# GLB 11848.1 Guidance for Issuers to aid Law Enforcement with Tokenized Data Requests

**Type:**
Bulletin announcement

**Category:**
Operations

**Audience:**
Issuer
Processor
Branded Processor
Network Enablement Partner

**Region:**
Global

**Brand:**
Mastercard®
Debit Mastercard
Maestro®

**Product or service:**
Mastercard Digital Enablement Service

**Action indicator:**
Informational

**Published:**
15 July 2025

**Effective:**
15 July 2025

## Executive overview

Law enforcement may make requests to issuers where a token may be linked to a specific criminal investigation. This announcement gives Mastercard Digital Enablement Service (MDES) issuers guidance on how to assist law enforcement with their inquiries on tokens.

### Table 1: Effective date details

| Date | Details |
|---|---|
| 15 July 2025 | The guidance for MDES issuers is effective. |

### Customer benefit

Issuers can efficiently assist law enforcement during investigations.

### What Mastercard is doing

Mastercard recognizes that issuers handling tokenized card credentials sometimes face challenges when engaging with law enforcement agencies, leading to uncertainty about how to provide assistance and share relevant information with law enforcement.

### Table 2: Version history

| Date | Description of change |
|---|---|
| 15 July 2025 | Initial publication date |

## Issuer guidance

Law enforcement may contact issuers with card or token details to assist with an investigation. There may be times when such requests are highly urgent, for example, to capture a criminal at large, or provide evidence for a serious crime and so on.

Issuers must:

- Have suitable processes in place for assisting law enforcement.
- Ensure that such processes can accommodate urgent requests.
- Validate that the requests are legal, and meet local regulatory requirements for sharing any requested cardholder data. If an issuer shares Primary Account Numbers (PANs), they may also benefit from Mastercard's free tools designed to support such requests. For

example, Mastercard offers services like the BIN Lookup API and the Simplified BIN and Account Range Table (SBART), both available at https://developer.mastercard.com, which can help confirm whether a PAN, group of PANs, token, or token set belongs to a specific issuer.

Issuers may also wish to inform law enforcement agencies about these tools when responding to official requests, as they can streamline verification and improve response accuracy.

Once a legal and vetted request has been received, issuers should be aware that such a request may be on a plastic card, or may be on a token, and that law enforcement would unlikely be able to tell from their data whether their request is relating to a token.

When a plastic card is part of the request, issuers should already have suitable processes in place.

When a token is part of the request, issuers should validate if the PAN presented is on one of their token account ranges.

To validate:

1. Navigate to MDES Manager
2. Click the ▾ button and select **View**

**Figure 1: View option in MDES Manager**

3. Scroll to the **Enablement Projects** section, and click the number of 'Account Ranges'

**Figure 2: Account Ranges in Enablement Project**



© 2025 Mastercard. Proprietary. All rights reserved.
GLB 11848.1 Guidance for Issuers to aid Law Enforcement with Tokenized Data
Requests • 15 July 2025                                                                                              5

Issuers:

- Can use various data extract files, such as IPM MPE tables, the Simplified BIN Account Range Table, or the BIN Lookup API to obtain all of their account ranges.
- May determine the underlying card and therefore the account, and the cardholder when issuers receive a request on a token, by one of these:
  - Using their own mapping:
    If a customer maintains their own token mapping, they can query this to retrieve the underlying PAN, and the real cardholder.
  - Using their own data:
    Customers may be able to use their own reports, databases, transaction logs or other tools, to find a transaction on the token, and retrieve the underlying PAN, and the real cardholder.
  - Using Transaction Investigator:
    Customers can use the Transaction Investigator tool, available in Mastercard Connect. To retrieve the real PAN, customers may search by the token, find a transaction, and obtain the real PAN. This process is a quick way to establish the underlying card, and an expedient way to assist law enforcement.

## Figure 3: Transaction Investigator tool

For transactions in the last 72 hours, select 'near real time', else select credit for dual message, or debit for single

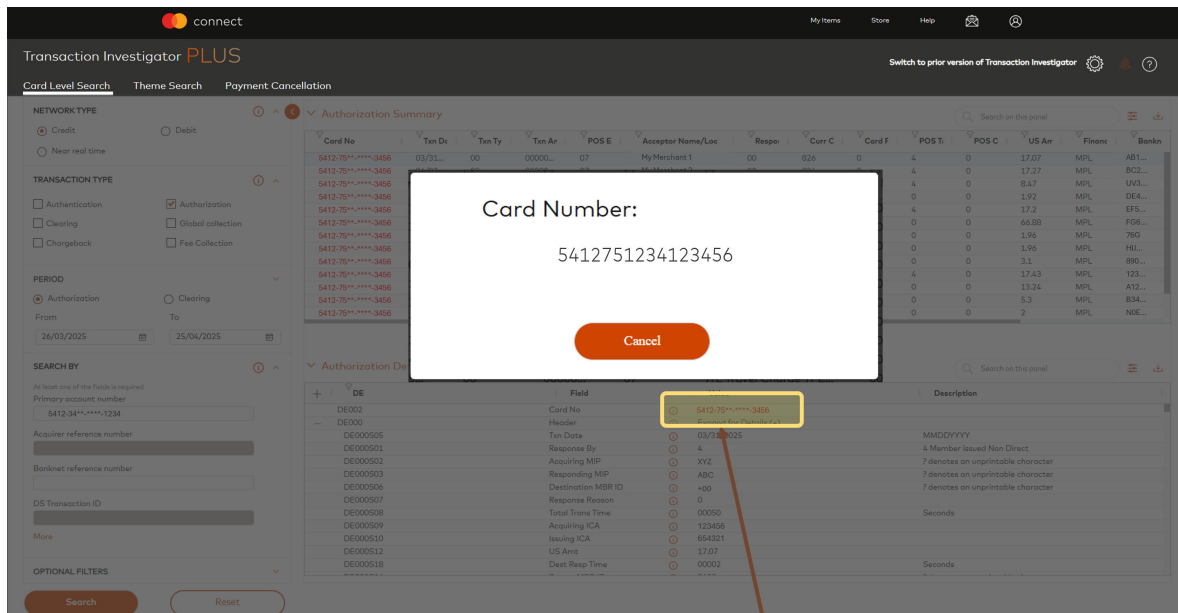Select the date range for the transaction(s) being researched



Enter the token/DPAN in this field

GLB 11848.1 Guidance for Issuers to aid Law Enforcement with Tokenized Data Requests • 15 July 2025

**Figure 4: Card number**



Click the masked card number to reveal the funding PAN

The Transaction Investigator tool can also search by Banknet reference, authorization response code, and other fields which may be useful when only partial information is available. Issuers may be able to combine information from their host platform with the Transaction Investigator tool to aid with law enforcement requests.

Once the issuer has the funding PAN from any of the above tools, they will be able to use their own systems to find the cardholder, and any specific details requested by law enforcement.

**NOTE: All PANs, bank identification numbers (BINs), and account ranges in this document are created using fictitious data. No cards or tokens will ever be issued on these ranges. The data is mocked up to help show how to use the tools.**

## Questions

Customers with questions about the information in this bulletin announcement should contact Global Customer Service using the contact information on the Technical Resource Center.