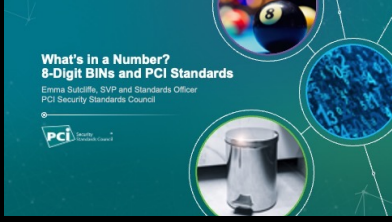
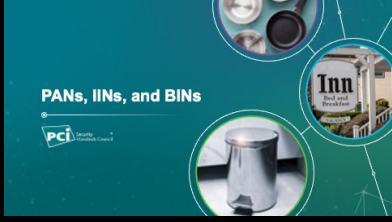
Welcome



- Hallo
- You may be wondering
- What does the number 8 Have to do with a BIN ?
- And why do we care?
- Well let’s find out…

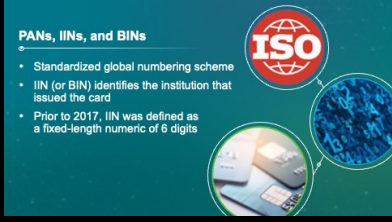
Next Slide: PANs, IINs, and BINs

PANs, IINs, and BINs



- When we talk about PAN and BIN and INN, what do we mean?

PANs, IINs, and BINs



- Hopefully you all know what a PAN is
  - Primary Ac Number - a number which is used to identify an individual account holder.
  - The PAN is of variable length, ranging from 8 to 19 digits.
- IIN- issuer identification number - is also part of a Standardized global numbering scheme - to identify the institution that issued the card
- IIN and PAN formats are defined within ISO/IEC 7812-1
  - International Organization for Standardization
  - Not PCI SSC
- BIN - "bank identification number" - is another term used for IIN
  - IINs have much broader usage than only banks – other types of companies also issue cards that follow this ISO standard format
  - We'll use the term (BIN) as that is the familiar term for the payments industry
- Prior to 2017, the IIN/BIN was defined as a fixed-length numeric of six digits.
- Why did this change?

CLICK CLICK

Why Now?

- The payments business continues to growing at a rapid pace,
- Increasing number of card issuers - putting pressure on the industry to ensure availability of new BINs
- To determine the best path forward, ISO convened payment industry stakeholders from around the world.
- After much discussion, they agreed to expand the length of the issuing BIN from 6 to 8 digits.
  - Increase was published in the 2017 revision of the ISO standard.
- The PAN will continue to remain a variable length, ranging from 10 to 19 digits
- Well that's interesting and all, but if you're wondering …

CLICK CLICK

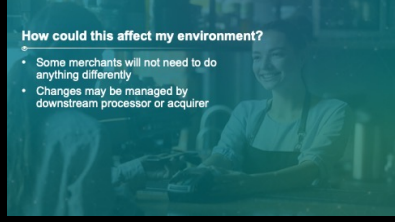
Notes Page: 4 of 23

Next Slide: What does this have to do with me?

What does this have to do with me?

- What do we need to know this …?
- Some payment brands have already started using the first eight digits as the BIN instead of the first six

Next Slide: How could this affect my environment?

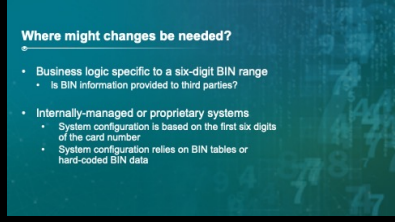


How could this affect my environment?

- This may or may not have a direct impact..
- Some merchants will not need to do anything differently
- Changes may be managed by downstream processor or acquirer
- For example, the introduction of 8-digit BIN is unlikely to affect those systems which have traditionally displayed only the last four digits.
- In that use case, no changes would be necessary when migrating to the use of 8-digit BINs.

Next Slide: Where might changes be needed?

Where might changes be needed?



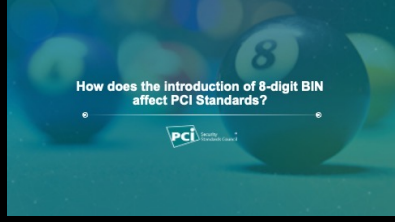
- However, some merchants may find that they do need to make changes
  - Any business logic specific to a six-digit BIN range may need to be changed
  - Is BIN information provided to third parties?
- Merchants with their own internal or proprietary systems, could need to examine how the BIN expansion will impact their back-end systems.
  - System configuration is based on the first six digits of the card number
  - Proprietary or third-party provided BIN tables are used
  - Hard-coded BIN data is used
- Examples of activities to be included in review :
  - Fraud and/or chargeback analytics
  - Issuer identification
  - Routing
  - Identification of participants for loyalty and proprietary benefits programs
- Identify any downstream and processing systems that may also be updating their business logic for 8 digit BINs.
- Coordinate and collaborate with your business partners. .

CLICK

Notes Page: 7 of 23

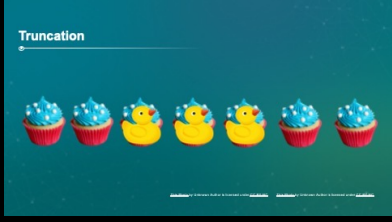
Next Slide: How does the introduction of 8-digit BIN …

How does the introduction of 8-digit BIN



- All our standards support use of 8-digit BINs
- Many PCI standards have requirements for cardholder data to be protected through truncation and masking. - e.g.,
  - PCI DSS
  - PTS POI
- Masking and truncation are not the same - each of these methods has different applications, and may be subject to different rules and requirements.
- Both truncation and masking, in the context of the PCI standards, apply specifically to the PAN but with different effects.

Truncation



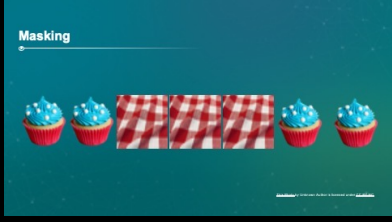
- truncation is a method of rendering a full PAN unreadable by removing a segment of PAN data,
- A truncation system may replace the removed digits with other, unrelated digits

[CLICK]

- such as ‘0000’ for example), letters (‘XXXX’), or reduce the stored PAN to only the remaining digits without any replacement.
- Truncation applies to PANs that are electronically stored (for example, in files, databases, etc.).
- Truncation may be used when the business only needs a subset of the PAN digits, say for routing or tracing purposes, and so the digits which are not required are stripped from the PAN prior to storage.
- The process of truncation is not reversible; once the PAN digits are removed,
- they cannot be retrieved without recreating the PAN from another source.
- So use truncation when the full PAN is not needed

CLICK CLICK

Masking



- The process of masking is used to ‘hide’ digits of the PAN,

CLICK

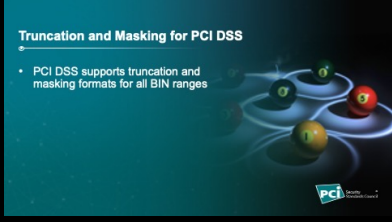
- so that only a subset can be seen by a particular person, program, or system.
- Masking is a method of concealing a segment of a PAN Where it is displayed or printed (for example, on paper receipts, reports, or computer screens), and is used when there is no business need to view the entire PAN.
- In this way, masking is a temporary process that is used to limit the exposure of the full PAN to only those people and systems where it is required.
- The full PAN still exists somewhere - masking is applied to a specific display instance and often systems may allow for an escalation process

CLICK

- to display the full PAN upon a suitable business need.
- So use masking to limit how much PAN can be seen by different people/roles/systems, filtering how much of the full PAN – which is securely stored somewhere - can be seen
- We have a number of FAQs on truncation and masking – go to our FAQ page search for key words

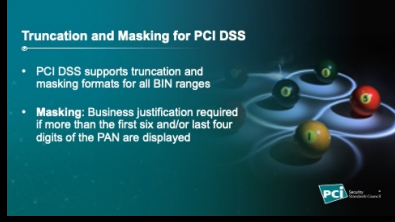
CLICK CLICK

Truncation and Masking for PCI DSS



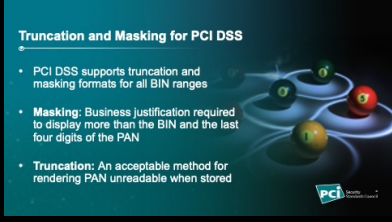
No Notes

Truncation and Masking for PCI DSS



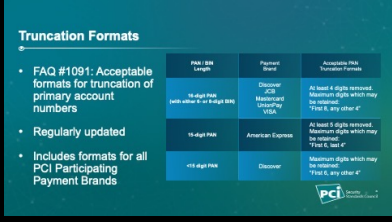
- PCI DSS masking Requirement
- V3.2.1 –
  - If more than the first six and/or last four digits of the PAN are displayed on computer screens, reports, etc., there is a documented business justification for seeing more digits.
  - This should explain why that person (or role) needs to see more digits of PAN, be approved by management, and available for an assessor to review as part of the PCI DSS assessment.
- V4.0 –
  - The BIN and last four digits are the maximum number of digits to be displayed, and only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.
- The masking approach should always display only the number of digits needed to perform a specific business function. For example, if only the last four digits are needed to perform a business function, PAN should be masked to only show the last four digits. As another example, if a function needs to view to the bank identification number (BIN) for routing purposes, unmask only the BIN digits for that function.

Truncation and Masking for PCI DSS



- Relevant requirement for truncation is - PAN is rendered unreadable anywhere it is stored
- The removal of cleartext stored PAN is designed to prevent an unauthorized individual gaining access to stored data, even if they have gained access to the system through exploitation of a vulnerability or a misconfiguration in the entity's primary access controls.
- Because truncation removes part of the PAN – it is no longer present on the entity's systems – the attacker will not be able to recover the full PAN
- Truncation formats are defined for different payment brands
    - Because they may evolve, the standard doesn't prescribe what format is – we have a FAQ to provide this information

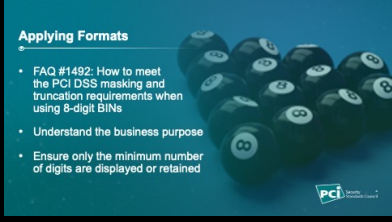
Truncation Formats



- FAQ #1091
- identifies the acceptable truncation formats as defined by each payment brand.
- Formats for 8-digit BINs were initially added to this FAQ in 2017
- The FAQ has been regularly updated since then to reflect recent payment brand changes to their truncation formats.
- It is important to remember that the formats in FAQ #1091 are the maximum permissible values and are intended for use only when needed to support a legitimate business need.
- Having PAN with larger ranges of digits available could expose more PAN data to attacks, allowing attackers to more easily deduce the full PAN

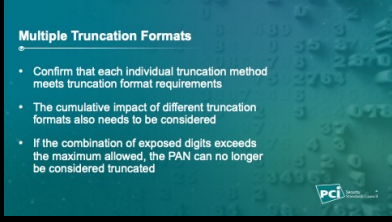
CLICK CLICK

Applying Formats



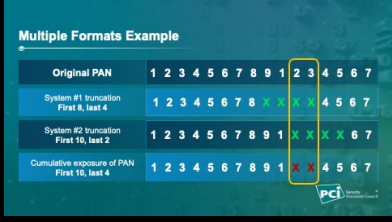
- FAQ #1492 explains how to meet the PCI DSS masking and truncation requirements when using 8-digit BINs.
- Important to understand the business purpose for displaying or retaining PAN.
- The truncation and masking formats used should always ensure that only the minimum number of digits are displayed or retained as necessary for the specific business need.

Multiple Truncation Formats



- When reviewing PAN truncation formats, as well as confirming that each individual truncation method meets truncation requirements, the cumulative impact of different truncation formats within the same environment also needs to be considered.
- If more than one truncation format is applied to the same PAN—for example, different truncation formats are used on different systems—and the combination of exposed digits exceeds the maximum allowable digits, then the PAN can no longer be considered truncated.

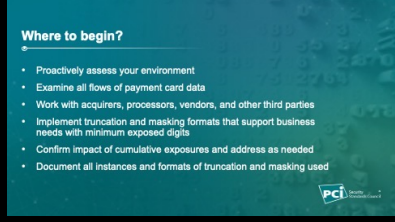
Multiple Formats Example



- When reviewing PAN truncation formats, as well as confirming that each individual truncation method meets truncation requirements, the cumulative impact of different truncation formats within the same environment also needs to be considered.
- If more than one truncation format is applied to the same PAN—for example, different truncation formats are used on different systems—and the combination of exposed digits exceeds the maximum allowable digits, then the PAN can no longer be considered truncated.
- 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

CLICK CLICK CLICK

Where to begin?



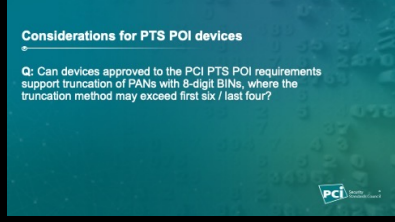
- Don’t wait
- List out what specific instances of truncation/masking are used, where and why they are implemented.
- The first step in knowing how 8-digit BINs may affect you is in understanding exactly how you use the PAN right now.
  - Examine all flows of payment card data to determine how many digits of the PAN are required throughout the data flow
  - Work with acquirers, processors, vendors, and other third parties involved in transaction processing, routing, or other downstream activities
- Routing and authorization processes, Fraud monitoring, Transaction analytics, Support for unique BIN ranges, POS reporting
- Implement truncation and masking formats that support business needs with minimum exposed digits
- Confirm impact of cumulative exposures and address as needed
- Document all instances and formats of truncation and masking used
- Consider cumulative exposure A vital point to remember is that just because 8-digit BINs allow for an increased number of digits to be available after truncation/masking, it does not mean that you should automatically start using these formats.
- Displaying anything beyond the first six and last four digits requires a business need-to-know. Remember the most important rule – don’t keep it if you don’t need it!

CLICK CLICK CLICK CLICK CLICK

Notes Page: 18 of 23

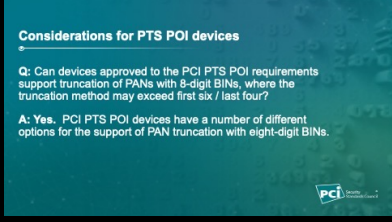
Next Slide: Considerations for PTS POI devices

Considerations for PTS POI devices



- PTS POI devices which are being assessed against the SRED requirements must meet the “Output of Clear-text Account Data” requirements.
- The answer is…

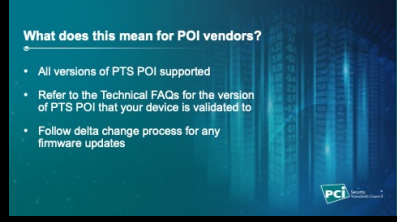
Considerations for PTS POI devices



- This requirement was updated in version 6.1 of the PCI PTS POI standard to allow for support of eight-digit BINs, per brand-defined truncation limits as defined in FAQs such as FAQ 1091 a
- POI device validated to previous versions of PCI PTS POI - v3, v4, and v5 - may follow the testing requirements of the most current version of the POI standard with regards to acceptable truncation.
- Specifically, truncation formats compliant to current brand requirements, as defined in FAQs such as FAQ 1091, may be included in firmware updates for PCI PTS POI devices approved to any PCI PTS POI version.

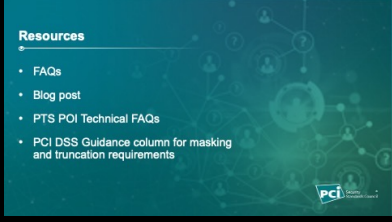
Next Slide: What does this mean for POI vendors?

What does this mean for POI vendors?



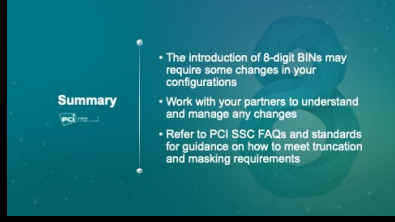
No Notes

Resources



No Notes

Summary



- A vital point to remember is that just because 8-digit BINs allow for an increased number of digits to be available after truncation/masking, it does not mean that you should automatically start using these formats.
- Understand the business purpose for all displays and retention (storage) of PAN
- Ensure that only the minimum number of digits are displayed or retained as necessary for the specific business need.
- Displaying anything beyond the first six and last four digits requires a business need-to-know. Remember the most important rule – don't keep it if you don't need it!

LAST SLIDE