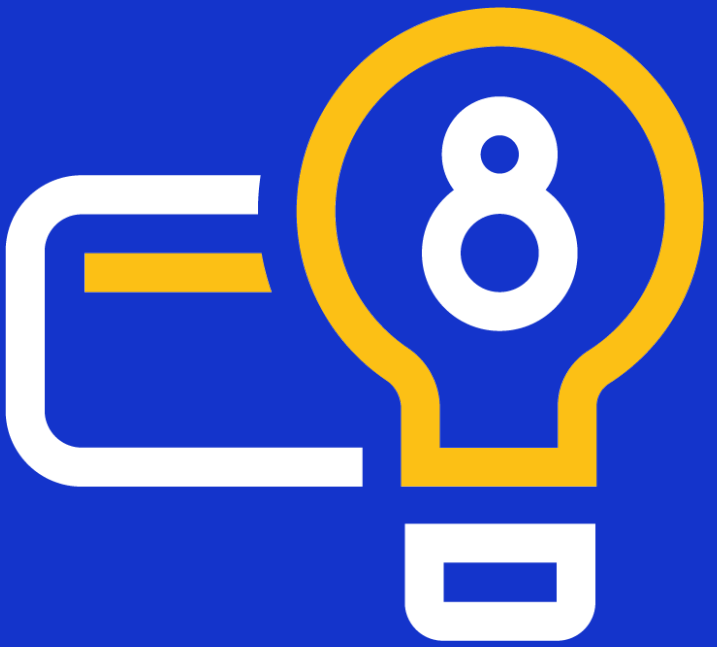
Numerics Initiative
8-Digit BIN PCI Webinar

Presenter: Chackan Lai

Date: 13 January 2022



Agenda

- **8-Digit Issuing BIN Overview**
- **PCI DSS Requirements**
  - PAN Masking
  - PAN Unreadable
    - PAN Hashing
    - PAN Truncation
      - PCI FAQ 1091
    - PAN Encryption
      - PCI FAQ 1086
- **PCI DSS Requirements and Solutions**
- **Q&A**

8-Digit Issuing BIN Overview

1

To address an **industry shortage**, the International Organization for Standardization (ISO) **expanded the length of the BIN standard from six to eight digits**

2

Visa is supporting this change with a client-focused plan; **most of the impacts are within client systems**; the issuing **BIN is not used in VisaNet processing**.

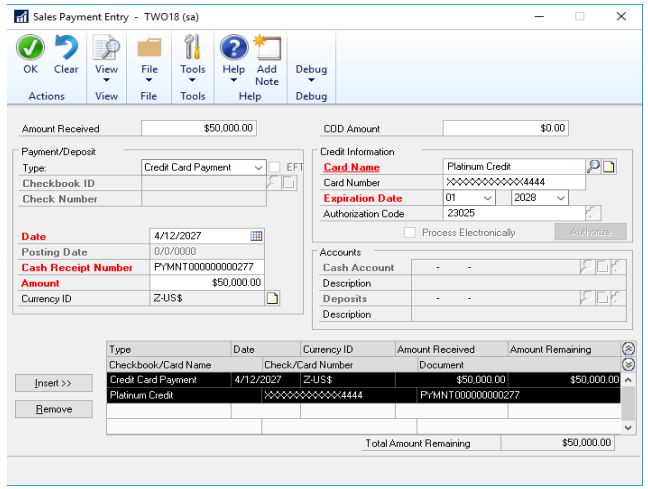
3

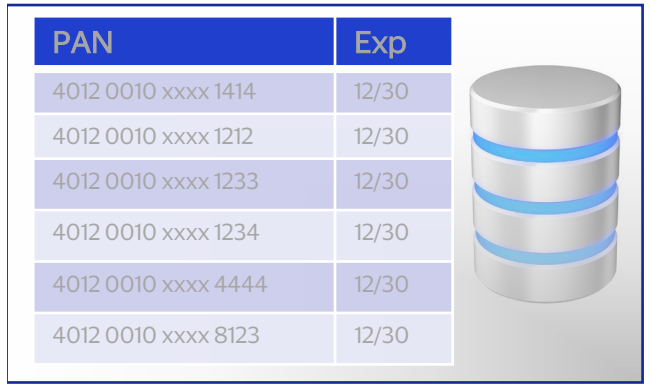
Clients should be well underway **now** with their cross-functional plans to **ensure readiness** across their processing and downstream systems.

PCI DSS Requirements

PCI 3.3 - PAN Masking

DSS Requirement	PAN Masking	Definition and Description
• **Only applies to the display of PAN in receipts, screens, printouts etc.** • **No changes with migration to 8-digit BIN** • **Maximum – first six; last four** • **PCI 3.3 allows for display of full 16 digits based on business need.**	Mask PAN when displayed (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	Masking is a method of concealing a segment of 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. When there are business needs, PCI allows display of full 16 digits.





PCI DSS Requirements

PCI 3.4 – Render PAN Unreadable

DSS Requirement	PCI 3.4 Render PAN Unreadable[1]	Definition and Description
Only applies to PAN when stored	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) • Strong cryptography with associated key-management processes and procedures.	One-way Hash A one-way function based on a cryptographic algorithm that creates an irreversible and unique dataset. PAN Truncation Truncation is a method of rendering a full PAN unreadable by *permanently* removing a segment of PAN data according to approved truncation formats. PAN Encryption A method that applies a reversible algorithm to secure the PAN or specific digits within the PAN such that the PAN or its digit is available to any entity with the cryptographic keys. PCI requirements only require the use of strong cryptography.

1. Applies to PANs that are electronically stored

PCI DSS Requirements

PAN Hashing

- No changes with migration to 8-digit

Cardholder Data Environment

In Scope*

Truncated Database

PAN	Exp
5FD924625F6AB16A19490E4BA675F843D5A1	12/30
A665A45920422F9D411F3FFF1FA07E998E86F	12/30
CC9807C7C506AE18137E4867EFDC4FB8A04A	12/30
4A0743E6B87F074864C2FAE5983C88956CB2	12/30
882D608F5882D608F549A68C15C0D6E26C8B	12/30
63B3B71038B968BB2781DC7873AD202B73	12/30

In Scope*

*Any client or partner acting on the recommendations herein should consult a PCI Qualified Security Assessor (QSA) to fully understand how changes to their environment may affect their compliance to the PCI Data Security Standard (PCI DSS).

PCI DSS Requirements

PAN Truncation

- Maximum allowed to be displayed is first 8 and any other 4. This applies to PANs with either 6- or 8-digit BINs
- Truncated PAN database – Out of scope for PCI DSS

Cardholder Data Environment

In Scope*

Truncated Database

PAN	Exp
4012 0010---- 1414	12/30
4012 0010---- 1212	12/30
4012 00 -- ---- 1233	12/30
4012 00 -- ---- 1234	12/30
4012 0010---- 4444	12/30

Out of Scope*

* Any client or partner acting on the recommendations herein should consult a PCI Qualified Security Assessor (QSA) to fully understand how changes to their environment may affect their compliance to the PCI Data Security Standard (PCI DSS).

PCI DSS Requirements

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

Link to PCI FAQ

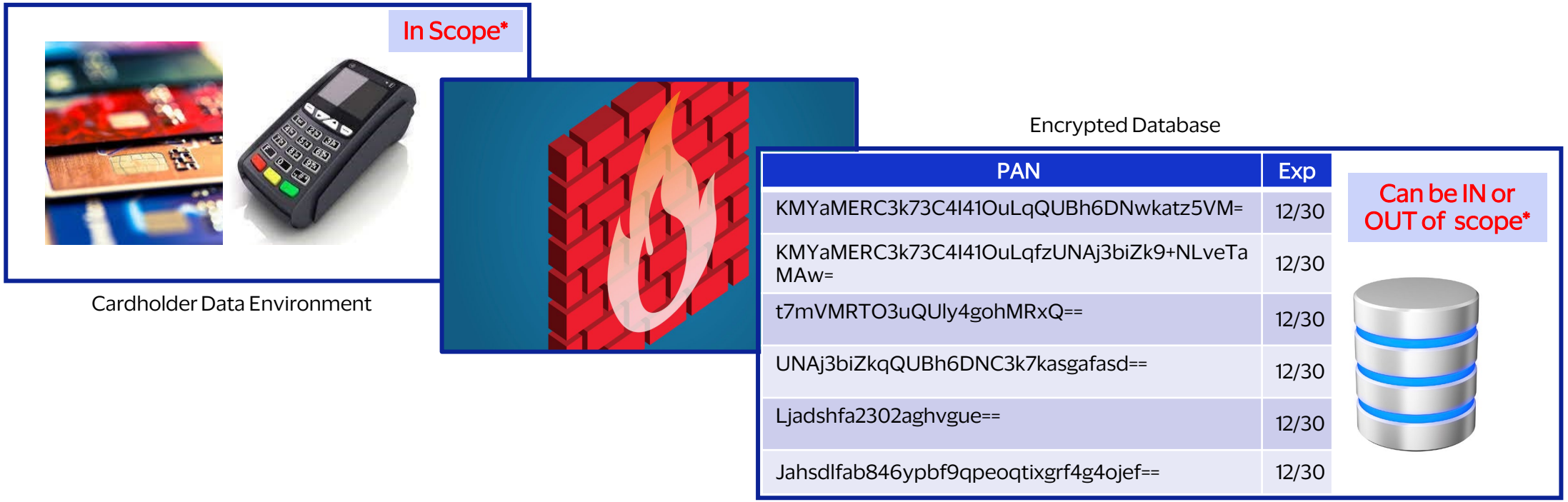
Type "1091" in Search box and click submit.

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: • digit PAN: "first 6, any other 5" • digit PAN: "first 6, any other 6" • 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"

PCI DSS Requirements

PAN Encryption

- No changes with migration to 8-digit BIN
- Use of strong cryptography as defined in PCI DSS is required.
- **Encrypted database MAY be out of scope for PCI DSS assessments – refer to FAQ 1086**



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

PCI DSS Requirements

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

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 in order 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?"

PCI DSS Requirements and Solutions

Masking vs Truncation vs Encryption – Applicability

Requirement	PAN Masking	PAN Truncation	PAN Encryption
• **Requirement 3.3 - Display of PAN**	Yes	No	No
• **Requirement 3.4 - Storage of PAN using acceptable methods**	No	Yes	Yes
• **Requirement 4.1 - Transmission of PAN**	No	No	Yes