Mastercard® Threat Scan FAQ

What is Mastercard Threat Scan?
Threat Scan assesses issuer production authorization networks for vulnerabilities to fraud by emulating known criminal transaction behavior. It evaluates issuer host network functionality and configurations against a number of actual and theoretical vulnerabilities to highlight potential points of exploitation for issuers.

What are the benefits to issuers?
As fraud behaviors evolve, issuer authorization networks are continually at risk of exploitation. To prevent attacks, issuers need to ensure proper authorization validation is in place, discover emerging fraud trends that expose their network to risk and ensure their network is functioning properly after a development release. Vulnerability assessments ensure the safety of issuer host production networks, but they can face challenges when implementing in-house testing strategies. Issuers may lack the expertise, support staff, time, budget or commitment to develop and perform tests to assess network safety. Threat Scan assesses issuer production authorization networks for vulnerabilities that can expose them to criminal attacks, helping issuers to:

- Gain critical insights into their authorization networks—enabling a greater understanding of vulnerabilities and gaps in authorization security that require extra attention
- Reduce fraud losses and preserve brand integrity by assessing vulnerabilities in host authorization networks *before* exploitation and fraud loss can occur

In which markets is it available?
Threat Scan is available to all issuers globally.

For which transactions is it available?
Threat Scan supports all Mastercard brands (i.e., Mastercard, Maestro©, and Cirrus©), segments (i.e., consumer and commercial), and products (i.e., credit, debit, and prepaid) for transactions processed via the Mastercard network.

How does Threat Scan Work?
Threat Scan assesses issuer production authorization networks for vulnerabilities by emulating known criminal transaction behavior and analyzing how issuers respond. Threat Scan assesses a multitude of transaction types such as chip, contactless, magstripe and eCommerce transactions to evaluate issuer host network functionality and configurations against a number of actual and theoretical vulnerabilities, highlighting potential points of exploitation for issuers such as:

- PIN manipulation—use of issuer-side weakness in the PIN validation process
- Pre-play attacks—use of defective number generation algorithms to send fraudulent transaction requests from rogue chip-enabled cards
- Relay attacks—use of real-time communication between a fraudulent terminal device and a fraudulent card; pulling transaction data from genuine card/cardholder and pushing it to a genuine terminal
- Counterfeit fraud—use of fake card data in magnetic stripe or EMV transactions based on stolen or created PANs
- Card-not-present (CNP) fraud—use of fake data in eCommerce based on stolen or created PANs

mastercard.
©2018 MASTERCARD. PROPRIETARY AND CONFIDENTIAL.

- Lost or stolen card (Wedge) attacks—use of an intermediate device inserted between a lost and stolen card and a genuine terminal
- Replay attacks—valid data for a transaction that has already been approved is fraudulently repeated
- Fraudster-induced exception processing—fraudster sends a transaction with unexpected data; causing confusion to the issuer's network
- Cross-contamination fraud—data that is read from one interface of the card is used to simulate a transaction conducted via a different interface

Threat Scan provides issuers with Scan Session Reports which may include:

- The scope of each scan session performed
- Parameters evaluated during the scan session
- High-level information of the detected vulnerabilities
- Additional observations which may have been discovered during the scan
- Detailed information of each vulnerability including a summary, background and suggested steps for remediation

After Threat Scan assesses the issuer network against vulnerabilities, all interjected transactions are immediately reversed, ensuring no impact to cardholders or issuers.

Does Threat Scan take the place of issuer fraud detection systems?
No. Threat Scan complements an issuer's existing fraud tools by calling out measures that can be taken to assess authorization networks in production *before* they can be exploited. Whereas Threat Scan works to assist in preventing known potential fraud by identifying gaps in the issuer network. Fraud detection systems and tools are needed to detect unknown fraud during authorization by using fraud models to identify evolving fraud patterns.

Does Mastercard guarantee fraud protection for issuers using Threat Scan?
No. Threat Scan provides an assessment that helps issuers prevent potential fraud attacks, alerting them to vulnerabilities and gaps within their authorization security. There is no guarantee that a fraud event will not occur. Mastercard franchise rules remain in place.

Does Threat Scan keep account-sensitive information secure?
Threat Scan complies with Payment Card Industry (PCI) Data Security Standards requirements. However, it also features components that are integrated and run on each user's system and may expose sensitive cardholder data if the user's system is not suitably protected. It is always the responsibility of the Threat Scan user to ensure their system is appropriately protected and that risks linked to potential disclosure of sensitive data are appropriately mitigated using industry best practices.

What are high-level implementation considerations for issuers (e.g., coding, system changes, etc.)?
Implementing Threat Scan is easy. To enroll, issuers must simply agree to terms and conditions located on Mastercard Connect®. There is no coding required. Issuers only need access to Mastercard Connect.

©2018 MASTERCARD. PROPRIETARY AND CONFIDENTIAL.

Issuers may choose from two complementary deployment options for Threat Scan.

1. ***Issuer-Managed*:** This option allows issuers to perform their own comprehensive set of assessments on their host production authorization network based on account criteria. Issuers control the frequency and timing of their network assessments, performing them at their convenience. They perform assessments using accounts they have issued and card readers/devices they support. After the scan session is complete, issuers will receive immediate detailed results via Scan Session Reports. Issuers must access the Threat Scan application on Mastercard Connect to perform assessments and review Scan Session Reports.

2. ***Mastercard-Managed*** *(coming soon)*: With this option, Mastercard performs a standard set of assessments of the issuer host production authorization networks using a basic set of test cases. Mastercard performs assessments once monthly using accounts selected from Mastercard authorization data or those supplied/registered by the issuer. Mastercard provides issuers with pass/fail results via Scan Session Reports.

Do Threat Scan customers participating in the Issuer-Managed deployment option require a terminal to test PANs in a production environment?
No. Issuers participating in the Issuer-Managed deployment option do not require a terminal for testing cards. Only a card reader and cards are required.

How does Threat Scan compare to similar services in the market?
To date, no other provider offers the same capabilities to issuers—since only Threat Scan:

- Identifies gaps in authorization security by conducting assessments within the issuer's production (instead of testing) environment,
- Assesses a multitude of transaction types such as chip, contactless, magstripe and card-not-present/eCommerce,
- Utilizes the Mastercard network to find new criminal behaviors and further update test cases – ensuring accurate assessments
- Leverages Mastercard's holistic and real-time global view of the payments ecosystem

What is the pricing?
The Threat Scan pricing structure includes a monthly service fee for issuers.

Fees vary by region. Please refer to the Mastercard Consolidated Billing System (MCBS) manual for additional pricing details.

©2018 MASTERCARD. PROPRIETARY AND CONFIDENTIAL.