Customer Website/Mobile Behavior

Definition/Description

Customer behavior on websites and mobile devices follows patterns. Variations to those patterns can suggest the likelihood of fraud. Monitoring customer behavior can help to identify fraudsters testing cards and detect bots. In addition, how users navigate to a purchase page can determine patterns of high risk. Machine learning is becoming widely used for monitoring behavior to improve the accuracy of detection.

Monitoring customer website behavior to mitigate payment fraud is relatively new, and approaches vary. Activity can be viewed for an individual user in single session, an individual user across multiple sessions, or an individual user as compared to all other users.

Use cases for this kind of analysis include (but are not limited to) recognizing card testing, detecting bot activity, and determining high-risk patterns in page navigation.

Applicability

Channel	Applicable?	Use Case	Applicable?	Stakeholder	Applicable?
In-app [merchant app]	Yes	Customer onboarding	NA	Merchants	Yes: internal
Mobile browser	Yes	Authentication (onboarding)	NA	Issuers	Yes: internal
Desktop/laptop computer	Yes	Authentication (transaction)	Yes	Issuer processors	NA
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

The merchant embeds a small snippet of computer code (JavaScript or mobile software development kit [SDK]) in their website or mobile application. This code (also known as a "beacon") transmits data to an analytics system when a shopper interacts with the site or app. This data provides the basis for the analysis, with different types of analysis identifying different types of fraud attacks.

Single session behavior analysis is the type most frequently offered by vendors. This method looks at what a user is doing on a website, such as: what pages they are navigating to; how much time they spend on each page; how quickly they fill in forms and text fields; and how often and how quickly they attempt to create accounts, log in or make a purchase. This information is then compared with a model of legitimate shopper behavior.

Viewing behavior over time with cross-session behavior analysis allows detection of account takeover fraud, by identifying when a user's behavior changes from what it was in the past.

Risks Associated with Technique

False positives are the biggest risk. More sophisticated pattern analysis can reduce the false positive risk. The technique can be most effective when combined with other techniques.

Customer Impact/Level of Friction

Monitoring tools work in the background and are transparent to the customer.

Implementation Considerations

The time required to implement such a solution depends the merchant (or merchant's website vendor) priorities and priorities of the any vendor involved.

Maturity

The technology has been around for web sites for approximately 10 years but has only recently become widely used. The technique is mature but being continuously refined, and is becoming a standard offering among fraud service providers (FSP).

Applicable Industry Standards

Each vendor has a propriety methodology.

Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

Further Reading

https://www.pymnts.com/news/security-and-risk/2018/fraudsters-cnp-behavioral-analytics-fraud-prevention-featurespace/

https://www.mastercard.us/en-us/merchants/safety-security/authentication-services/biometrics.html

https://simility.com/blog/fighting-fraud-without-wounding-customer-experience/

https://www.fraud-magazine.com/article.aspx?id=4295002770

http://www.fraudpractice.com/gl-behavior-monitor.html

https://www.riskmanagementmonitor.com/using-adaptive-behavioral-analytics-to-detect-fraud/

https://precognitive.com/2017/10/12/using-behavioral-analytics-detect-ecommerce-fraud/

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.*