

Check ID or Credit Card upon Order Pick-up

Definition/Description

One security or fraud mitigation technique is checking an ID or credit card upon order pick-up. This technique is applicable to: merchants or warehouses who have a buy-online, pick-up in-store (BOPIS) option to ensure that a product is released to the appropriate party; businesses that sell controlled products (e.g., alcohol, firearms, tobacco).

Applicability

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

Technical Features/How the Technique Works

When a customer has placed an order online and is coming to retrieve their merchandise, service, or order, an associate can request an ID and check it to ensure that the name on the order matches the name on the ID. The associate may also check that the customer has the same credit or debit card used to place the order.

Each merchant can tailor how they wish to proceed if this request is not met by the customer. For example, if a customer refuses, a business may wish to continue to allow the pick-up or fulfillment and not place their associates in a situation that may escalate. Or, a business might refuse to release the product unless an ID is shown. Merchants would choose the approach that meets their requirements for customer friction, customer experience, and level of risk.

Risks Associated with Technique

Fake IDs are not difficult to procure by seasoned fraudsters.

Having a customer interact with an associate responsible for the final decision may be risky, impact customer satisfaction, and possibly create a confrontation at time of pick-up if the associate refuses to release the product or service.

Customer Impact/Level of Friction

This technique is familiar to customers since individuals often need to produce a government-issued ID or driver's license for any number of purchasing scenarios:

- Writing a check
- Applying for credit at a bank
- Ordering a drink at a restaurant
- Checking into a hotel
- Picking up certain medication
- Flying
- Starting your transaction online and then picking up in store.
- Picking up a parcel from a shipping company

While use of an ID or credit card check is familiar to customers and therefore considered to be a low friction technique, it may also be a viable option depending on the situation. For example, picking up items over certain dollar amounts may require an ID, while picking up low-cost merchandise may not.

Implementation Considerations

Implementation of this technique can range from easy with little/no cost to more complex with expensive technological solutions.

- Low cost/implementation: Changing standard operating procedures for associates to ask for an ID upon pick-up. Practices can vary by merchant or business.
- Medium cost/implementation: Black-light readers that help associates spot fake IDs by showing holograms. ID validation technology varies by state and store associates will require training.
- High cost/implementation: Several third-party services or vendors have technological solutions that will authenticate the ID or use facial recognition. This approach might require IT integration with existing systems, create privacy considerations on how that data is transmitted or stored, and involve layers of management to monitor performance, effectiveness, and experience.

Maturity

Checking IDs in different environments has been standard practice. Use of technological solutions have varying maturity.

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

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.*