mastercard

Limit fraud exposure by assessing vulnerabilities in authorization networks

MASTERCARD® THREAT SCAN

Issuer authorization networks are continually at risk of exploitation. Threat Scan assesses issuer production authorization networks for vulnerabilities that can expose them to criminal attacks, providing network insights that can help issuers realize fewer fraud losses with a proactive approach to fraud prevention.

Fraudsters continue to find points of vulnerability in issuer networks

Fraudsters are finding ways around seemingly secure authorization networks. It is estimated that 8% of all fraud losses globally are attributed to weaknesses in issuers' authorization networks.[1] By 2020, 60% of enterprise security budgets will be allocated to rapid detection and response approaches.[2]

Over **1,530 issuers** have experienced **62K+ fraudulent cryptograms** this year meant to exploit gaps in authorization networks. If these had been successful, issuers would have **lost > $6.7 million**.[3]

8% of all fraud losses are attributed to weak authorization networks[1]

Issuers may face challenges implementing in-house network testing efforts

Issuers need to assess vulnerabilities and gaps in their production authorization networks to:

Learn from past fraud attacks by ensuring proper authorization validation is in place to prevent against future attempts

Discover emerging fraud trends that expose their network to risk

Ensure their network is functioning properly after a development release

Exploitation of issuer networks warrants additional safety measures. However, issuers may lack the expertise, support staff, time, budget or commitment to develop and perform tests to assess network safety.

1. COGNIZANT. SECURE PAYMENTS: HOW CARD ISSUERS AND MERCHANTS CAN STAY AHEAD OF FRAUDSTERS. 2016. 2. GARTNER. SHIFT CYBERSECURITY INVESTMENT TO DETECTION AND RESPONSE. 2017. 3. MASTERCARD DATA WAREHOUSE. 2016.

Identifying vulnerabilities within issuer authorization networks

Threat Scan assesses issuer production authorization networks for vulnerabilities to fraud by emulating known criminal transaction behavior against a number of actual and theoretical vulnerabilities—highlighting potential points of exploitation for issuers.

Issuers can:

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

Threat Scan offers a pragmatic way for issuers to identify gaps in authorization security by conducting assessments within production vs. testing environments.

Threat Scan helps issuers find vulnerabilities that can expose them to criminal attacks such as:

- PIN manipulation
- Pre-play attacks
- Relay attacks
- Counterfeit fraud
- Card-not-present (CNP) fraud
- Lost or stolen card (Wedge) attacks
- Replay attacks (e.g., cryptogram replay)
- Fraudster-induced exception processing
- Cross-contamination fraud

Implementing is easy—with two deployment options

To enroll, issuers must simply agree to terms and conditions on MC Connect®. With no additional coding required, issuers may choose from two complementary deployment options available via Mastercard Connect®:

OPTION 1
Issuer-Managed

Issuers...

- Perform assessments based on account criteria
- Controls assessment frequency and timing
- Receive immediate detailed results via Scan Session Reports

OPTION 2 (*COMING SOON*)
Mastercard-Managed

Mastercard...

- Performs a standard set of assessments using a basic set of test cases
- Conducts assessments once monthly
- Provides issuers with pass/fail results via Scan Session Reports

For more information, contact your Mastercard account representative.