequently, models used for fraud scoring, and the data the models work from, need to be frequently updated, whether internally built or sourced from a third party.

In order to help improve fraud mitigation, some fraud scoring engines provide not only a score but a reason for the score.

It is important to remember that a significant portion of the data collected for this technique may fall under GDPR rules.

Customer Impact/Level of Friction

This technique has no impact on customers at checkout.

Implementation Considerations

Fraud engines are typically sourced from a third-party vendor. While they can be built internally, this limits the effectiveness, due to the smaller dataset.

Maturity

Fraud scoring has been used since fraud mitigation started. The techniques that feed the scoring engine have changed, with some newer than others.

Applicable Industry Standards

This technique has no applicable industry standards.

Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

Further Reading

http://blog.unibulmerchantservices.com/fraud-scoring/

http://fraudpractice.com/FL-FraudScore.html

Source Document: This technique is extracted from the *Card-Not-Present (CNP) Fraud Mitigation Techniques* white paper. That white paper was developed to provide a high-level document that directs readers to relevant fraud mitigation techniques while providing easy access to details about the solutions. The white paper is available at: https://www.uspaymentsforum.org/card-not-present-cnp-fraud-mitigation-techniques/

Please note: *The information and materials contained in this document ("Information") is provided solely for convenience and does not constitute legal or technical advice. All representations or warranties, express or implied, are expressly disclaimed, including without limitation, implied warranties of merchantability or fitness for a particular purpose and all warranties regarding accuracy, completeness, adequacy, results, title and non-infringement. All Information is limited to the scenarios, stakeholders and other matters specified, and should be considered in light of applicable laws, regulations, industry rules and requirements, facts, circumstances and other relevant factors. None of the Information should be interpreted or construed to require or promote the establishment of any solution, practice, configuration, rule, requirement or specification inconsistent with applicable legal requirements, any of which requirements may change over time. The U.S. Payments Forum assumes no responsibility to support, maintain or update the Information, regardless of any such change. Use of or reliance on the Information is at the user's sole risk, and users are strongly encouraged to consult with their respective payment networks, acquirers, processors, vendors and appropriately qualified technical and legal experts prior to all implementation decisions.*