Negative/Positive Database

Definition/Description

Negative and positive databases are lists of ecommerce customer attributes that could indicate a purchase should be declined or approved. Negative databases are also referred to as "blacklists," and positive databases as "whitelists." Customer attributes for can include (but are not limited to):

- IP address
- Shipping address
- Country
- Email address
- Card account number

Applicability

Channel	Applicable?	Use Case	Applicable?	Stakeholder	Applicable?
In-app [merchant app]	Yes	Customer onboarding	Yes	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	Yes	Authorization	Yes	Wallet/online payment providers	Yes: for clients
		Post-authorization review	Yes	Acquirer processors	Yes: for clients

Technical Features/How the Technique Works

Negative databases are created from many different types of data that are associated with risky or fraudulent activity. Positive databases can be broad or specific to a certain industry.

Third parties offer lists as merchant tools, and merchants can add to the databases.

When a customer tries to make a purchase, the customer's attributes are compared to those in the negative database; if there is a match, the customer may be blocked or flagged for additional review.

Risks Associated with Technique

Missed fraud and false positives are both risks of using negative databases.

Fraudsters change the methods and information they use when buying online, making it difficult to obtain a match in a negative database.

Attributes associated with a fraudulent transaction may not always be fraudulent; for example, some addresses, such as university dorms, corporate offices, and re-shippers, serve a large number of people. Fraud committed by one person at such an address could lead to all orders being blocked from shipping to that address.

Use of negative databases to flag transactions for further review is often part of a layered fraud solution.

Positive databases also have risks. Some third-party solutions depend on successful customer use at other merchants, with this use flagging the customer as positive. This dependence leaves the merchant vulnerable to how the data is sourced.

Customer Impact/Level of Friction

Negative/positive databases are transparent to the customer, but a false decline can affect future sales.

Implementation Considerations

Internal systems must be able to receive and take actions based on output of the comparison.

Maturity

Both positive and negative database are widely used by merchants and have been for many years.

The 2017 MRC Global Fraud Survey found that 96% of merchants surveyed were using negative databases, and 79% positive databases.[1]

Negative and positive databases are limited in their effectiveness, so are typically used as part of a layered approach.

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://fraudpractice.com/gl-lists.html#

https://blog.bluepay.com/fight-fraud-with-negative-database-services

https://www.riskified.com/blog/fraud-prevention-blacklists-the-ecommerce-sales-killer/

https://www.onlinemerchantcenter.com/mpartners/html/fraud_protection.html

https://pay-lobby.com/en/guides-payment/fraud-management/blacklisting-and-whitelisting

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/

[1] "2017 MRC Global Fraud Survey, Merchant Risk Council, https://www.merchantriskcouncil.org/resource-center/surveys/2017/

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.*