Card-Not-Present (CNP) Fraud Mitigation Techniques

Version 1.0

Publication Date: July 2020

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

EMV® is a registered trademark of EMVCo, LLC in the United States and other countries around the world.

Comments or recommendations for edits or additions to this document should be submitted to: info@uspaymentsforum.org.

Table of Contents

1. Introduction

There is no dispute that card-non-present (CNP) payment fraud is growing and will continue to do so. Moreover, those who commit fraud—fraudsters—are creative and engaged in a relatively low cost but high payoff game. A recent study from Juniper Research[1] indicated that retailers are expected to lose $130 billion in digital CNP fraud between 2018 and 2023.

Security technologist Bruce Schneier offered the following perspective on securing systems against attackers:

> "…security experts like to speak about the attack surface of a system: all the possible points that an attacker might target and that must be secured. A complex system means a large attack surface, and that means a huge advantage for a would-be attacker. The attacker just has to find one vulnerability—one unsecured avenue for attack—and gets to choose the time and method of attack. He can also attack constantly until successful. At the same time, the defender has to secure the entire attack surface from every possible attack all the time. And while the defender has to win every time, the attacker only has to get lucky once. It's simply not a fair battle—and the cost to attack a system is only a fraction of the cost to defend it. Complexity goes a long way to explaining why computer security is still so hard, even as security technologies improve. Every year, there are new ideas, new research results, and new products and services. But at the same time, every year, increasing complexity results in new vulnerabilities and attacks. We're losing ground even as we improve. Complexity also means that users often get security wrong….This doesn't mean that defense is futile, only that it's difficult and expensive.[2]"

Given the difficulty and complexity of securing systems, becoming familiar with techniques to defend against fraud is critical for planning mitigation strategies and evaluating solution alternatives.

1.1 Objective and Audience

The objective of this white paper is 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 intended for payments industry stakeholders who need to understand and make business decisions about implementing technologies that are designed to fight CNP fraud. The primary audiences are business decision makers at issuers, merchants, issuer processors, wallet/online payment service providers (PSPs), and merchant processors/acquirers.

This document refers extensively to other sources for additional information. (See section on "Further Reading" accompanying each technique.)

The U.S. Payments Forum and other industry groups have also written guides on CNP fraud, including the Forum's Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud (2016), CNP Fraud around the World (2017), and True Costs of Fraud (2018).[3] The Accredited Standards Committee

[1] "Retailers to Lose $130bn Globally in Card-Not-Present Fraud over the Next 5 Years," Juniper Research, Jan. 2, 2019, https://www.juniperresearch.com/press/press-releases/retailers-to-lose-130-bn-globally-in-card-fraud.

[2] Schneier, Bruce, "Click Here to Kill Everybody: Security and Survival in a Hyper-connected World," pp. 27-28, W. W. Norton & Company.

[3] https://www.uspaymentsforum.org/working-committees-sigs/card-not-present-fraud-working-committee/.

X9 also published a detailed white paper[4] in 2018 which covers both types of fraud attack vectors as well as means to mitigate fraud from those vectors.

1.2 White Paper Scope

In scope for this white paper are CNP fraud mitigation techniques and categories; out of scope are non-card payments fraud, fraud attack vectors, and card-present fraud.

1.3 Structure/Using this Document

This document has two sections: *general concepts/best practices* to consider with any fraud mitigation approach, and a *listing of selected techniques* that are currently available, along with attributes that will help readers decide which techniques are most relevant to their situations.

For each technique, the section summarizes the following elements:

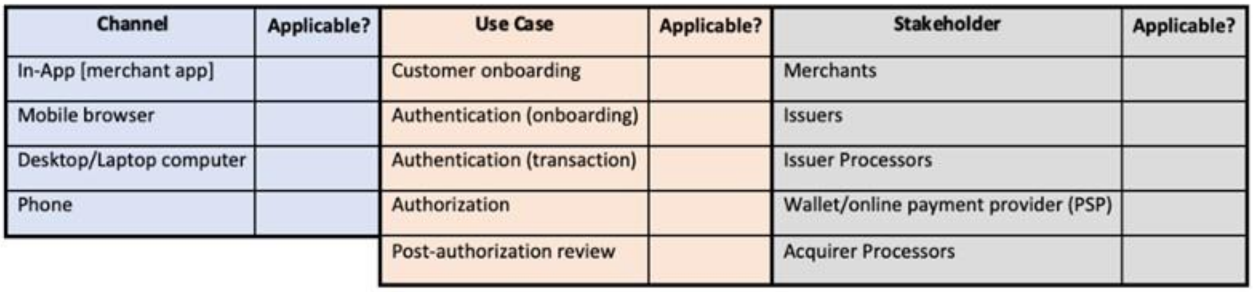
1. Definition/description
2. Applicability to channels, use cases, and stakeholders ("attributes")
3. How the technique works
4. Risks associated with the technique
5. Customer impact: level of friction
6. Implementation considerations
7. Maturity of the technique
8. Applicable industry standards (if available)
9. Publicly available statistics on implementations and use (if available)

In many sections, links are also included for further reading.

Note that the techniques discussions are intended only to provide high-level snapshots to help familiarize readers with factors that may be relevant when assessing the applicability of the techniques described. Providing a comprehensive guide regarding how to assess the applicability of and/or implement these techniques is beyond the scope and intent of this white paper. Accordingly, readers are cautioned that applicability of a given technique may depend on specific facts and circumstances, including the nature and systems of the stakeholder in question, and the white paper may not include (and does not attempt to attempt to address) all factors that may be relevant, including but not limited to, applicable risks, implementation considerations or customer impacts. Readers are advised to consult their professional advisors, the relevant payments industry stakeholders with which they interact, and other sources for detailed information about each technique.

The technique attributes are presented in a table format (see example in Figure 1).

[4] "Card-Not-Present (CNP) Fraud Mitigation In The United States: Strategies For Preventing, Detecting, And Responding To A Growing Threat," ASC X9 TR 48-2018, https://webstore.ansi.org/Standards/ASCX9/ASCX9TR482018.



Channel	Applicable?	Use Case	Applicable?	Stakeholder	Applicable?
In-App [merchant app]		Customer onboarding		Merchants	
Mobile browser		Authentication (onboarding)		Issuers	
Desktop/Laptop computer		Authentication (transaction)		Issuer Processors	
Phone		Authorization		Wallet/online payment provider (PSP)	
		Post-authorization review		Acquirer Processors	

Figure 1. Example Table of Attributes Used with each Technique

2. General Concepts/Best Practices

2.1 Know Your Customer (KYC)

Know your customer (also known as KYC, “know your client,”) is the process of a business verifying the identity of its clients and assessing their suitability for a business relationship, along with the potential risks of illegal intentions. KYC is a series of legally required measures meant to prevent financial crimes (such a money laundering), as well as decrease the risk of fraud. Many countries have a version of KYC; in the U.S., it is mandatory for regulated financial institutions such as banks and money transmitters. Institutions for whom KYC is mandatory may require similar actions for those with whom they do business.

As required by Section 326 of the USA Patriot Act, the Department of the Treasury adopted regulations that require financial institutions to implement reasonable procedures to verify and maintain records relating to the identity of persons seeking to open an account and to determine whether the persons are listed among known or suspected terrorists or terrorist organizations.

These procedures require proper identification from every customer (i.e., a customer identification program), at the time a relationship is established, in order to prevent the creation of fictitious accounts. If a potential customer refuses to produce any of the requested information, the relationship will not be established. Likewise, if the potential customer is not forthcoming with requested follow-up information, any relationship that has already been established may be terminated.

The challenge with KYC is balancing the needs for compliance and risk reduction with the friction that could negatively affect a current or potential customer.

Best practices for KYC will include some form of the following:

- A Customer Identification Program (CIP): collecting information to verify a potential customer’s identity and verifying that information; and checking the person’s name against databases of higher risk persons.
- Customer Due Diligence (CDD): using the above and additional information to assess the potential customer’s risk, often by determining expected transactions in order to flag unusual, and potentially riskier, transactions.
- Enhanced Due Diligence (EDD): requesting additional information from for customers believed to be a higher risk.
- Ongoing monitoring and record keeping.

Further reading:

KYC-brief history

https://urjanet.com/blog/kyc-kyb-brief-history/

https://authenteq.com/the-evolution-of-kyc-part-3/

http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

2.2 Layering Fraud Tools

Fraud is a constant threat in ecommerce. Fraudsters are always looking for ways to penetrate any fraud tool deployed by ecommerce sites. Each tool addresses certain types of fraud, and no tool addresses all types of fraud. Mitigating losses requires more than one technique, a “multilayered” approach.

Many merchants have been using a very limited form of multilayered fraud management for years. For example, any merchant who uses Address Verification Service (AVS) in conjunction with card security codes or 3-D Secure is using a multilayered approach. This example applies fraud mitigation techniques at the point of a transaction. It does not address fraud that begins before the transaction is started (e.g., synthetic identity fraud).

The best solutions—the ones that are increasingly needed—look at all points of the customer journey and include techniques such as adaptive authentication and transaction risk analysis to spot fraud based on device, user behavior and other indicators. While it is not possible to completely protect an ecommerce site from fraud, a recent Association for Financial Professionals report went so far as to suggest that "having a variety of protective measures in place will likely frustrate fraudsters and they'll move on to easier targets."[5]

As with other risk management techniques, stakeholders are encouraged to consider the given techniques in light of their own overall risk appetite in terms of loss prevention versus revenue lost due to the customer friction. Additionally, the sensitivity of a particular control should consider the impact on customer friction of "false positives" (a genuine transaction identified as fraudulent) vs. "false negatives" (a fraudulent transaction identified as genuine).

In general, a layered fraud prevention system will include both passive and active controls:

1. Passive control: tools that monitor for anomalies while allowing non-suspicious traffic to flow unimpeded. These controls are invisible to the customer.
2. Active controls: tools and processes that challenge a user to provide a response, often triggered by a passive control or by a policy set for higher risk activities.

Holistic risk management makes use of both passive and active controls to efficiently separate anomalous activity from low-risk legitimate usage and respond accordingly. This process can help determine whether to allow the requested action to proceed and can incorporate the riskiness of the requested action—i.e., lower risk activities typically may have a lower threshold for proceeding compared to higher risk activities.

Generally, the detection process leads to one of three outcomes:

1. Request approved.
2. Request challenged. The requestor is presented with a challenge which must be completed to continue (i.e., the active control).
3. Request denied.

In an ideal world, all legitimate requests would be approved, and all fraudulent attempts would be denied. However, requests fall along a spectrum of risk. The best systems can isolate the majority of good attempts from the bad attempts; however, a certain number will be indeterminate and require a challenge.

Effective risk management typically requires balancing the volume of challenges against the potential for loss—i.e., balancing the impact on customer experience against fraud prevention. Layering more advanced forms of fraud detection solutions may greatly improve the system's ability to discriminate

[5] "2019 Payments Fraud and Control Survey Report," Association for Financial Professionals, April 2019, https://www.jpmorgan.com/content/dam/jpm/commercial-banking/documents/fraud-protection/2019-afp-final-report-highlights.pdf.

between good and bad activities and enable organizations to achieve the competing objectives of fraud prevention and low customer friction.

A challenge method will often take into account both the friction it causes the legitimate customer and the security it provides. In order to manage customer friction security should be aligned with the risk of the particular activity that is being requested by the end user.

Further reading

https://www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/layered-approach-fraud-detection-prevention-106072.pdf

https://seon.io/resources/multi-layered-fraud-prevention-what-is-it-and-how-to-do-it-right/

https://chargebacks911.com/credit-card-fraud-detection-techniques/

https://www.ncr.com/financial-services/enterprise-fraud-prevention/fractals

2.3 Tokenization

In payment processing, tokenization is the process of substituting sensitive data with a non-sensitive equivalent. This sensitive data could be a card primary account number (PAN) or other personally identifiable information (PII).

The non-sensitive data is referred to as a token. It is a mathematically generated number that has no extrinsic or exploitable meaning or value. Thus, if the tokenized information is stolen, it has no value.

Additional information on tokenization can be found in the U.S. Payments Forum white paper, EMV Payment Tokenization Primer and Lessons Learned,[6] which provide definitions of the different forms of tokenization and details on EMV payment tokenization.

2.4 Vendor Selection

When building a fraud prevention infrastructure, companies routinely assess and address factors such differentiation, technology, or skill gaps/needs. As gaps are identified, using a build/buy/partner framework can be a useful decision tool and process.

A company can build internally, partner with one of more vendors, or buy a firm. The decision will depend on factors such as company's culture, budget, and implementation timeline.

Partnering with a vendor often has the fastest time to market, low amount of cost/risk for acquisition, and less impact on internal resources, plus may provide some flexibility (e.g., being able try before you buy). Depending on the terms of a contract, however, a partnership may lock a company in to a specific solution for a long period of time, have potentially high integration costs, provide the least amount of control vs. build/buy a company, and, over the long term, be an expensive option.

Working with a single vendor may often be a better option than either building in-house capability or piecing together a layered strategy with multiple vendors, particularly for smaller firms, since it reduces complexity for vendor integration and management. Understanding specific requirements is important, since there may not be a single vendor that satisfies all needs.

[6] https://www.uspaymentsforum.org/emv-payment-tokenization-primer-and-lessons-learned/

The items noted in this section offer a framework to use in making a build/buy/partner decision. Most of the items listed below will apply to any partnering or purchase process. Many of the items apply when considering whether or not to build in house.

Partner vendor selection can be done via a request for proposal (RFP), or through a test and trial of multiple vendors' services. Careful consideration of requirements may help a company choose which route they prefer. For example, while an RFP may provide a more uniform understanding of vendors and competitors in an industry, it can be very time consuming, arduous, and slow. Going directly to vendors and testing their offers may be faster than an RFP, but a company may not get a full understanding of what differentiates vendor A from vendor B.

Although each use case can be different, a few selection criteria include (not in order of priority):

- Willingness to work with the company on pricing and service level guarantees
- Client service – responsiveness to customer needs
- Contractual terms
- Geographic coverage
- References
- Industry credibility
- User experience: are the user-facing interfaces good? Are APIs easy to work with?
- Ability to provide multiple fraud prevention services
- Ability to meet requirements (including technology, growth, scalability, and flexibility)
- Compatibility of vendor organization with customer organization. For example, if the purchasing company does agile development and the potential vendor follows the waterfall method, are the operating models compatible?
- Scalability
- Competitive pricing
- Strength of project management team
- Strength of account team
- Change management capabilities
- Financial stability
- Vendor innovativeness
- Supplier diversity. Is the potential vendor vulnerable to supply chain issues?
- Legal compliance and internal controls
- Disaster recovery/business continuity

3. CNP Fraud Mitigation Techniques and Attributes

This section provides a summary of the selected fraud prevention techniques that are profiled in this white paper, as well as those that are not covered. Each technique has attributes assigned: the applicable channels and use cases, and the applicability of each technique to different stakeholders.

The review of the attributes in this section is intended to provide information that may help readers when deciding which techniques to investigate in more depth. Each technique heading links[7] to the related section in the white paper.

Attributes defined for each technique are:

Channel	Applicable?
In-app [merchant app]	
Mobile browser	
Desktop/laptop computer	
Phone	

Possible conditions

- Yes: used for the channel
- NA: not applicable for channel

Use Case	Applicable?
Customer onboarding	
Authentication (onboarding)	
Authentication (transaction)	
Authorization	
Post-authorization review	

Possible conditions

- Yes: applicable
- NA: not applicable

Stakeholder	Applicable?
Merchants	
Issuers	
Issuer processors	
Wallet/online payment providers	
Acquirer processors	

Applicability of the technique applies stakeholders

- Yes: internal (for use by the stakeholder whose fraud rates are affected)
- Yes: for clients (potentially offered to the stakeholder's client as product—usually by a vendor)
- NA: not applicable

[7] Additional techniques are expected to be added in future versions of the document; those currently being written are listed below.

One-Time-Passcode (OTP) Display Card

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

Customer Website/Mobile Behavior

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

Interactive Voice Response (IVR) Voice Verification

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

Negative/Positive Database

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

Velocity Checks

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

Address Verification Service (AVS)

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

Browser Cookies

Channel	Applicable?	Use Case	Applicable?	Stakeholder	Applicable?
In-app [merchant app]	NA	Customer onboarding	NA	Merchants	Yes: internal
Mobile browser	Yes	Authentication (onboarding)	NA	Issuers	NA
Desktop/laptop computer	Yes	Authentication (transaction)	Yes	Issuer processors	NA
Phone	NA	Authorization	Yes	Wallet/online payment providers	NA
		Post-authorization review	Yes	Acquirer processors	Yes: for clients[8]

Multifactor Authentication

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	NA
Phone	Yes	Authorization	Yes	Wallet/online payment providers	Yes: for clients
		Post-authorization review	Yes	Acquirer processors	Yes: for clients

Check ID or Credit Card upon Order Pick-up

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

[8] Browser cookies are typically implemented by whoever provides the website.

Transaction Alerts/Controls/Notification Services

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

Static Card Security Code

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	NA
Desktop/laptop computer	Yes	Authentication (transaction)	Yes	Issuer processors	NA
Phone	Yes	Authorization	Yes	Wallet/online payment providers	Yes: for clients
		Post-authorization review	NA	Acquirer processors	Yes: for clients

Fraud Scoring

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

Common Point-of-Purchase Analysis

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

Note: the following techniques are not included in this white paper, but may be added to a future update.

- EMV 3DS 2.0
- Real-time predictive risk scoring/risk analytics
- Adaptive rules-based authentication
- Identity and verification (ID&V)
- Machine learning/AI, event monitoring and anomaly detection
- Security/acquirer token
- Virtual credit card/single-use PAN
- Behavioral analytics/behavioral biometrics
- Knowledge-based authentication (KBA)
- Push-based multifactor authentication (MFA) with mobile public key infrastructure (PKI)
- Consumer Device Cardholder Verification Method (CDCVM)/On-Device Cardholder Verification Method (ODCVM)
- Dynamic cryptogram
- Device familiarity, risk, and attack signals
- Static PIN or passcode
- Out-of-band one-time passcode (OTP)
- Physical biometrics: hardware
- Mobile network operator (MNO) risk scoring/MNO intelligence
- EMV payment tokenization
- Secure Remote Commerce (SRC)
- W3C web payments handler API
- FIDO

4. One-Time-Passcode (OTP) Display Card

4.1 Definition/Description

An OTP display card is a token in credit card format with a display, an on-off button, and a PIN pad (optional). The card generates a one-time passcode that is used to authenticate the cardholder attempting to access a specific resource or sign a transaction. The PIN pad protects access to the OTP and enables transactions to be signed. If the OTP display card is an EMV chip card, the card can act as a both the Chip Authentication Program (CAP) reader[9] and the payment card.

An OTP display card is an alternative form factor to other OTP generating tokens (e.g., dongles).

4.2 Applicability

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

4.3 Technical Features/How the Technique Works

When a website asks for entry of a one-time passcode, the cardholder presses the on/off button on the card, enters a PIN if requested, and then enters the code displayed on the card on the website. The server associated with the OTP solution will determine whether the code is correct and allow or not allow login. When using the card to sign a transaction, a challenge-response algorithm is used with a dialogue between the cardholder and the card.

4.4 Risks Associated with Technique

The OTP display card has a shelf life based on the presence of a battery on the card. Depending on the type of algorithm used (time-based, or event-based) the card life will vary. The card issuer needs to issue a new card before the battery fails to prevent the cardholder from not being able to use the card for login.

[9] A handheld device that accepts a chip card and has a keypad and display. The CAP reader is used to provide second factor of authentication for CNP transactions. Additional information can found at https://en.wikipedia.org/wiki/Chip_Authentication_Program.

The strength of the technique depends on the cryptography used. This technique is vulnerable to a 'man in the middle' attack.

4.5 Customer Impact/Level of Friction

The card form factor provides advantages to cardholders since cards can be carried in a wallet. However, in the case of cards with PIN pads, some users with large fingers may experience difficulty pressing the appropriate keys.

4.6 Implementation Considerations

The card issuer needs to have a matching server to authenticate the OTPs generated by the card. The server can be offered as a cloud service.

OTP display cards are more expensive than other OTP devices (such as traditional dongles or clamshell tokens); however, they provide more convenience for the cardholder.

4.7 Maturity

The OTP display card is a mature technology.

4.8 Applicable Industry Standards

OTP algorithm specifications are either open (e.g., OATH) or proprietary to a vendor.

4.9 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

4.10 Further Reading

https://openauthentication.org

https://blog.bluepay.com/dynamic-cvv-solution-comparisons

5. Customer Website/Mobile Behavior

5.1 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.

5.2 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

5.3 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.

5.4 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.

5.5 Customer Impact/Level of Friction

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

5.6 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.

5.7 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).

5.8 Applicable Industry Standards

Each vendor has a propriety methodology.

5.9 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

5.10 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/

6. Interactive Voice Response (IVR) Voice Verification

6.1 Definition/Description

IVR voice verification is a biometric authentication technique used when a telephone call is involved—principally with call centers. It provides additional security in a channel that depends heavily on humans, and, as a result, is vulnerable to fraud resulting from social engineering attacks. Without IVR voice verification, fraud can be committed by answering security questions using compromised customer data. IVR voice verification is one of the few, if not the only, biometric method available to call centers.

Voice recognition is more customer friendly than knowledge-based authentication, and requires less time when interacting with customers, improving call center processes.

6.2 Applicability

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

6.3 Technical Features/How the Technique Works

Voice biometrics require a "voiceprint" for each customer which is then used for authentication. Words are broken down into segments based on dominant frequencies and are stored digitally in a database. There are two common methods of voice recognition: active and passive. Active requires the customer to speak a set phrase to create the voiceprint. Passive uses normal conversation to create the voiceprint.

Voiceprints associated with known fraudsters can also be used to identify risks.

6.4 Risks Associated with Technique

The European Union General Data Protection Regulation (GDPR) lists biometrics as one of the methods that requires customers to opt-in. Organizations need to be very aware of privacy issues when implementing any system that uses biometrics.[10]

[10] "The importance of consent and privacy when deploying voice biometrics," PrivSec report, June 24, 2019, https://gdpr.report/news/2019/06/24/the-importance-of-consent-and-privacy-when-deploying-voice-biometrics/

Privacy poses an issue for this technology, as with all biometric technologies. Biometrics are unique to individuals and cannot be replaced if compromised. The manner in which the voiceprints are stored is critical.

Hacking using a pre-recorded voice sample is a risk. This can be prevented using a challenge-response system that requires the user to repeat a requested word or phrase.

Voiceprints can be affected by physical condition, heightened moods, or background noise, resulting in a failed verification.

6.5 Customer Impact/Level of Friction

Other than the initial step of providing the voice sample, this technique has minimal to no impact on customers.

6.6 Implementation Considerations

Vendors provide IVR software packages for IVR, and consultant companies may provide ratings of the various packages. Implementers should review vendor offerings to find the one best suited to their requirements.

Although not a requirement, companies may want to verify that the IVR voice recognition software has been assessed by a reputable company that determines the security risk of third-party software.

6.7 Maturity

Although the concept of using voice biometrics has been around since 1867 when Alexander Melville Bell invented Universal Alphabetics, it was in 1976 that Texas Instruments created a device that could accurately determine an individual's voiceprint. The first international patent for voice recognition was filed in 1983. In the late 1990s, voice recognition was used at U.S.-Canada border crossing. The private banking division of Barclays was the first to deploy this technology as the primary means of identifying call center customers in 2013.[11] The technology has advanced so significantly that some IVR companies guarantee a 99.99% success rate for identifying individuals.

6.8 Applicable Industry Standards

The ANSI/NIST-ITL 1-2011 standard documents the data format standards needed for the interchange of biometric data such as IVR. ISO/IEC JTC 1/SC 37 is another standard developed for biometrics.

6.9 Publicly Available Statistics on Implementations and Use

According to Voicevault, it is expected that the global market for speech and voice biometrics to be $5.1 billion by 2024.[12]

6.10 Further Reading

https://www.nice.com/engage/real-time-authentication/

[11] https://en.wikipedia.org/wiki/Speaker_recognition

[12] "Let's Get the Facts Straight about Voice Biometrics," Voicevault, May 18, 2016, https://voicevault.com/lets-get-facts-straight-voice-biometrics/

https://www.sestek.com/2018/11/fighting-against-call-center-fraud-with-voice-biometrics/

https://www.nice.com/engage/blog/passive-voice-biometrics-in-an-active-channel-2287/

https://www.biometricupdate.com/wp-content/uploads/2014/05/Voice-Biometrics.pdf

https://voicevault.com/the-difference-between-active-and-passive-voice-authentication-in-contact-centers/

7. Negative/Positive Database

7.1 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

7.2 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

7.3 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.

7.4 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.

7.5 Customer Impact/Level of Friction

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

7.6 Implementation Considerations

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

7.7 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.[13]

As noted in Section 7.4, negative and positive databases are limited in their effectiveness, so are typically used as part of a layered approach.

7.8 Applicable Industry Standards

This technique has no applicable industry standards.

7.9 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

7.10 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

[13] "2017 MRC Global Fraud Survey, Merchant Risk Council, https://www.merchantriskcouncil.org/resource-center/surveys/2017/

8. Velocity Checks

8.1 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.

8.2 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

8.3 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?

8.3.1 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.

8.4 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.

8.5 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.

8.6 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.

8.7 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.

8.8 Applicable Industry Standards

This technique has no applicable industry standards.

8.9 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

8.10 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/

9. Address Verification Service (AVS)

9.1 Definition/Description

AVS allows CNP merchants to check the cardholder billing address with card Issuer. The merchant includes the AVS request as part of the authorization.

9.2 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

9.3 Technical Features/How the Technique Works

A merchant can use AVS during checkout to verify the customer’s billing address and/or zip code against the information on file at the issuer.

AVS can be used as a pre-authorization step known as an 'address verification,’ or the AVS request can be embedded in the authorization request to the issuer.

The issuer responds with either a full match, partial match, or no match. If it is part of an authorization request, the issuer will embed the AVS response within the approval or decline message.

The merchant may use the AVS response to augment the response from the issuer. Most typically, a merchant may choose to decline a transaction, even if the issuer approves the transaction, if the AVS check returns a 'no match.'

9.4 Risks Associated with Technique

AVS typically would be used as part of a layered fraud solution. Fraudsters often have access to the cardholder’s address information along with the stolen card credentials, so an AVS match alone should not be accepted as proof of a legitimate transaction.

False positives are a risk. Since AVS requires matching numerical fields in an address, which is often in a non-structured format, false declines are a possibility.

9.5 Customer Impact/Level of Friction

The process requires that the customer enter billing information when checking out or when establishing an account with the merchant. The customer needs to be aware of the address on file with the issuer and ensure it is up to date.

9.6 Implementation Considerations

Billing information is standard KYC information and capturing it is relatively easy.

Integration is not complicated. Using AVS is a common practice and is incorporated in the existing authorization message infrastructure.

AVS requires a low level of investment and provides a low level of protection. The technique is a standard part of typical CNP risk management and is used as part of a layered approach.

9.7 Maturity

AVS has been in use for many years and is a standard tool for addressing CNP fraud risk.

9.8 Applicable Industry Standards

Specifications for AVS vary by payment network.

9.9 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

9.10 Further Reading

https://www.signifyd.com/resources/fraud-101/detection/avs-how-it-works/

https://www.verifi.com/kb/what-is-address-verification-service-avs/

https://www.vantiv.com/vantage-point/safer-payments/address-verification-service

10. Browser Cookies

10.1 Definition/Description

Browser identifiers are a subset of more general device identifiers that provide a means to identify and later recognize a user's device. One the first methods of doing this was browser cookies.

Browser cookies were one of the first tools enterprises used for authentication and fraud detection. Cookies allow a device to be tagged and used as the "something you have" component of the authentication process, replacing hardware tokens. If a device is unknown, the enterprise could use additional step-up authentication measures.

10.2 Applicability

Channel	Applicable?	Use Case	Applicable?	Stakeholder	Applicable?
In-app [merchant app]	NA	Customer onboarding	NA	Merchants	Yes: internal
Mobile browser	Yes	Authentication (onboarding)	NA	Issuers	NA
Desktop/laptop computer	Yes	Authentication (transaction)	Yes	Issuer processors	NA
Phone	NA	Authorization	Yes	Wallet/online payment providers	NA
		Post-authorization review	Yes	Acquirer processors	Yes: for clients[14]

10.3 Technical Features/How the Technique Works

Browser cookies allow a merchant to identify familiar devices, by associating bits of data to a specific device/user. Cookies are small amounts of data stored as text files on a browser.

For example, when a user visits a website, the site may deliver a cookie to the browser identifying the user as "User X." If the user leaves the site and returns to it again, that cookie will be used by the website to recognize that the user is the same User X that was at the site previously.

Cookies necessarily contain, at a minimum, two pieces of data: a unique user identifier and some information about that user.

10.4 Risks Associated with Technique

Cookies can be easily erased, making the device anonymous and usually requiring stepped-up authentication.

Modern device ID solutions have become significantly more sophisticated than the early cookie-based solutions, so browser cookies are often used as part of a multi-layered solution.

[14] Typically done by whoever provides website.

10.5 Customer Impact/Level of Friction

Cookies are invisible to the customer. However, customers will experience friction if a cookie is deleted and they are asked to authenticate their identity through a different method.

10.6 Implementation Considerations

The merchant website would be implemented to store cookies on users' browsers and use them to identify returning customers.

10.7 Maturity

Internet browser cookies were first patented in the late 1990s. They are widely used today.

10.8 Applicable Industry Standards

The Internet Engineering Task Force (IETF) 6265 standard defines cookies.

10.9 Publicly Available Statistics on Implementations and Use

Browser cookies are very widely used. Published statistics are not available.

10.10 Further Reading

https://securityintelligence.com/why-device-id-may-not-be-enough-to-stop-fraud/

https://www.whoishostingthis.com/resources/cookies-guide/

https://sift.com/sift-edu/prevent-fraud/device-ip-analysis

Cookie patent:
https://worldwide.espacenet.com/patent/search/family/024155035/publication/US5774670A?q=pn%3DUS5774670

11. Multifactor Authentication

11.1 Definition/Description

Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

Multifactor authentication combines two or more independent factors:

- Something you know ("knowledge") – for example, passwords, PINS, knowledge-based answers
- Something you have ("possession") – for example, card, bracelet, key fob, mobile phone
- Something you are ("inherence") – for example, fingerprint, voice, facial image

A system that depends on only one factor (e.g., a password) is vulnerable to fraud. MFA reduces that vulnerability by adding one or more unaffiliated factors.

A variation of MFA is "out-of-band" authentication. With out-of-band authentication, each factor is delivered through a separate communication channel. A one-time password delivered through a hard token with a user-provided password is an example of two factors delivered though different communication channels.

Examples of MFA include:

- Swiping or inserting a card and entering a PIN.
- Logging into a website and being requested to enter an additional one-time password
- Swiping/inserting a card, scanning a fingerprint, and answering a security question.
- Using a USB hardware token with a desktop computer to generate a one-time passcode and using the one-time passcode to log into a VPN client.
- Using voice recognition on a phone call.[15]

11.2 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	NA
Phone	Yes	Authorization	Yes	Wallet/online payment providers	Yes: for clients
		Post-authorization review	Yes	Acquirer processors	Yes: for clients[16]

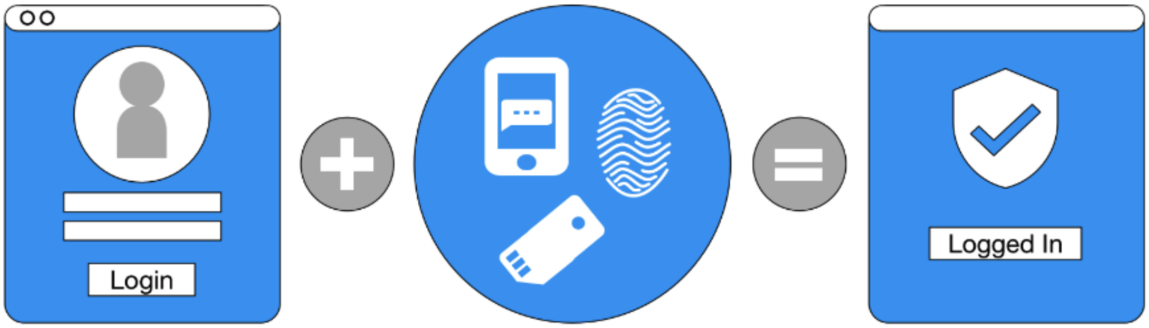
[15] This method is explained in Section 6.

[16] Often done by whoever provides website.

11.3 Technical Features/How the Technique Works

With MFA, the customer is asked for two or more factors—typically a password ("something you know") and at least one other factor. The additional factor or factors come from different sources, including:

- "Something you have", such as
  - One-time password delivered through SMS
  - One-time password delivered through a hard token; the hard token can be separate device or embedded in a plastic card.
  - One-time password delivered through an application
- "Something you are" — biometric authentication, such as
  - Fingerprint ID
  - Face ID
  - Iris scan



Source: NIST

Figure 2. Using Multifactor Authentication for Login

Many factors can be used, but all are not equally convenient and safe. A very secure second factor may increase customer friction and decrease completion of a transaction, and so be less beneficial to a business. The disadvantages of some factors can be balanced by the advantages of others.

Despite greater security, adding authentication factors increases the effort and time it takes to authenticate a user and authorize access. Using MFA trades off customer friction for increased security.

MFA techniques typically involve more than one party, such as an issuer and a vendor. It is not common for one stakeholder to offer all factors internally.

11.4 Risks Associated with Technique

Some methods of sending the second factor are more secure than others.

Using SMS to send one-time passwords is vulnerable to hacking. In 2016, the National Institute of Standards and Technology (NIST) withdrew support for SMS-based two-factor authentication, pointing to the risk of interception or spoofing.

App-based second factor generators are more secure. These require customers to have their mobile devices on hand; however, the applications can be hacked.

Hardware tokens can be even more secure. However, they are costly and can be misplaced by customers.

Biometrics are convenient, but, if compromised, can eliminate that factor completely.

Given the potential risks of MFA alone, it is often used as part of a layered approach.

11.5 Customer Impact/Level of Friction

All MFA methods involve some customer friction; the amount depends on the method used. Using a hardware token, for example, causes significant friction. If a time limit is required for use, the friction can be greater. Biometric authentication generally causes much less friction.

11.6 Implementation Considerations

As with customer friction, implementation difficulty depends on the MFA method used. Using a password plus a one-time password delivered via SMS is relatively easy to implement. Offering hard tokens or implementing biometrics generally requires significantly more time and resources.

11.7 Maturity

Patents for multi-factor authentication were issued as early as 1995.[17] Widespread use did not begin until the middle of the following decade.

11.8 Applicable Industry Standards

Industry standards for MFA include:

- NIST SP 800-63 Digital Identity Guidelines
- FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF) and the Client to Authenticator Protocols (CTAP)

11.9 Publicly Available Statistics on Implementations and Use

A categorized list of websites that have implemented two-factor authentication can be found at www.twofactorauth.org.

11.10 Further Reading

https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication

https://www.onelogin.com/learn/what-is-mfa

https://www.protectimus.com/blog/two-factor-authentication-types-and-methods/

[17] “Kim Dotcom claims he invented two-factor authentication—but he wasn’t first,” ars Technica, May 23, 2013, https://arstechnica.com/information-technology/2013/05/kim-dotcom-claims-he-invented-two-factor-authentication-but-he-wasnt-first/

12. Check ID or Credit Card upon Order Pick-up

12.1 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).

12.2 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

12.3 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.

12.4 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.

12.5 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.

12.6 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.

12.7 Maturity

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

12.8 Applicable Industry Standards

This technique has no applicable industry standards.

12.9 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

12.10 Further Reading

Additional resources are not available.

13. Transaction Alerts/Controls/Notification Services

13.1 Definition/Description

Transaction alerts are generally an issuer-based control that alerts cardholders of particular activities, which can include both purchase transactions as well as non-monetary actions (such as change of address or activation of a new card). Alerts can also be triggered based on preset thresholds (i.e., alert if the credit limit is utilized > x% or if a payment is due).

13.2 Applicability

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

13.3 Technical Features/How the Technique Works

A cardholder would receive an alert message based on a particular activity on their account. Alerts can be delivered in a variety of channels, with in-app push notifications, SMS text, and e-mail being the most popular. Outbound calls are generally not used for alerts except in the case of calls to verify suspicious activity. Certain alerts can also be sent by physical mail, but these are generally confirmations related to account information changes.

Alerts can be set up as mandatory, opt out or opt in depending on type of activity involved and the risk tolerance of the bank.

- Mandatory or opt out would generally be used for suspicious activity alerts and payment due notices.
- Opt-in would generally be set up for specific transaction parameters.
  - A further option would be for a cardholder to specify certain transaction types that should be declined.

Types of activity that could generate an alert include:

- Authorization activity
  - Transactions from a certain POS mode (e.g., ecommerce, keyed).
  - Transactions > $x
  - Transaction amount > baseline spending $x
  - All transactions
  - Transactions at a certain merchant category

    - One small CNP transaction followed by a big purchase
- Payments
    - Payment due
    - Payment posted
- Account changes
    - Authorized user added
    - Address change
    - Phone change
- Geolocation
    - New place, first transaction with large amount
    - Two card-present transactions at different locations in short period of time
- Other
    - Card activated
    - Replacement card ordered
    - Card mailed

13.4 Risks Associated with Technique

This technique has few risks since the cardholder opts in to participate.

13.5 Customer Impact/Level of Friction

Friction varies based on the delivery channel and frequency of the alerts. Since most alerts do not require a cardholder action, friction is lower than if the customer was specifically required to respond before completing a transaction.

13.6 Implementation Considerations

Implementation of this technique requires:

- Determining what types of actions will trigger alerts, to identify which authentication and posting processes need to be linked to a communication process.
- Determining delivery channels, which will drive complexity, especially if one or more channels are managed through a vendor service.
- Determining how opt-in selections are made. Selection needs to be made available through self-service channels (e.g., online, mobile) as well as through an internal console which can be accessed by phone agents and back office personnel.
- Implementing security approaches that, at a minimum, need to log any changes made to alert thresholds.

Integration complexity is moderate and depends on the channels, activity types and level of integration that already exists between them.

Implementers will need to balance their desired level of investment in preventative tools and risk appetite. Alerts will provide additional protection above and beyond internal detection tools as cardholders know their activity the best. However, the bank cannot rely on cardholders to police their usage as a control and typically use alerts in conjunction with a robust fraud mitigation strategy. In addition, the sheer volume of alerts can cause some cardholders to tune out or turn off the functionality.

13.7 Maturity

Electronic alerts have been in use approximately as long as online banking. Alerting functionality is a key service in mobile banking apps.

13.8 Applicable Industry Standards

This technique has no applicable industry standards.

13.9 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

13.10 Further Reading

https://www.thebalance.com/credit-card-fraud-alert-notifications-4135739

https://usa.visa.com/visa-everywhere/security/transaction-alerts.html

14. Static Card Security Code

14.1 Definition/Description

A card security code (CSC) is a security feature that is used with CNP transactions. The card security code is also known as card verification data (CVD), card verification number, card verification value (CVV), card verification value code, card verification code (CVC), verification code (V-code or V code), or signature panel code (SPC). Major payment networks use the following names:

- Visa: Card Verification Value 2 (CVV2)
- Mastercard: Card Validation Code 2 (CVC2)
- Discover: Card Identification Data (CID)
- American Express: Card Identification Number (CID)

The CSC is supplemental to the primary account number (PAN) that is embossed or printed on most cards, and is three or four digits depending on the payment network.

The CSC is printed on the card, and when used, provides an indication that the cardholder possesses the card at the time of transaction.

14.2 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	NA
Desktop/laptop computer	Yes	Authentication (transaction)	Yes	Issuer processors	NA
Phone	Yes	Authorization	Yes	Wallet/online payment providers	Yes: for clients
		Post-authorization review	NA	Acquirer processors	Yes: for clients

14.3 Technical Features/How the Technique Works

The cardholder provides the CSC to the merchant at the time of the transaction. The CSC is sent to the issuing bank as part of the authorization request. The issuing bank uses the code in deciding whether to authorize the transaction.

14.4 Risks Associated with Technique

The technique is vulnerable to methods such as keylogging, where keyboard input is captured, and phishing, where the cardholder is tricked into providing the code to a fraudster.

Because the static CSC is printed on the card, if the card has been stolen or information on the card copied, whoever has access to that card can potentially make online purchases.

14.5 Customer Impact/Level of Friction

Requiring a CSC introduces some friction into the transaction since the customer must manually enter the code. Since the customer will also be entering the card number and expiration date, the additional effort is small. However, the CSC is not stored by the merchant, so cardholders will need to reenter it when checking out at merchants where other card data is on file.

14.6 Implementation Considerations

Static CSC implementation requires low effort. Because CSCs are widely used, they are a part of virtually all shopping carts.

14.7 Maturity

The CSC technique was originally developed in the UK as an 11-character alphanumeric code by Equifax employee Michael Stone in 1995.[18] The concept was adopted by the UK Association for Payment Clearing Services (APACS)[19] and streamlined to the three-digit code known today. MasterCard started issuing CVC2 numbers in 1997, and Visa issued them in the U.S. by 2001.[20]

14.8 Applicable Industry Standards

This technique has no applicable industry standards.

14.9 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

14.10 Further Reading

https://en.wikipedia.org/wiki/Card_security_code

https://www.cvvnumber.com/cvv.html

https://chargebacks911.com/card-security-codes/

https://www.merchantmaverick.com/what-is-cvv2-cvv-checks/

https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/

[18] https://en.wikipedia.org/wiki/Equifax

[19] https://en.wikipedia.org/wiki/Association_for_Payment_Clearing_Services

[20] https://en.wikipedia.org/wiki/Card_security_code

15. Fraud Scoring

15.1 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.

15.2 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

15.3 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.

15.4 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.

15.5 Customer Impact/Level of Friction

This technique has no impact on customers at checkout.

15.6 Implementation Considerations

Fraud engines are typically sourced from a third-party vendor. While they can be built internally, this limits the effectiveness, as noted in Section 15.4, due to the smaller dataset.

15.7 Maturity

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

15.8 Applicable Industry Standards

This technique has no applicable industry standards.

15.9 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

15.10 Further Reading

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

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

16. Common Point-of-Purchase Analysis

16.1 Definition/Description

Common point-of-purchase (CPP) analysis is a technique that helps determine the source of a card breach and, with that, indicates the likelihood that specific cards have been compromised. This helps issuers decide which cards need to be canceled and re-issued.

When investigating cards flagged with fraudulent activity or when researching compromised cards being sold or handled in an illicit fashion (e.g., through dark web activity), issuers may analyze authorization history on these cards to triangulate a common point where the cards were used and subsequently compromised.

A CPP happens only after cards have been identified as compromised or an incident has been reported. Using CPP analysis does not prevent all losses related to a breach; instead, it allows affected issuers to mitigate additional fraud related to that breach.

16.2 Applicability

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

16.3 Technical Features/How the Technique Works

When fraud is reported or a card is suspected of being compromised, an issuer flags the card and the places where the card was previously used. Repeating this process on multiple cards may show common points of purchase—merchants—where the cards were likely compromised. This allows an issuer to identify additional cards used at those merchants that may also be compromised, even though they have not yet experienced fraud, and take appropriate action.

Large issuers have the staff and transaction volume to do CPP analysis for themselves. Smaller issuers typically do not.

Vendors aggregate volume from many issuers to flag CPPs and potentially breached portfolios.

16.4 Risks Associated with Technique

A card issuer using results from a CPP analysis must make its own decision about which cards to cancel and re-issue. Each cancellation and reissuance has a direct cost, and may have an indirect cost—e.g., cardholders may reduce spend if a card has been cancelled and re-issued due to suspected fraud.

16.5 Customer Impact/Level of Friction

This technique initially has no impact on customers if the cardholder’s card is unaffected.

16.6 Implementation Considerations

Issuers and vendors implementing a successful CPP analysis program will need access to authorization/transaction history for their card populations. Additionally, issuers and vendors may employ various research methods to identify compromised cards online and on the dark web.

16.7 Maturity

The practice of CPP analysis has been present and active with issuer for over 10 years.

16.8 Applicable Industry Standards

This technique has no applicable industry standards.

16.9 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

16.10 Further Reading

https://finance.uw.edu/ps/sites/default/files/Fraud%20Prevention%20Best%20Practices.pdf

https://www.sas.com/en_us/insights/articles/risk-fraud/common-point-of-purchase.html

17. Legal Notice

This document is provided solely as a convenience to its readers. While great effort has been made to ensure that the information provided in this document is accurate and current, this document does not constitute legal or technical advice, should not be relied upon for any legal or technical purpose, and all warranties of any kind, whether express or implied, relating to this document, the information or materials set forth or otherwise referenced herein, or the use thereof are expressly disclaimed, including but not limited to all warranties as to the accuracy, completeness or adequacy of such information or materials, all implied warranties of merchantability and fitness for a particular purpose, and all warranties regarding title or non-infringement. All third party materials referenced herein are the property of their respective owners, the U.S. Payments Forum is not responsible or liable for the content or use thereof, and all references to or summaries of such third party materials are qualified by the actual third party materials, as made available by such third parties. Stakeholders interested in CNP fraud mitigation techniques are strongly encouraged to consult with their respective payment networks, acquirer processors, and appropriate professional and legal advisors regarding all aspects of implementation, prior to implementation.

18. Appendix: KYC – A Brief History

In 1950, the Federal Deposit Insurance Act[21] was passed to govern the Federal Deposit Insurance Corporation (FDIC). The bill included regulations that banks must comply with in order to remain insured by the FDIC. These formed the foundation of modern KYC laws.

In 1970, the U.S. Congress passed the Bank Secrecy Act (also known as the Federal Deposit Insurance Act Amendments). The BSA is an amendment to the Federal Deposit Insurance Act and requires banks to file five types of reports with the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) and the Treasury Department:

1. Currency Transaction Reports (CTR): Cash transaction that exceeds $10,000 in one business day (can include multiple transactions).
2. Suspicious Activity Reports (SAR): Any cash transaction where it looks like a customer is trying to skirt BSA reporting requirements.
3. Foreign Bank Account Report (FBAR): Any U.S. citizen or resident that owns a foreign bank account with at least $10,000 is required to file an FBAR report each year.
4. Monetary Instrument Log (MIL): Banks must keep a record of all cash purchases of monetary instruments (e.g., money orders, cashier's checks, traveler's checks) valued between $3,000 and $10,000 for at least five years.
5. Currency and Monetary Instrument Report (CMIR): Anytime a person or institution that physically transports monetary instruments in excess of $10,000 into or outside of the U.S. must file a CMIR.

In 2001, the U.S. federal government passed the USA Patriot Act. Title III of the Act (the "International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001") included a series of regulations designed to limit the power and funding of terrorist organizations. The Act required banks to develop Customer Identification Programs (CIP) that would be incorporated into their Bank Secrecy Act and anti-money laundering compliance program. CIP programs require banks to:

- Verify the identity of any customer seeking to open an account.
- Maintain records of that CIP verification process for five years after the account is closed.
- Compare the customer's name against the government's list of known or suspected terrorists.
- Provide customers with adequate notice of the requirements for customer identification.

In 2016, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) issued a new rule[22] requiring all banks to collect the name, birth date, address, and Social Security number of individuals who own 25% or more of an equity interest in a legal entity.

[21] https://www.fdic.gov/regulations/laws/rules/1000-100.html

[22] https://www.avoka.com/blog/fincen-and-cdd-what-banks-need-to-know-about-the-new-rule/