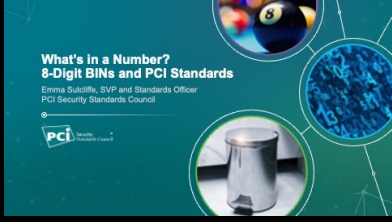
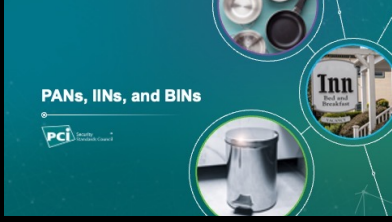
Welcome



- 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…

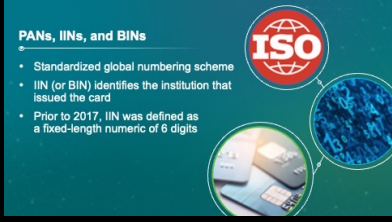
Next Slide: PANs, IINs, and BINs

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
  - Assigned to individual a/c holder - variable length 8 - 19 digits.
- IIN- issuer identification number - identify the institution that issued the card
- Both are part of a Standardized global numbering scheme – formats defined within ISO/IEC 7812-1
  - International Organization for Standardization / International Electrotechnical Commission
  - Not PCI SSC
- BIN - "bank identification number" – often used interchangeably with IIN
  - While IINs have much broader usage than BIN – companies other than banks also issue cards that follow the ISO 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?

Why Now?

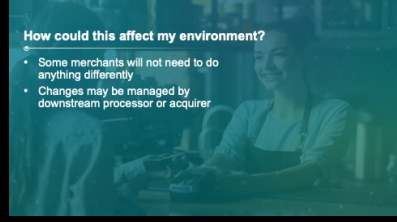
- The payments business has been growing at a rapid pace,
- Increasing number of card issuers & putting pressure on the industry to ensure availability of new BINs
- To address the impending shortage of available BINs, ISO convened payment industry stakeholders from around the world to determine the best path forward
- After much discussion,
- it was agreed to increase the length of the issuing BIN from 6 to 8 digits.
  - Published in the 2017 revision of the ISO standard.
  - PAN continues to be variable length, from 10 - 19 digits
- Well that's interesting and all, but if you're wondering …

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 …?
- While 6-digit BIN may be still be the most commonly-seen format,
- 8-digit BINs are already in use, and will become more prevalent as we go forward
- And depending on how you manage your payment card data, the changing BIN range might have an affect on how your systems are configured

Next Slide: How could this affect my environment?

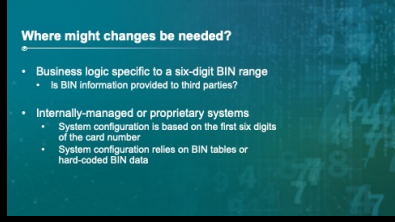


How could this affect my environment?

- This may or may not have a direct impact..
- Some merchants will not need to do anything differently
- As changes to accommodate 8-BIN may be managed by the downstream processor or acquirer
  - E.g., if merchant payment systems send all transaction data to the same processor,
  - Or the processor manages all the system configurations
- Another Eg – if merchant only needs to see the last four digits of a PAN, the changing BIN ranges is unlikely to make a difference to this bus need

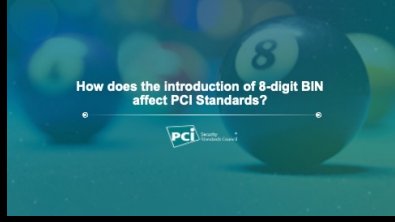
Next Slide: Where might changes be needed?

Where might changes be needed?



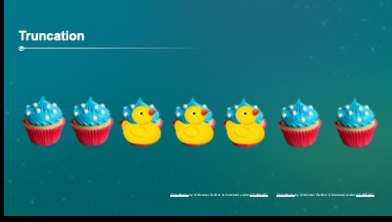
- However, some merchants may find that they do need to make changes
- Any business logic specific to the BIN range may need to be changed
  - E.g., Is BIN information provided to third parties or used to determine routing?
- Merchants with their own internal or proprietary systems, may need to look at how their systems use, or don't use, BIN info for their configs
  - E.g., System configurations that rely on proprietary or third-party provided BIN tables
  - Or BIN data is hard-coded into configs
  - Will need to determine config changes for new BIN ranges
- May also need to coordinate and collaborate with your business partners
- Identify any downstream systems that may be updating their business logic for 8 digit BINs.

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 has different applications, may be subject to different requirements
- Both truncation and masking, in the context of the PCI standards, apply specifically to the PAN but with different effects

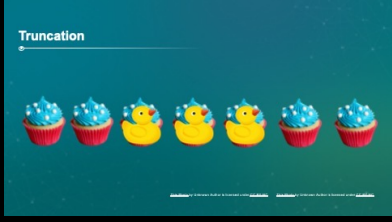
Truncation



- Method of rendering a full PAN unreadable
- By removing a segment of PAN data

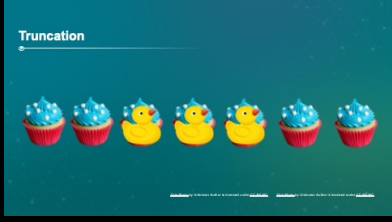
Next Slide: Truncation

Truncation



- A truncation system will often replace the removed digits with other, unrelated digits
- or characters (‘XXXX’)
- Truncation applies to PANs that are electronically stored (for example, in files, databases, etc.).
- 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…

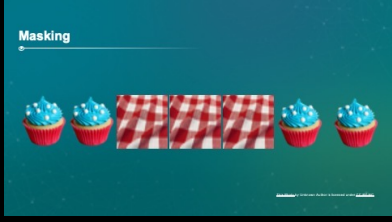
Truncation



- 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

Next Slide: Masking

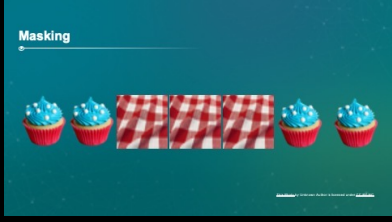
Masking



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

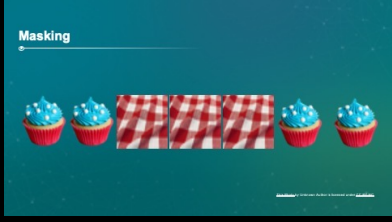
Next Slide: Masking

Masking



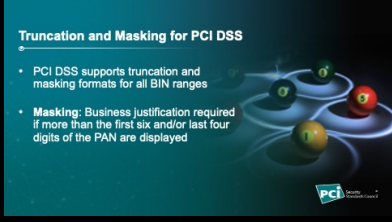
- So that only a subset can be seen by a particular person, program, or system.
- Used to conceal a segment of a PAN where displayed or printed (paper receipts, reports, or computer screens), where there is no business need to view the entire PAN.
- Masking is a temporary process –
- The full PAN still exists somewhere – Masking is applied to a specific display instance

Masking



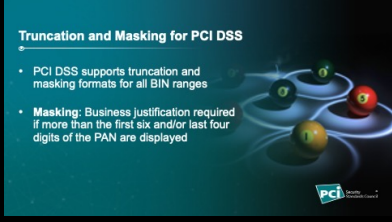
- Often systems may allow for alternative configurations
- That allow display of the full PAN when needed
- So use masking to limit how much PAN – which is securely stored somewhere - can be seen can be seen by different people/roles/systems

Truncation and Masking for PCI DSS



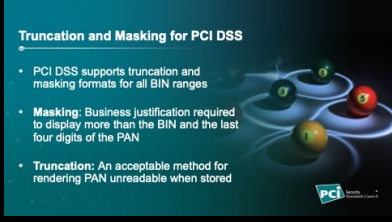
- Let’s look at PCI DSS
- Supports truncation and masking formats for all BIN ranges

Truncation and Masking for PCI DSS



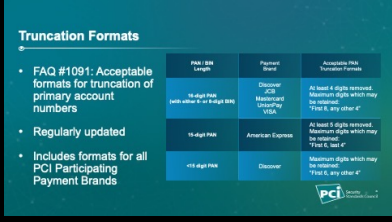
- PCI DSS masking Requirement
  - v3.2.1 – Baseline format – display up to first 6 / last 4
  - v4.0 – Baseline format – display up to the BIN and last four digits
- Both versions support use of masking formats that display more of the PAN
  - If a documented business need to explain why a person/role needs to see more digits of PAN
- The masking approach should always display only the number of digits needed to perform a specific business function.
  - If only the last 4 digits are needed to perform a business function, only show the last 4 digits.
  - 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



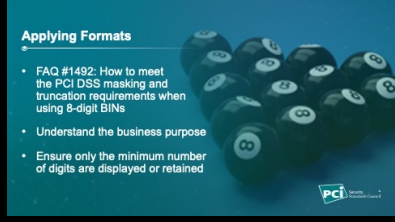
- For truncation – relevant DSS req relates to rendering PAN unreadable when stored
- Designed to prevent unauthorized individual gaining access to stored PAN, even if they have gained access to the system
  - Via exploitation of a vulnerability or a misconfiguration in the system access controls.
  - Because truncation removes part of the PAN – 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 based on brand requirements, the standard doesn't prescribe what the formats are – we have a FAQ to provide this information

Truncation Formats



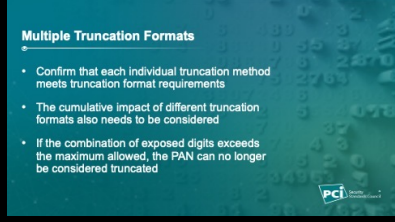
- FAQ #1091 - identifies the acceptable truncation formats as defined by each payment brand.
- Formats for 8-digit BINs were initially added to this FAQ in 2017
- Has been regularly updated since then to reflect recent payment brand changes to their truncation formats.
- Important Note – the formats in FAQ are the maximum permissible values that are to be retained
  - These formats are intended for use only when needed to support a legitimate business need
  - If no business need to retain this number of digits, then remove more digits so fewer retained
  - Retaining larger ranges of digits could expose more PAN data to attacks, allowing attackers to more easily deduce the full PAN

Applying Formats



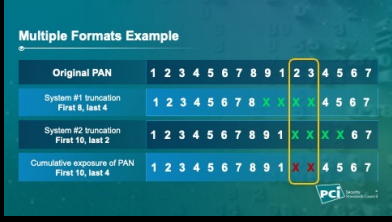
- FAQ #1492 – guidance on how to meet the PCI DSS masking and truncation requirements when using 8-digit BINs.
- Key point – Important to understand the business purpose for displaying or retaining PAN.
- The truncation and masking formats used should always ensure that
- Only the minimum number of digits are displayed or retained as necessary for the specific business need.
- Just because increased truncation/masking formats are permitted to support 8-digit BINs, it does not mean that you should automatically start using these formats.
- Remember the most important rule – don’t keep it if you don’t need it!

Multiple Truncation Formats



- When reviewing PAN truncation formats – as well as confirming that each individual trunc method meets trunc requirements,
  - The cumulative impact of different trunc formats within the same environment also needs to be considered.
- If more than one trunc format is applied to the same PAN – e.g. different formats are used on different systems –
  - And the combination of exposed digits exceeds the max. allowable digits,
  - Then the PAN can no longer be considered truncated.
- Let's look at an example of this cumulative impact

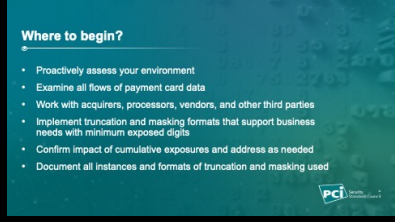
Multiple Formats Example



- After example - You can see from this example how:
  - Using different trunc formats for same PAN can increase the ability to reconstruct full PAN
  - Significantly reducing the security value of the truncation
- Scenarios like this – where a PAN is truncated using more than one format:
  - Additional controls should be in place to ensure that the trunc versions cannot be correlated to reconstruct additional digits of the original PAN.
- From scoping perspective – in order to consider the truncated PAN out of scope, the additional controls must be verified to confirm that
  - correlation is not possible, and
  - The different trunc formats do not result in more than the max. allowable # of digits being in the environment.

CLICK CLICK CLICK

Where to begin?



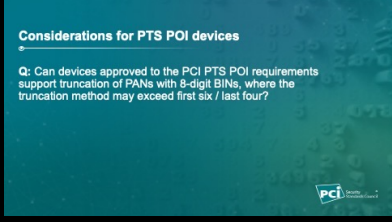
- Don’t wait – be proactive
- First step in knowing how 8-digit BINs may affect you is understanding exactly how you use PAN right now. <click>
- Examine all flows of payment card data – determine how many digits of the PAN are required throughout the data flow. This includes… <click>
- Working with business partners - acquirers, processors, vendors, other third parties – involved in transaction processing, routing, or other downstream activities. Once you know what you have… <click>
- Identify and implement truncation and masking formats that support business needs with minimum exposed digits. And don’t forget to… <click>
- Confirm the impact of any cumulative exposures – and address identified issues to avoid reduced security and incorrect scoping decisions. Finally…<click>
- Document all specific instances of truncation/masking used, and where, and why they are implemented.

CLICK CLICK CLICK CLICK CLICK

Notes Page: 22 of 27

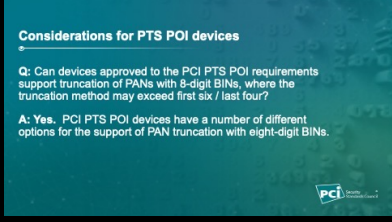
Next Slide: Considerations for PTS POI devices

Considerations for PTS POI devices



- Moving on to PTS POI devices – the intro of 8-digit BINs has led some vendors and users of POI devices to ask whether:
- Devices approved to the PTS POI standards can implement truncation methods that exceed first six / last four digits, in order to support PANs with 8-digit BINs?
- The answer is, of course...
- Yes

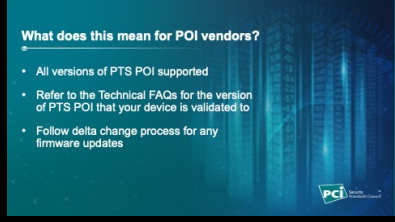
Considerations for PTS POI devices



- The applicable requirement in PTS POI was updated in version 6.1 of the standard
  - Allow for support of 8-digit BIN, per brand-defined truncation limits as defined in FAQs such as FAQ 1091
- Devices validated to previous versions - v3, v4, and v5 – that need to support evolving truncation formats can also follow the testing requirements of the most current version of the POI standard
- This means that acceptable truncation formats (as defined in FAQs) can be included in firmware updates for POI devices approved to any version of the POI standards.

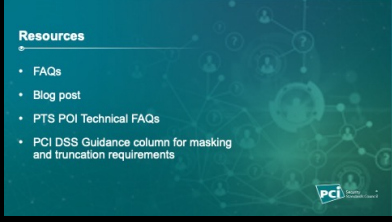
Next Slide: What does this mean for POI vendors?

What does this mean for POI vendors?



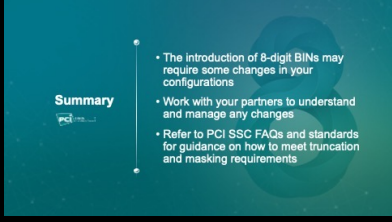
- All versions of PTS POI standards support updated truncation formats
- Vendors are encouraged to read the Technical FAQs for the version of PTS POI that your device is validated to,
- and
- Follow the PTS delta change process for any firmware updates that need to be made in order to support 8-digit BIN

Resources



- If you're looking for more info on 8-db, PCI SSC has a number of resources that can help
- FAQs – search 'BIN' – guidance on truncation and masking considerations
- Blog post – Intro to 8-db and what to keep in mind
- Standard specific:
  - Technical FAQ docs for PTS POI standards
  - PCI DSS Guidance column for masking and truncation requirements

Summary



- To understand if/how 8-db might impact your environment -
  - First 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.
  - Remember that you're current trunc. format could still meet your needs
- You're not alone – talk to your processing partners to understand and manage any changes
- Refer to our FAQs and guidance for truncation and masking requirements for different standards

LAST SLIDE