Velocity Checks

Definition/Description

Velocity checks monitor the number of times that certain transaction data elements occur within certain intervals and look for anomalies or similarities to known fraud behavior.

Velocity checks are also used in some rules-based fraud systems. Examples include:

- Looking at the number of transactions (velocity) by a card within a specified period of time (e.g., five transactions in 15 minutes).
- Looking at the total dollar amount for multiple transactions with a card in a specified period of time.
- Checking for fraudsters testing cards by reviewing repeated checks of the card security code or use of address verification.
- Checking for multiple cards being used that are associated with same device or IP address.

For example, if a merchant sells cameras online, it may be expected that customers would have no more than one purchase within a 12-month period. It may be suspicious if a customer bought more than one camera per day from a single computer, keeping in mind that the customer could buy multiple cameras as part of the same order.

Typical data elements used for velocity checks are the email address, phone number, credit card number, billing address and shipping address. Customer name does not work very well, since there could be multiple people with the same name, affecting good customers in the process.

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	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

A velocity check is made up of three or more variables, always including quantity, data element, and timeframe. Examples that help frame velocity checks include:

- How many transactions has a customer completed in the last 24 hours?
- How much has a customer spent in the last 24 hours?
- How many transactions have originated from a single device in the last 24 hours?

- How many orders have been placed with the same credit card number in the last 24 hours? Have the orders had multiple shipping addresses?
- How many transactions have originated from one IP address in the last 24 hours?
- How many billing zip codes have are associated with a customer loyalty card? How often has that loyalty card been used within a given time frame?

How the Technique Works

The database containing selected data elements is accessed or "called" twice. The first time adds to the count of a data element, and the next counts the total number.

The rule for that data element will have a count and time interval component.

The total number is compared to the rule for that element (e.g., "if orders placed with the same card number within 24 hours exceed five"); if the total number exceeds what the rule indicates, the transaction is reviewed further.

More sophisticated velocity controls will incorporate the bespoke activity of a customer or segment of customers to avoid a one-size-fits-none approach that may be either too restrictive and customer unfriendly, or too lenient and therefore not effective at stopping fraud.

Risks Associated with Technique

The risk of a hard velocity decline rule is that it could result in a large volume of false positives which require either raising limits to ineffective levels or scrapping the control altogether. Simple velocity controls can also be reverse engineered by fraudsters who will keep activity just below the alert threshold.

Velocity check implementers must be aware of what customer information is used and how its use complies with privacy rules.

Customer Impact/Level of Friction

Purchase velocity limits often lack transparency to the customer, leading to difficult customer conversations. Customers may feel that the bank or merchant is impeding on their 'rights' by limiting their purchases. Stated cash limits for transactions are generally better understood as long as they are clearly communicated.

Implementation Considerations

The velocity check technique requires a supporting database. Building this database requires:

- Determining what data elements to check.
- Deciding on the number of changes to flag and the time interval to use.
- Refining controls to balance client friction and fraud prevention through ongoing analytics.

This technique performs much better as part of an integrated approach that includes customer spending patterns, known fraud patterns, and an anomaly detection or fraud scoring model.

Using a third-party service that combines data from multiple merchants or banks to track velocity may provide advantages, as merchants will get a much fuller picture of activity by a potential fraudster and have a better chance of discovering fraudulent activities.

Maturity

The velocity check technique has been in use since the early days of ecommerce. Rules-based fraud and risk platforms were utilizing velocity checks at the POS and ATM even before ecommerce.

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

https://chargeback.com/velocity-checks-fraud-prevention/

http://www.fraudpractice.com/gl-veluse.html

https://www.chargebee.com/blog/credit-card-fraud-detection-tools/

https://sift.com/sift-edu/prevent-fraud/velocity-detection

https://due.com/blog/velocity-attacks-avoid-merchant-account/

http://www.fraudpractice.com/gl-velchange.html

https://www.signifyd.com/blog/2013/07/18/velocity-checks-fraud-detection/

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.*