GLENBROOK

FraudWatch: The ‘How To’ of Preventing BIN Attacks

Q2 2023

About FraudWatch

- Quarterly briefings from Mastercard and Glenbrook
- Each briefing focuses on a specific payments risk or fraud topic
- Format
  - Trends and metrics related to the quarter's topic
  - A deep dive into a specific payments risk or fraud topic
  - Observations and takeaways

For any specific questions, please reach out to your Mastercard representative or fraudwatch@Mastercard.com

Speakers

Glenbrook

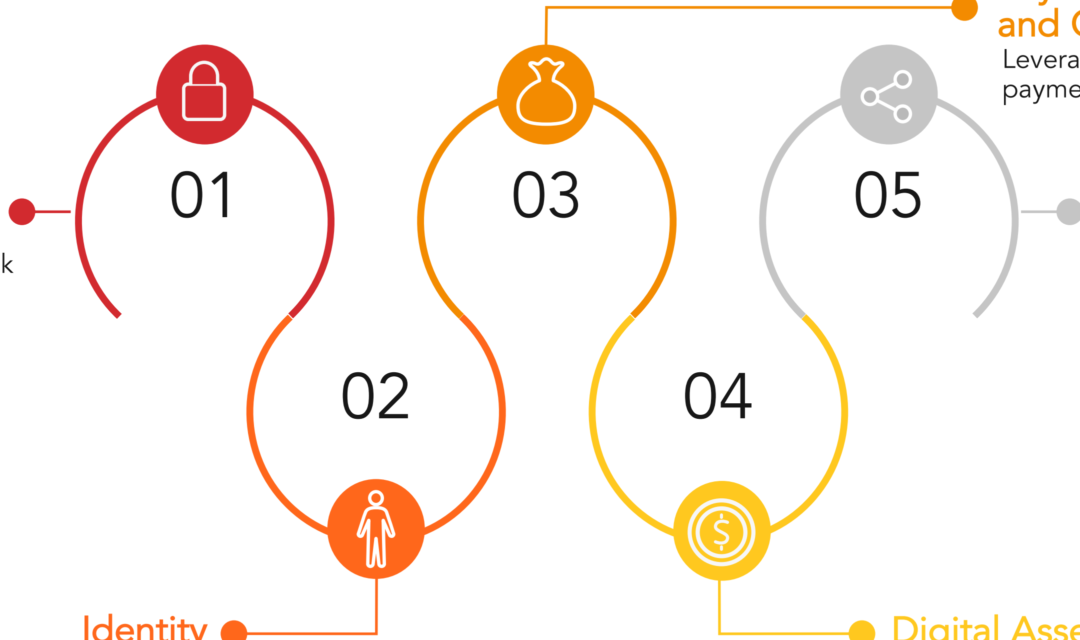
Chris's 25+ years in payments and risk management and C-suite experience brings Glenbrook's education programs to life and incorporates practical expertise in our client engagements

Mastercard

Kerry is SVP of Fraud and Decisioning Products at Mastercard with over 25 years' experience in banking, payments, and fraud risk management.

Andrew is the Director of Product Management and has 20+ years of experience in the card industry with expertise in card fraud mitigation, risk management and prevention technologies.

Mastercard is evolving with the ecosystem…from securing transactions to protecting trust in every interaction while maintaining the best customer service



Cybersecurity and Risk Management
Ability to monitor cyber risk and ESG

Identity
Provide identity information & behavioral biometrics to any digital experience

Payment Fraud and Optimization
Leverage solutions to reduce card payment fraud and chargebacks

Digital Assets
Add visibility to CRYPTO risk exposure

Connectivity
One connection to access multiple network and services

One trusted source for protection

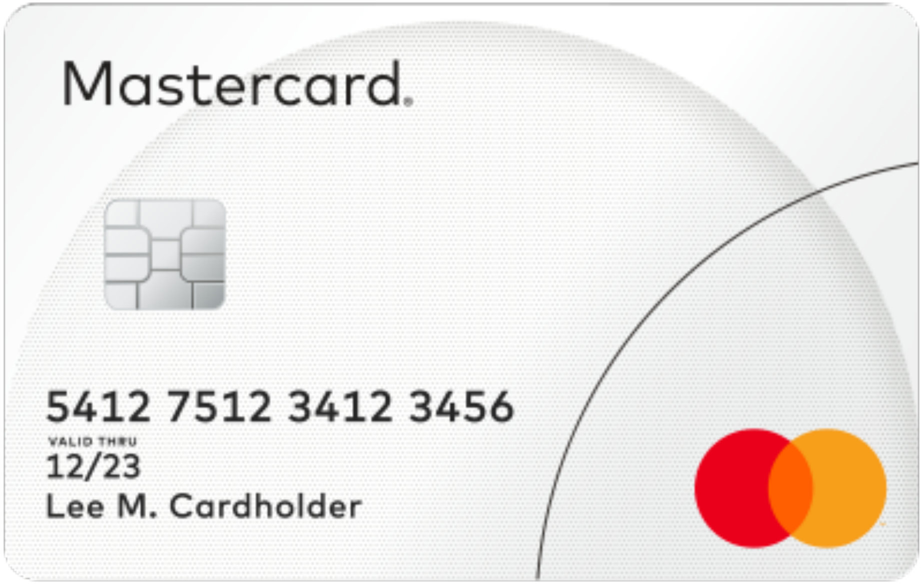
Source: Mastercard

GLENBROOK

Trends and Metrics

A Quick Reminder on BIN Attacks

One type of a third-party payments fraud



Generate cards

Test card for validity

Conduct payments fraud with valid cards

"As new payment features have evolved, BIN file intelligence has not necessarily kept up" – Global Merchant

GLENBROOK

Source: Mastercard

Enablers and Indicators

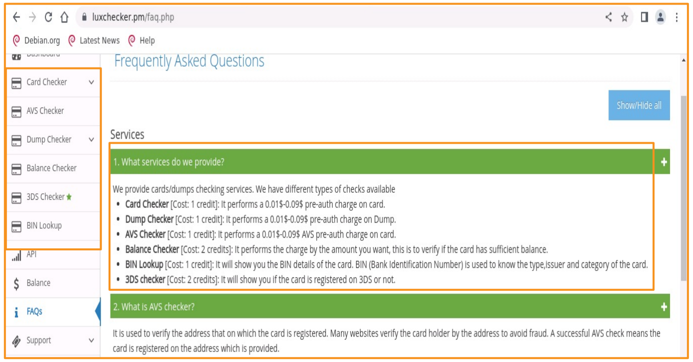
Fraudster BIN Attack Toolkit

Compromised Account Data

Software Tools (e.g., Checker Service)

Merchant Accounts with Weak Controls

Create Merchant Accounts



Frequently Asked Questions

Services

1. What services do we provide?

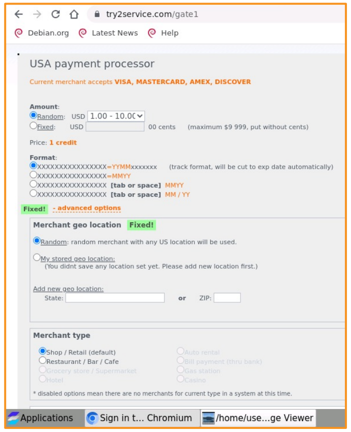
We provide cards/dumps checking services. We have different types of checks available

- **Card Checker** [Cost: 1 credit]: It performs a 0.01-0.09 pre-auth charge on card.
- **Dump Checker** [Cost: 1 credit]: It performs a 0.01-0.09 pre-auth charge on Dump.
- **AVS Checker** [Cost: 1 credit]: It performs a 0.01-0.09 AVS pre-auth charge on card.
- **Balance Checker** [Cost: 2 credits]: It performs the charge by the amount you want, this is to verify if the card has sufficient balance.
- **BIN Lookup** [Cost: 1 credit]: It will show you the BIN details of the card. BIN (Bank Identification Number) is used to know the type,issuer and category of the card.
- **3DS checker** [Cost: 2 credits]: It will show you if the card is registered on 3DS or not.

2. What is AVS checker?

It is used to verify the address that on which the card is registered. Many websites verify the card holder by the address to avoid fraud. A successful AVS check means the card is registered on the address which is provided.

Automated card checking including BIN Lookup



USA payment processor

Current merchant accepts **VISA, MASTERCARD, AMEX, DISCOVER**

Amount:
● Random: USD 1.00 - 10.0(
○ Fixed: USD 00 cents (maximum $9 999, put without cents)

Price: **1 credit**

Format:
● XXXXXXXXXXXXXXXX=YYMMxxxxxxx (track format, will be cut to exp date automatically)
○ XXXXXXXXXXXXXXXX=MMYY
○ XXXXXXXXXXXXXXXX **[tab or space]** MMYY
○ XXXXXXXXXXXXXXXX **[tab or space]** MM / YY

Fixed! **- advanced options**

Merchant geo location **Fixed!**

● Random: random merchant with any US location will be used.

○ My stored geo location:
(You didnt save any location set yet. Please add new location first.)

Add new geo location:
State: or ZIP:

Merchant type

● Shop / Retail (default) ○ Auto rental
○ Restaurant / Bar / Cafe ○ Bill payment (thru bank)
○ Grocery store / Supermarket ○ Gas station
○ Hotel ○ Casino

* disabled options mean there are no merchants for current type in a system at this time.

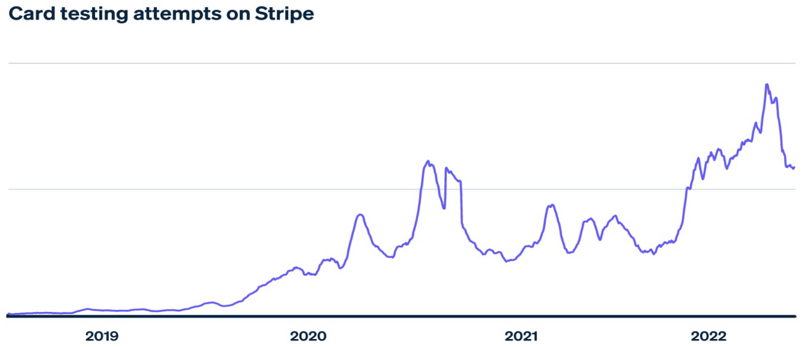
Service that allows you to setup a fraudulent merchant in minutes

Source: Chargeback Gurus

Growth and Impact

On the rise

- Increased 80% globally since 2020
- Many known providers are increasingly being targeted


Card testing attempts on Stripe

Impacts entire payments ecosystem

- Issuers bear the most burden: Financially liable, reputation risk, loss of interchange
- Merchants: goods, money, time, reputation
- End users: money, time, impactful experience

> *"As an enterprise level company, we have to deal with automated attacks, including BIN attacks" – Global Merchant*

GLENBROOK

Source: Insights Co, Stripe

Tell us what you're thinking!

Have you observed an increase in BIN attacks? What do you attribute this to?

Source: Freepik

GLENBROOK

Mastercard Observations and Control Strategies

BIN Attack Trends

Mostly the same with a convergence of different BIN Attack features

Global Phenomenon – Attacks emanate from many geographies

Acquirer Merchant/Issuer Exploitation
Weaknesses in Acquirer/merchant and Issuer controls

Velocity Game
Low dollar with high or low velocity

Weekend Attacks
Late evening/early morning attack

Merchant Info Manipulation
Multiple Names with same Merchant ID & vice versa

Is it Contactless Chip?
POS Entry Mode manipulation

POS Transaction Status Manipulation
Account Status Inquiries (ASI) etc.

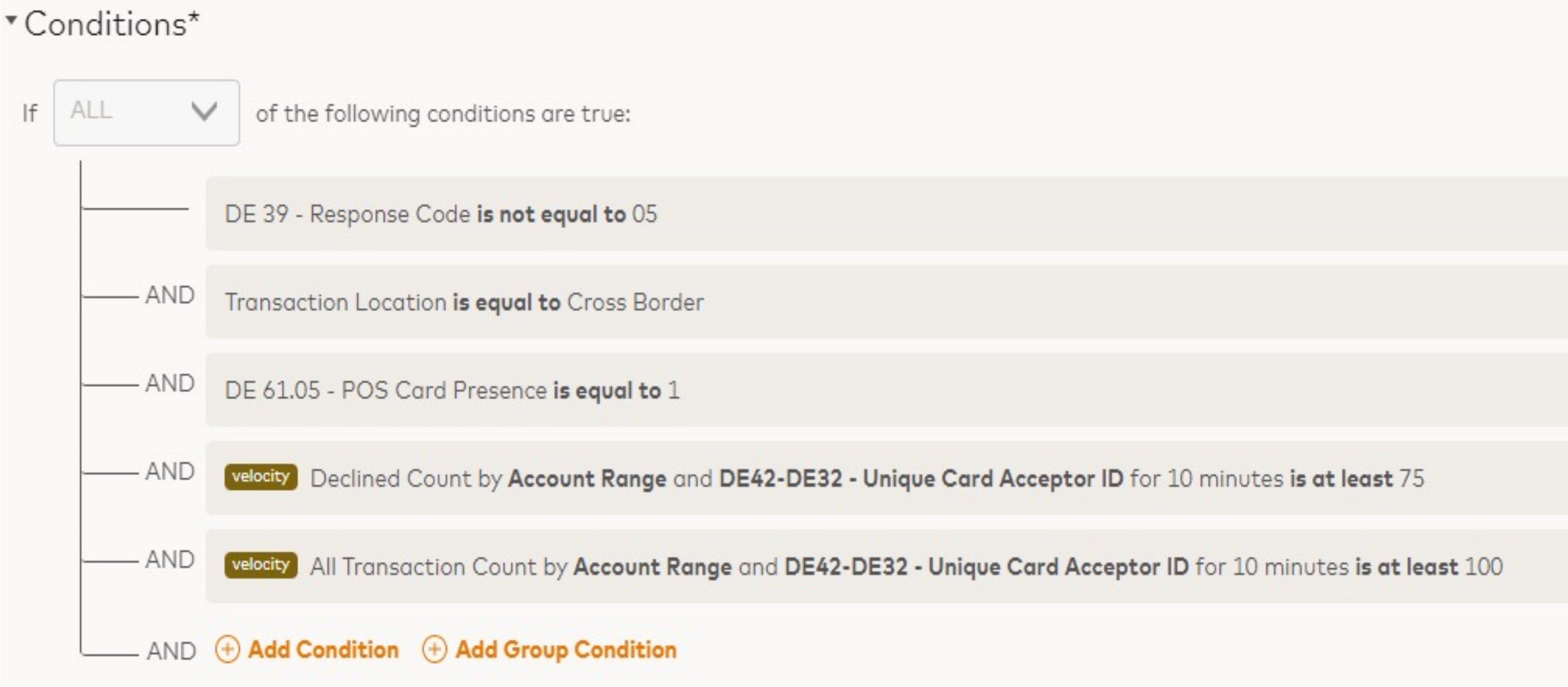
BIN Attacks: What is Mastercard doing?

Education|Enhancement|Enforcement

1. Publication of best practices and other guidelines on Mastercard Connect
2. Identify Egregious Behavior by detecting problematic entities on Mastercard's network that pose risk to overall processing
3. Enforce Transaction Integrity by publishing Mastercard Standards to address repeated instances of account testing
4. Enhance Network Capabilities by implementing solutions to safeguard transaction processing on the payment network
5. Empower Stakeholders by providing the ability to opt-in to receiving authorization advice messages and control real time rule capabilities to address merchant vulnerabilities
6. Self Service Support: Mastercard rule writing platform – Support for BIN level rules with over 150 variables to craft basic and complex rule strategies.
7. Investment in improved AI & Machine Learning Tools

BIN Attack –Mitigation Example

Declined transaction Activity Against Overall Transaction Activity



▾ Conditions*

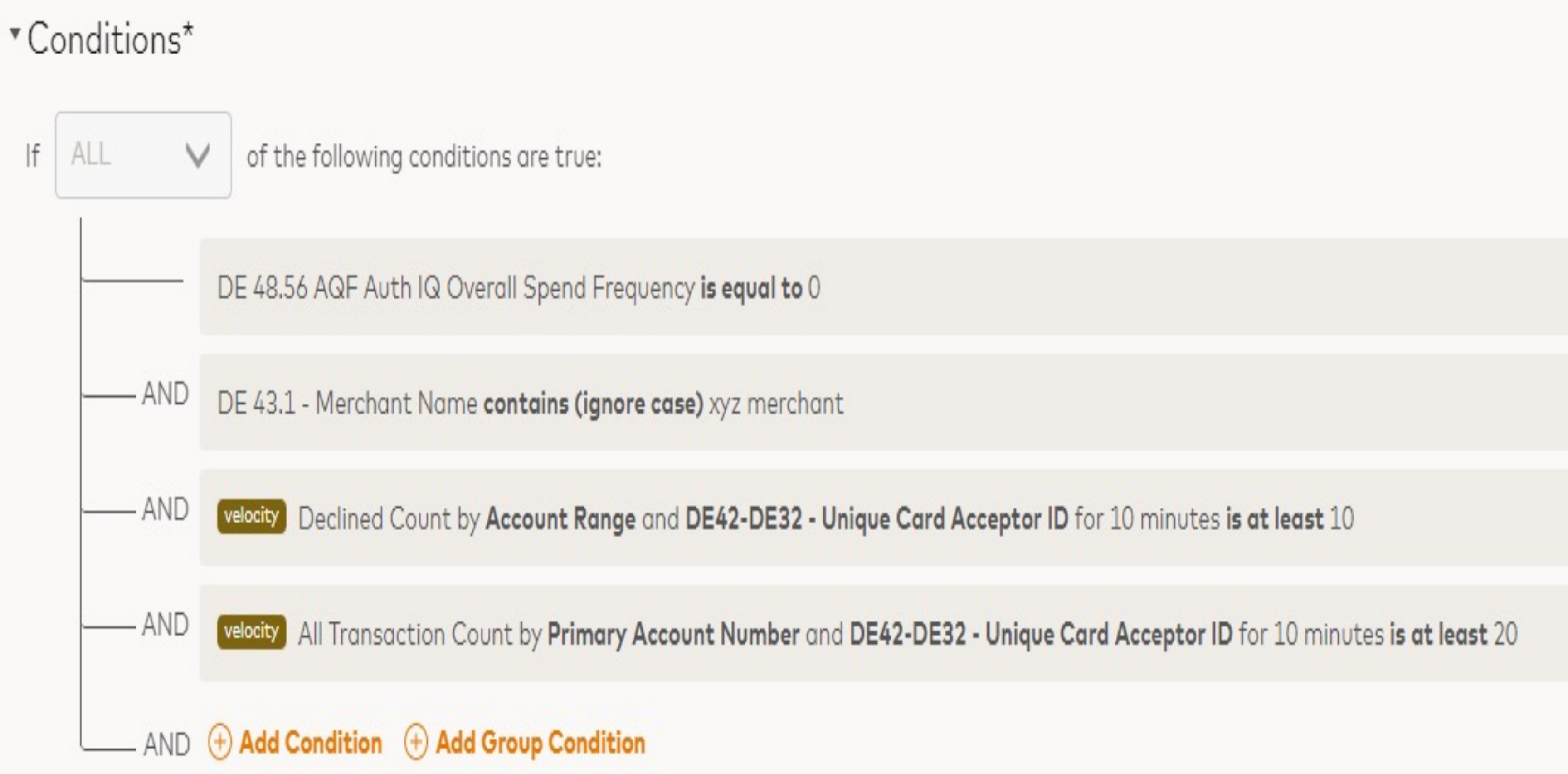
If ALL of the following conditions are true:

- DE 39 - Response Code **is not equal to** 05
- AND Transaction Location **is equal to** Cross Border
- AND DE 61.05 - POS Card Presence **is equal to** 1
- AND velocity Declined Count by **Account Range** and **DE42-DE32 - Unique Card Acceptor ID** for 10 minutes **is at least** 75
- AND velocity All Transaction Count by **Account Range** and **DE42-DE32 - Unique Card Acceptor ID** for 10 minutes **is at least** 100

GLENBROOK

BIN Attack – Mitigation Example

Decline Activity: New cards Same Merchant Short time Duration



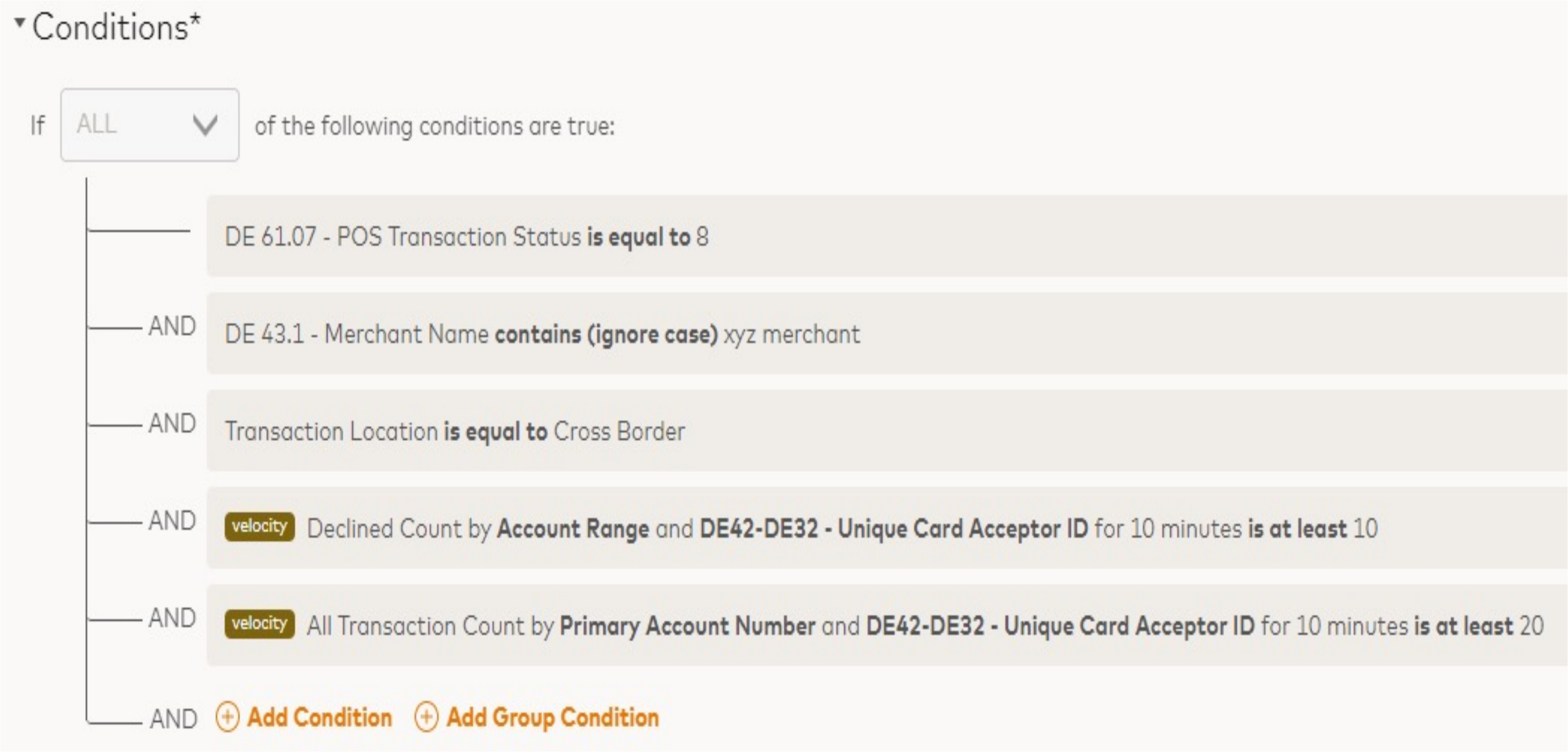
▾ Conditions*

If ALL ⌄ of the following conditions are true:

- DE 48.56 AQF Auth IQ Overall Spend Frequency **is equal to** 0
- AND DE 43.1 - Merchant Name **contains (ignore case)** xyz merchant
- AND velocity Declined Count by **Account Range** and **DE42-DE32 - Unique Card Acceptor ID** for 10 minutes **is at least** 10
- AND velocity All Transaction Count by **Primary Account Number** and **DE42-DE32 - Unique Card Acceptor ID** for 10 minutes **is at least** 20
- AND ⊕ Add Condition ⊕ Add Group Condition

BIN Attack – Mitigation Example

Account Status Inquiries



▾ Conditions*

If ALL ⌄ of the following conditions are true:

- DE 61.07 - POS Transaction Status **is equal to** 8
- AND DE 43.1 - Merchant Name **contains (ignore case)** xyz merchant
- AND Transaction Location **is equal to** Cross Border
- AND velocity Declined Count by **Account Range** and **DE42-DE32 - Unique Card Acceptor ID** for 10 minutes **is at least** 10
- AND velocity All Transaction Count by **Primary Account Number** and **DE42-DE32 - Unique Card Acceptor ID** for 10 minutes **is at least** 20

GLENBROOK

Relevant Mastercard Solutions

Solution	Key Capabilities
Identity Check	• Leverages the 3-D Secure to complete more transactions without disruption • Help eliminate unnecessary friction • Drive approval rates and transaction grow
SafetyNet	• Provides network-level monitoring on a global scale to help identify the occurrence of widespread fraud attacks stakeholders may be unable to detect or defend against them
Decision Intelligence	• Real-time authorization decisioning solution that applies thousands of data points and sophisticated modeling techniques to each transaction • Simplifies insights into a single transaction decision score that helps issuers fine-tune their authorization decisions in order to approve more genuine transactions without increasing risk.
Fraud Insights	• Provides detailed insights and transaction details for fraud, chargebacks, and authorization declines originating on Mastercard network • Enables insights aggregated across an issuer or acquirer's entire portfolio to help detect, analyze, and prevent further fraud
RiskRecon	• Provides risk oversight and management services including Third Party Risk management, supply chain risk, enterprise and subsidiary monitoring • Used by Informatic and Tufts Health Plan
Other Tools	• Fraud Rule Manager – Self-Service Rule Deployment Application • Rules Services – On-behalf fraud prevention rules leveraging Mastercard scores and insights. • Enhanced Services + - Customized Rules with Escalation support

Source: Mastercard

GLENBROOK

Additional Control Strategies

Merchant Controls

1. Monitor and manage the digital environment and vulnerabilities
2. Implement transactional risk management services and other third-party tools to address general payments fraud
3. Put controls specific controls in place to prevent and detect card testing
4. Implement & improve chargeback and dispute management tools

"We talk to our third party to help us make sense of the data" – Global Merchant

Merchant and PSPs/ Third Parties Controls

Monitor / manage digital environment and vulnerabilities

Consider more rigorous merchant onboarding requirements

Modernize transaction fraud and chargeback tools

GLENBROOK

Source: Glenbrook analysis

Issuer Controls

In many ways, Issuer controls mirror Merchant controls

1. Monitor and manage digital environment and vulnerabilities

2. Prevent and detect card testing

3. Implement controls to avoid related payments fraud

4. Implement post transaction review processes

5. Understand and mitigate third party risk

6. Educate consumers

Source: Glenbrook analysis, : Insights Co

Tell us what you're thinking!

What are some of the most effective BIN attack controls that may often be overlooked?

Source: Freepik

GLENBROOK

Q&A