Product Risk Advisory Position Paper

8-Digit BIN – PCI Security Requirements

Visa Public

Date:
November 12, 2021

Contact

Chackan Lai	Global Risk Advisory and Innovation	chlai@visa.com
Janet Cookson	Global Risk Advisory and Innovation	jcookson@visa.com

EXECUTIVE SUMMARY

Given the significant growth in payments, the industry recognized a need to increase the available pool of BIN values and adopted a process to increase the available supply. To that end, the payment industry has been working on the migration from a 6-digit BIN to 8-digit BIN since the International Organization for Standardization (ISO) published the updated standard ISO/IEC 7812-1: Identification Cards – Identification of issuers in January 2017. As the date for migration draws near, there is a concerted push by the industry to ensure all stakeholders can successfully cross the finish line.

This paper will focus on and provide a detailed summary of the PCI requirements and how they may, or may not, be impacted by this new industry standard. PCI requirements for securing the display, storage and processing of payment data do not change regardless of a 6-digit BIN or 8-digit BIN PAN.

However, confusion exists over what is allowed under PCI requirements for PAN Masking, PAN Truncation and PAN Encryption for PANs with a 6-digit or 8-digit BIN.

In view of the need for clarity in the payment industry between business needs and PCI requirements, this paper will address the various concerns, and specifically make the distinction between the following:

1) PCI DSS Security Requirements
2) PCI DSS Assessment Scoping
3) Business needs to obtain information from the BIN

Finally, the paper will provide Visa recommendations to ensure stakeholders are able to continue meeting PCI requirements, while at the same time meet their business needs. Additional clarification on the impacts to other business practices will be covered in a separate document.

PCI DSS Security Requirements

PCI DSS security requirements have driven innovative solutions over the years in balancing the need for payment ecosystem participants to maintain a strong security posture while at the same time enabling the participants to meet business goals and objectives.

Today, a common phrase in the payment industry, when talking about the security of the 16-digit PAN, is "First 6, last 4", meaning that only the first 6 digits and the last 4 digits of a PAN are displayed or stored to ensure the security of the PAN, while still enabling the business to meet its business process needs.

As the world transitions to an 8-digit BIN standard, please note that the new BINs could potentially impact certain business processes. To that end, this paper includes some guidance and recommendations to ensure the industry can continue to maintain high levels of PAN security, while meeting its business goals and objectives.

With that in mind, it is important to understand the core PCI DSS security requirements. Over the years, solutions developed to meet the requirements have resulted in assumptions and misunderstandings regarding these PCI requirements. Hence, making the distinction between PCI Security Requirements and solutions that have been developed to meet those requirements is very important.

The following are the key concepts referenced by the PCI DSS requirements:

	PCI DSS Requirement	Additional Notes
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.	**PAN Masking is a specific PCI Requirement**. It is a method of concealing a segment of PAN when displayed or printed (for example, on paper receipts, reports, or computer screens), to limit exposure of the full PAN. Display of the full PAN is permitted with legitimate business need.
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN). • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored). • • Strong cryptography with associated key-management.	**Neither PAN Truncation nor PAN Encryption have specific PCI requirements (compared to masking).** PAN Truncation and PAN Encryption are two of the four approaches that can be used to render PAN unreadable. **PAN Truncation** One of the allowable methods for rendering a full PAN unreadable by permanently removing a segment of PAN digits (see PCI FAQ 1091). It applies to PANs that are electronically stored (for example, in files, databases, etc.). **PAN Encryption** An allowable method that applies a reversible algorithm to render the PAN unreadable. **PCI requirements only require the use of strong cryptography. It does not mandate that encryption solutions only encrypt specific digits of the PAN. Solutions that encrypt specific digits within the PAN are design decisions of the solution vendor.**

Specifically, the concepts above would apply when PAN is displayed, stored, or transmitted. The applicability of PAN Masking, PAN Truncation and PAN Encryption as PAN is displayed, stored, and transmitted is captured in the table below:

	PAN Masking	PAN Truncation	PAN Encryption
Display of PAN	X		
Storage of PAN		X	X
Transmission of PAN			X

PCI DSS Assessment – Scoping

A closely related topic to PCI DSS Requirements is how the implementation of PAN Masking, PAN Truncation and PAN Encryption would be viewed by a PCI Qualified Security Assessors (QSA) as part of an organization's annual PCI assessment process. Specifically of interest is the ability for entities to "de-scope" certain system components from the PCI DSS scope if certain criteria are met.

PAN Masking

PAN Masking is a core PCI DSS requirement (3.3), and it has no relevance in the scoping exercise for an entity's annual PCI DSS assessment. All displays of PAN must be masked unless there is a business need for the display of the full PAN. The current PCI DSS requirements have provisions to allow any person with business needs to view the full PAN.

PAN Truncation

PAN Truncation is the simplest and most effective way most organizations use to limit the scope of their PCI DSS Assessment. PAN Truncation is an irreversible process and, when properly implemented, completely removes the middle digits of a PAN. It is both simple and effective since there are no means of reconstructing the deleted digits. Environments that only store PAN using approved truncation formats can typically be considered out of scope for the annual PCI DSS assessment process (See PCI FAQ 1117).

PAN Encryption

PAN Encryption is the process where the data is cryptographically secured. In contrast to PAN Truncation, encryption is a reversible process. Any entity with the cryptographic key is able to reverse the process and obtain the underlying clear text PAN. For environments that use full PAN Encryption using strong cryptography to secure their PAN data, the encrypted PAN is still subject to the annual PCI DSS assessment process (See PCI FAQ 1086).

PCI requirements for encryption do not define nor mandate the encryption of just the middle 6 digits of the PAN. Encryption solutions that only encrypt the middle digits of the PAN are created to meet business needs. (See PCI Requirement 3.4)

The table below summarizes the impact of PAN Truncation and PAN Encryption in the scoping exercise.

Display of PAN	Storage of PAN		PCI DSS Assessment
Masked / Unmasked	Cleartext	è	In Scope
Masked / Unmasked	Encrypted	è	In Scope
Masked / Unmasked	Truncated	è	Out of Scope[1]

[1] While truncation is a major requirement for an environment to be deemed out of scope for compliance audits, other associated criteria must also be met. Entities to consult with their QSA for scoping.

Visa Recommendations for 8 Digit BIN Migration

PAN Masking

PAN Masking requirements are applicable only for the display of the PAN. This requirement is captured in PCI DSS 3.3 (see Appendix for full requirement) and allows for the display of first 6 and last 4 digits of the PAN. At the same time, there are already provisions in the PCI DSS standards for the display of the full PAN to any persons with the business need for access. Therefore, there are no impacts due to 8-digit BIN migration.

Case Study

A customer service representative needs to verify a cardholder that called in with questions about the transaction.

The customer support system is not impacted by the 8-digit BIN migration because generally customer service representatives only ask for the last 4 digits of a cardholder's account number to verify the customer's identity. Should there be a need to display the full 16-digit PAN, PCI requirements already allow for this today (see PCI Requirement 3.3)

Visa's recommendation

Entities to continue their current PAN masking practices with the migration to 8-digit BIN.

PAN Truncation

PAN Truncation recommendations are the only updates made as a direct result of migrating to 8-digit BIN. These changes are covered by PCI FAQ 1091.

The reason for the update is because there may be business processes that rely on needing the 8-digit BIN of the PAN. Hence, there is a need to maintain visibility of the 8-digit BIN while the PAN is in storage within the payment environment. To satisfy the requirement for truncation, and thereby de-scope the environment from PCI validation assessments, at least 4 digits must be permanently removed from the PAN value for storage. Visa requirements are to remove 4 digits leaving the first 8 and any other 4 digits of the PAN value for storage in the database or in a file (see PCI FAQ 1091).

Case Study A

To de-scope the merchant store environment from PCI DSS validation assessments, the POS system only exposes the first 6 and last 4 digits to the payment application which stores the truncated PAN in the database. This database of truncated PANs is then used by store representatives to identify the cardholder in support of customer queries post transaction.

The store payment application database is not impacted by the 8-digit BIN migration because the use case does not use information from the 6-digit BIN. The merchant can continue supporting the business processes using just the first 6 and last 4 digits stored in the database.

Case Study B

To de-scope the merchant store environment from PCI DSS assessments, the fuel merchant's acquirer sends the merchant a transaction file with the PAN truncated leaving first 6 and last 4 digits in the clear and permanently removing the other digits per PCI truncation requirements. This file is then used by store

representatives to extract information from the truncated 6-digit BIN PAN to determine if the card used is a fleet card.

If the merchant received their file from a third party, the merchant should contact the third party for questions and/or verification of items. If the merchant receives the file directly from Visa, the acquirer has the option to update their system to send the merchant a truncated transaction file with the first 8 and last 4 digits in the clear to enable the fuel merchant to continue its existing process or develop alternative means of providing that product funding source information. (As mentioned, product information is NOT uniquely defined at the BIN level, it exists in the ARDEF tables and is based on 9 significant digits as well as in the transaction).

In addition, Visa transaction responses contain product information. In order to determine product information prior to a transaction the first 9 digits of the account must be available, else product information will be returned in the transaction response in a separate field.

Table	Data	Uses	Important Notes
Account Range Table (ARDEF) via Edit Package	Processing attributes such as funding source, type of product, geography, eligibility for cash back, etc.	Defines valid clearing account ranges and their attributes, including funding source.	Should not be used for routing. Does not contain issuing BIN.
Routing Tables	Batch files that are updated and distributed daily, weekly, etc., are based on subscription and contain account ranges (i.e., PAN prefixes) applicable to each program.	Used by Visa, PLUS and Interlink acquirers to make authorization routing decisions.	Multiple types of routing tables are defined for specific card programs (e.g., PLUS Routing File). Does not contain issuing BIN.
ACQ/ISS Identifier Table (Formerly known as BIN Validation Table - Renamed Effective July 2020)	Issuing and Acquiring Identifiers and associated attributes like country, region, type of identifier, eligibility for Visa Direct and various OCT attributes.	Used to identify the source and destination for Visa clearing transactions.	Does not contain funding source or product type. Does not contain issuing BIN.

Visa's recommendation

Truncation is not a PCI nor Visa requirement but one of four means to render cardholder data unreadable and hence allow entities to de-scope portions of their environment from their PCI DSS annual assessments.

Visa recommends removing at least 4 digits leaving the First 8 and any 4 digits in their PAN database and storage intact. (See PCI FAQ 1091). Any other combinations that truncate more than the allowable 4 digits, (e.g., Truncating the middle 6 and leaving the first 8 and last 2) are also compliant with PCI and Visa's security requirements.

Specifically, if you do not need to obtain information from the BIN to support your business processes, you can continue your current truncation process of leaving the first 6 and last 4 digits in the clear for both 6-digit and 8-digit BINs.

PAN Encryption

Many entities today deploy encryption solutions to secure PAN in storage. Given the PCI Security requirement to secure card data both in transit as well as in storage, most of such PAN encryption solutions, including Point to Point Encryption (P2PE), encrypt the PAN data immediately after the PAN is read/entered into the environment (aka at the POS terminal).

While not an explicit PCI DSS requirement, many such encryption solutions at the POS terminal leave the first 6 and last 4 digits alone while encrypting only the middle 6 digits. Hence, migrating to 8-digit BIN while maintaining the business need to obtain information from the BIN would require that such solutions be updated to support encryption of only the middle 4 digits instead.

Case Study C

To de-scope the merchant store environment from PCI DSS annual assessments, the POS system encrypts the middle 6 leaving the first 6 and last 4 digits in the clear before storing it in the store database.

In situations where the merchant extracts information from the BIN to make business decisions, they will have to either obtain the information via other means or update the POS system to leave the 8 –digit BIN in the clear.

Visa's recommendation

Entities should engage with their POS encryption solution provider to discuss updating the solution to support leaving the 8-digit BIN in the clear. If there are any challenges when it comes to ensuring PCI DSS compliance (e.g. by updating the POS encryption software, the solution falling out of compliance with P2PE requirements), please reach out to cisp@visa.com and Visa staff will work collaboratively to resolve the challenge and ensure that they are able to continue meeting all Visa requirements.

CONCLUSION

The migration from a 6- to 8-digit BIN has been an ongoing initiative since January 2017. The payment industry has gone through many changes over this period and has introduced new secure technology like EMV chip and tokens. As a result, the need for securing PAN data, especially PAN by itself without other authentication data like expiration date, CVV etc. has been greatly reduced over the years.

To continue to adhere to the PCI DSS requirements with the migration to 8-digit BIN, the majority of businesses today do not require any changes. These businesses can continue to keep the first 6 and last 4 even after the migration to 8-digit BIN.

Only businesses that tie their internal processes to the information that may be obtained from the BIN may require a change. Hence, the first step is to conduct an assessment and determine where the BIN is used in their internal processes, downstream systems and with their partners.

Visa will continue to update key stakeholders impacted by this industry change. To learn more about the 8-digit BIN industry change, please reach out to your Acquirer, Processor or Visa representative. Or visit www.visa.com/8digitBIN.

Any client or partner acting on the recommendations herein should continue to consult a qualified security accessor on how any changes to PCI compliance standards apply to a specific organization.

APPENDIX – PCI REQUIREMENTS and FAQs

The following information reflects published information on the PCI SSC website at the time of this document publication. As a best practice always reference the PCI website for the most current versions.

REQUIREMENTS

- PCI DSS can be accessed from the PCI SSC Document Library at PCI DSS - Requirements and Security Assessment Procedures .
- PCI FAQs can be accessed from the PCI SSC website at www.pcisecuritystandards.org/faqs (entering a keyword, ex. FAQ number, in the search box and clicking on the submit button recommended).

PCI DSS Standard Requirement 3.3

PCI DSS Requirements	Testing Procedures	Guidance
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. *Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point of sale (POS) receipts.*	3.3.a Examine written policies and procedures for masking the display of PANs to verify: • A list of roles that need access to displays of more than the first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to have such access. • PAN must be masked when displayed such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. • All roles not specifically authorized to see the full PAN must only see masked PANs. 3.3.b Examine system configurations to verify that full PAN is only displayed for users/roles with a documented business need, and that PAN is masked for all other requests. 3.3.c Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displaying cardholder data, and that only those with a legitimate business need are able to see more than the first six/last four digits of the PAN	The display of full PAN on items such as computer screens, payment card receipts, faxes, or paper reports can result in this data being obtained by unauthorized individuals and used fraudulently. Ensuring that full PAN is only displayed for those with a legitimate business need to see the full PAN minimizes the risk of unauthorized persons gaining access to PAN data. The masking approach should always ensure that only the minimum number of digits is displayed as necessary to perform a specific business function. For example, if only the last four digits are needed to perform a business function, mask the PAN so that individuals performing that function can view only the last four digits. As another example, if a function needs access to the bank identification number (BIN) for routing purposes, unmask only the BIN digits (traditionally the first six digits) during that function. This requirement relates to protection of PAN displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.4 for protection of PAN when stored in files, databases, etc.

PCI DSS Standard Requirement 3.4

PCI DSS Requirements	Testing Procedures	Guidance
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. *Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*	3.4.a Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods: • One-way hashes based on strong cryptography, • Truncation • Index tokens and pads, with the pads being securely stored • Strong cryptography, with associated key-management processes and procedures. 3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text). 3.4.c Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable. 3.4.d Examine a sample of audit logs, including payment application logs, to confirm that PAN is rendered unreadable or is not present in the logs. 3.4.e If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception or troubleshooting logs) must all be protected. One-way hash functions based on strong cryptography can be used to render cardholder data unreadable. Hash functions are appropriate when there is no need to retrieve the original number (one-way hashes are irreversible). It is recommended, but not currently a requirement, that an additional, random input value be added to the cardholder data prior to hashing to reduce the feasibility of an attacker comparing the data against (and deriving the PAN from) tables of precomputed hash values. The intent of truncation is to permanently remove a segment of PAN data so that only a portion (generally not to exceed the first six and last four digits) of the PAN is stored. An index token is a cryptographic token that replaces the PAN based on a given index for an unpredictable value. A one-time pad is a system in which a randomly generated private key is used only once to encrypt a message that is then decrypted using a matching one-time pad and key. The intent of strong cryptography (as defined in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms) is that the encryption be based on an industry-tested and accepted algorithm (not a proprietary or "homegrown" algorithm) with strong cryptographic keys. By correlating hashed and truncated versions of a given PAN, a malicious individual may easily derive the original PAN value. Controls that prevent the correlation of this data will help ensure that the original PAN remains unreadable.

Frequently Asked Questions

FAQ-1146 - What is the difference between masking and truncation?

FAQ Response:
Masking is addressed in PCI DSS Requirement 3.3, whereas truncation is one of several options specified to meet PCI DSS Requirement 3.4.

Requirement 3.3 relates to protection of PAN where it is displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.4 for protection of PAN when stored, processed, or transmitted in files, databases, etc.

Masking is a method of concealing a segment of a primary account number (PAN) when displayed or printed (for example, on paper receipts, reports, or computer screens), and is used when there is no business need to view the entire PAN.

Truncation is a method of rendering a full PAN unreadable by removing a segment of PAN data and applies to PANs that are electronically stored (for example, in files, databases, etc.).

Masking is not synonymous with truncation and these terms cannot be used interchangeably. Masking refers to the concealment of certain digits during display or printing, even when the entire PAN is stored on a system. This is different from truncation, in which the truncated digits are removed and cannot be retrieved within the system. Masked PAN could be “unmasked”, but there is no "un-truncation" without recreating the PAN from another source.

Note that even if a PAN is masked when displayed, the full PAN might still be electronically stored and would need to be protected in accordance with PCI DSS Requirement 3.4.

Entities should also be aware of any stricter requirements that may apply to displays of cardholder data, such as specific Payment Brand regulations and regulatory or legislative requirements —for example, restrictions for data displayed on point-of-sale (POS) receipts. PCI DSS does not supersede local or regional laws or other legislative requirements.

See also the following FAQs:
FAQ 1117: Are truncated Primary Account Numbers (PAN) required to be protected in accordance with PCI DSS?
September 2021
Article Number 1146

FAQ-1117 - Are truncated Primary Account Numbers (PAN) required to be protected in accordance with PCI DSS?

FAQ Response:
Systems that store, process, or transmit only truncated PANs (where a segment of PAN data has been permanently removed) may be considered out of scope for PCI DSS if those systems are adequately segmented from the cardholder data environment, and do not otherwise store, process, or transmit

cardholder data or sensitive authentication data. This applies to any truncation that meets the acceptable PAN truncation formats specified in FAQ 1091.

However, the system performing the truncation of the PANs, as well as any connected systems and networks, would be in scope for PCI DSS.

Some entities use solutions that combine truncation with tokenization or encryption to create format-preserving values that can be passed through legacy payment systems. For example, the BIN and the last four digits of the PAN are retained in accordance with FAQ 1091 while the remaining digits are replaced with values generated via a tokenization or encryption operation. Whether such format-preserving values may be considered out of scope for PCI DSS is dependent on a variety of factors and can only be determined in respect of an entity's specific implementation by an Assessor. However, the systems performing encryption or tokenization of the PAN segment and those performing key management for the encrypted or tokenized PANs would be in scope for PCI DSS.
For solutions that combine truncation with tokenization or encryption, factors that indicate the resulting truncation result would be in scope for PCI DSS, include, but are not limited to the following:

- The tokenization or encryption of the PAN segment can be reversed in the environment in which the segment resides.
- The encrypted or tokenized PAN segment is not isolated from related key management processes.
- The encrypted or tokenized PAN segment is present on a system or media that also contains the decryption key.
- The encrypted or tokenized PAN segment is present in the same environment as the decryption key.
- The encrypted or tokenized PAN segment is accessible to an entity that also has access to the decryption key.

Note that access to different truncation formats of the same PAN greatly increases the ability to reconstruct full PAN, and the security value provided by an individual truncated PAN is significantly reduced. If the same PAN is truncated using more than one truncation format (for example, different truncation formats are used on different systems), additional controls should be in place to ensure that the truncated versions cannot be correlated to reconstruct additional digits of the original PAN. To consider the truncated PAN out of scope, the additional controls must be verified to confirm that correlation is not possible, and that the different truncation formats do not result in more than the maximum allowable digits being present in the environment. If a PAN is truncated using different truncation formats, and this results in more than the allowable number of PAN digits being present in an environment, then that environment would be in scope for PCI DSS.

See also the following FAQs:
FAQ 1091: What are acceptable formats for truncation of primary account numbers?
FAQ 1146: What is the difference between masking and truncation?
September 2021
Article Number 1117

FAQ 1086 - How does encrypted cardholder data impact PCI DSS scope?

FAQ Response:

This FAQ has been updated in consideration of changes to payment environments and standards, including the PCI P2PE Standard.

Use of encryption in a merchant environment does not remove the need for PCI DSS in that environment. The merchant environment is still in scope for PCI DSS due to the presence of cardholder data. For example, in a card-present environment, merchants have physical access to the payment cards to complete a transaction and may also have paper reports or receipts with cardholder data. Similarly, in card-not-present environments, such as mail-order or telephone-order, payment card details are provided via channels that need to be evaluated and protected according to PCI DSS.

Encryption of cardholder data with strong cryptography is an acceptable method of rendering the data unreadable in order to meet PCI DSS Requirement 3.4. However, encryption alone may not be sufficient to render the cardholder data out of scope for PCI DSS.

The following are each in scope for PCI DSS:

- Systems performing encryption and/or decryption of cardholder data, and systems performing key management functions
- Encrypted cardholder data that is not isolated from the encryption and decryption and key management processes
- Encrypted cardholder data that is present on a system or media that also contains the decryption key
- Encrypted cardholder data that is present in the same environment as the decryption key
- Encrypted cardholder data that is accessible to an entity that also has access to the decryption key

Where a third party receives and/or stores only data encrypted by another entity, and where they do not have the ability to decrypt the data, the third party may be able to consider the encrypted data out of scope if certain conditions are met. For further guidance, refer to FAQ 1233: How does encrypted cardholder data impact PCI DSS scope for third-party service providers?

Additionally, for information about how a merchant may receive scope reduction through use of a validated P2PE solution, please see the FAQ 1158: What effect does the use of a PCI-listed P2PE solution have on a merchant's PCI DSS validation?

August 2016
Article Number 1086

FAQ 1091 - What are acceptable formats for truncation of primary account numbers?

FAQ Response:
This FAQ reflects updates as of November 2021 for acceptable truncation formats for different PAN / BIN lengths.

Acceptable truncation formats vary according to PAN length and Participating Payment Brand requirements.

- A maximum of the first 6 and last 4 digits of the PAN is the starting baseline for entities to retain after truncation, considering the business needs and purposes for which the PAN is used.
- When more digits of the PAN are necessary for business functions, entities should consult the table below for the acceptable formats for each Participating Payment Brand.

PAN / BIN Length	Payment Brand	Acceptable PAN Truncation Formats
>16-digit PAN (with either 6- or 8-digit BIN)	UnionPay	At least 6 digits removed. Maximum digits which may be retained: 17-digit PAN: "First 6, any other 5" 18-digit PAN: "First 6, any other 6" 19-digit PAN: "First 6, any other 7"
16-digit PAN with 8-digit BIN	UnionPay	At least 6 digits removed. Maximum digits which may be retained: "First 6, any other 4"
16-digit PAN with 6-digit BIN	JCB UnionPay	At least 6 digits removed. Maximum digits which may be retained: "First 6, any other 4"
16-digit PAN (with either 6- or 8-digit BIN)	Discover Mastercard Visa	At least 4 digits removed. Maximum digits which may be retained: "First 8, any other 4"
15-digit PAN	American Express	At least 5 digits removed. Maximum digits which may be retained: "First 6, last 4"
<15-digit PAN	Discover	Maximum digits which may be retained: "First 6, any other 4"

When using truncation formats for purposes other than storage, or for PAN lengths not covered within this FAQ, entities should confirm that their format is compatible with each of the applicable Participating Payment Brands. Contact information for the Participating Payment Brands can be found in FAQ 1142 How do I contact the payment card brands?

Note: *Access to different truncation formats of the same PAN greatly increases the ability to reconstruct full PAN, and the security value provided by an individual truncated PAN is significantly reduced. If the same PAN is truncated using more than one truncation format (for example, different truncation formats are used on different systems), additional controls should be in place to ensure that the truncated versions cannot be correlated to reconstruct additional digits of the original PAN.*
November 2021
Article Number 1091

FAQ 1492 - How can an entity meet PCI DSS requirements for PAN masking and truncation if it has migrated to 8-digit BINs?

FAQ Response:

There are two PCI DSS requirements that may be affected when considering 8-digit BINs. Requirement 3.3 pertains to masking (concealing) digits of the PAN so that the full PAN is not displayed, and Requirement 3.4 is for rendering PAN unreadable when stored. These requirements are different and distinct and therefore it is important to understand each requirement and how it pertains to the entity's implementation.

PCI DSS Requirement 3.3 requires that no more than the first six and/or last four digits of the PAN are displayed on computer screens, reports, etc. unless there is a documented business justification for seeing more digits. The documented business justification should explain why that person (or role) needs to see more digits of PAN, be approved by management, and available for an assessor to review as part of the PCI DSS assessment.

PCI DSS Requirement 3.4 applies when PAN is stored (i.e., data at rest). This requirement specifies four acceptable methods for rendering PAN unreadable when stored. One of the techniques is truncation, which permanently removes the middle digits of the PAN, leaving the rest of the PAN to be stored in the clear. FAQ #1091 *What are acceptable formats for truncation of primary account numbers?* provides information about acceptable truncation formats for each payment brand based on the length of PAN/BIN. Because each payment brand has different PAN/BIN lengths and different requirements, questions on payment brand truncation requirements should be directed to the applicable payment brands. Contact details for the payment brands are provided in FAQ #1142 *How do I contact the payment card brands?*

Please note that truncation is only one acceptable method for rendering PAN unreadable during storage; other options include encrypting the entire PAN, using index tokens, or using one-way hashes.

February 2021
Article Number 1492