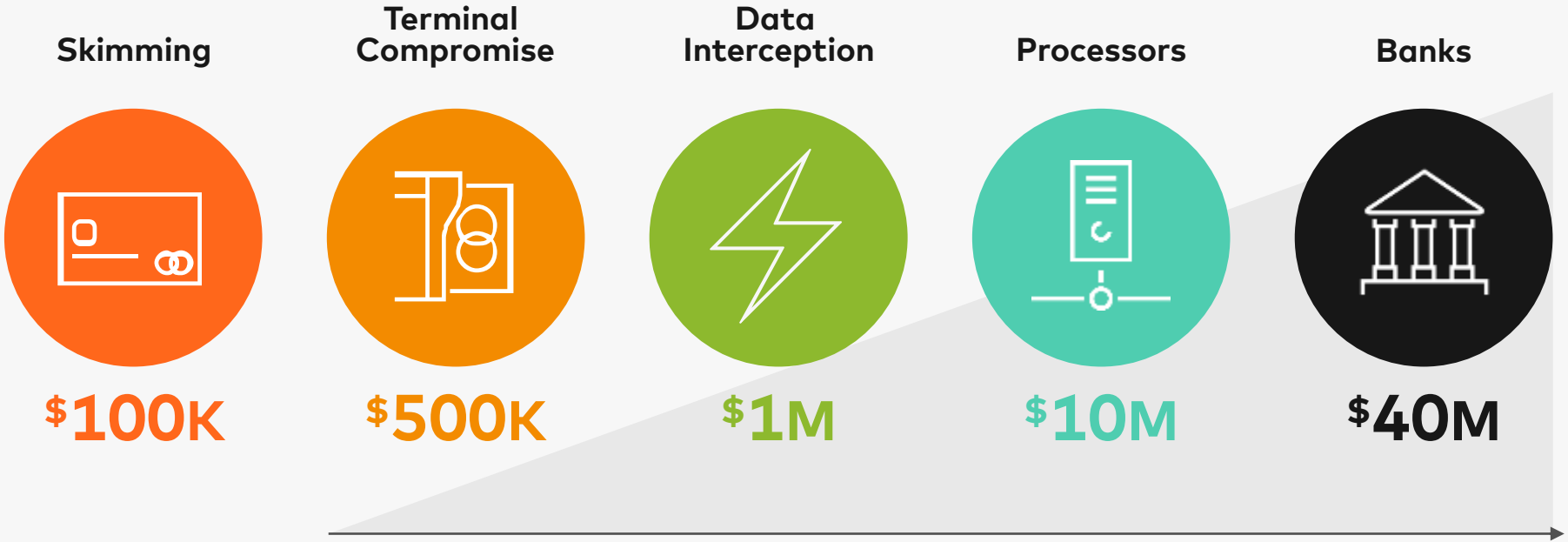
Mastercard Safety Net™

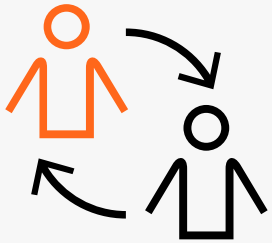
Safeguard against
large-scale fraud events

mastercard

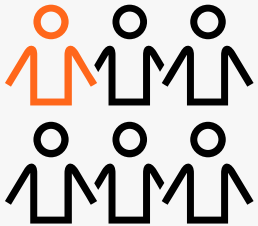
As data compromise evolves, fraudsters grow more sophisticated and drive for scale



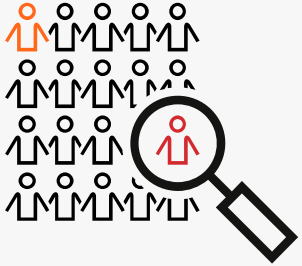
As your business grows, more connections mean greater exposure to large-scale fraud



Growth through innovation, mergers and acquisitions ties your business to **MORE THIRD-PARTY** vendors and partners.



As your network becomes more complex and intertwined, your business is **INCREASINGLY EXPOSED** to fraud on a much larger scale.



Fraudsters drive for scale by exploiting the **WEAKEST LINK** in large network chains, leaving you unable to defend against a large-scale fraud attack.

The sophistication and scale of widespread fraud attacks is escalating

Large-Scale Fraud can occur when an issuer authorization and/or fraud detection system have been disabled and they are unable to detect or defend against an attack.

Map of Carbanak targets

Up to 100 financial institutions were hit at more than 300 IP addresses in almost 30 countries worldwide.

Illicitly obtained credentials result in global card-not-present and counterfeit fraud

Criminals execute fraudulent behavior by abusing merchant terminals and processing information in search of valid cardholder credentials

$46 Billion

Transactions submitted for authorization and tied to various types of fraud attacks—impacting acquirers and merchants in 2017[1]

20 Attacks

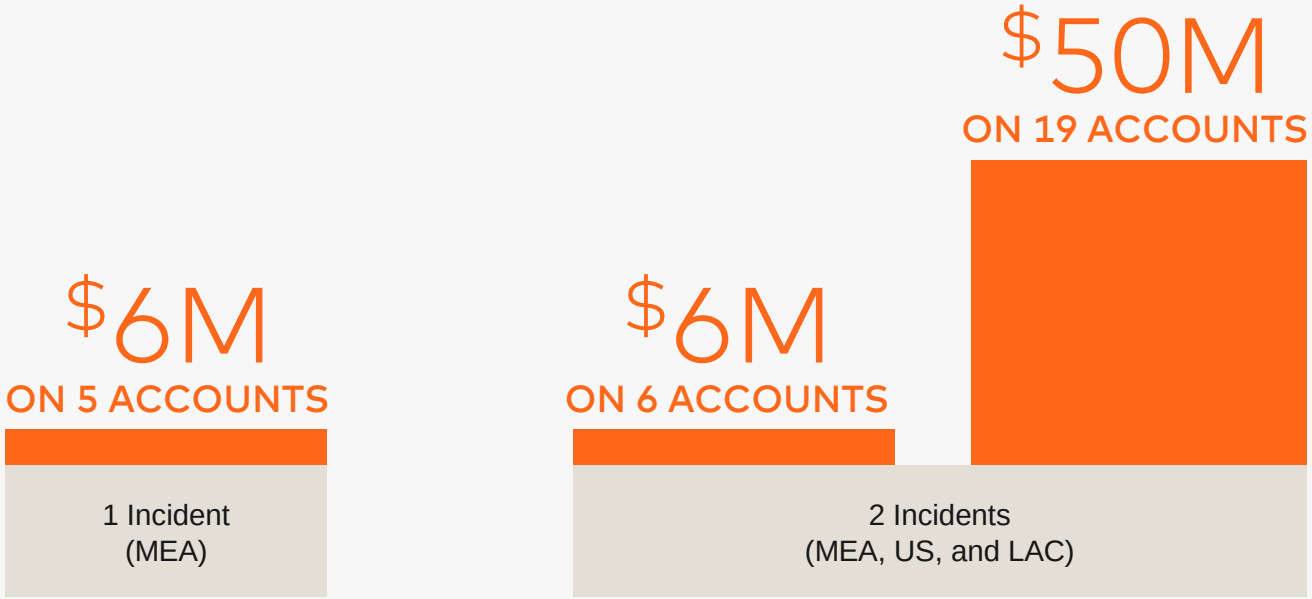
Mastercard Network sees more than 20 attacks per day globally[1]

300 Issuers

Are impacted by brute force attacks every month[1]

1. MASTERCARD. 2017.

Large-scale fraud can quickly result in millions in financial losses from a few unprotected accounts



Beyond financial fraud losses, your reputation and business are at stake

Crisis Containment

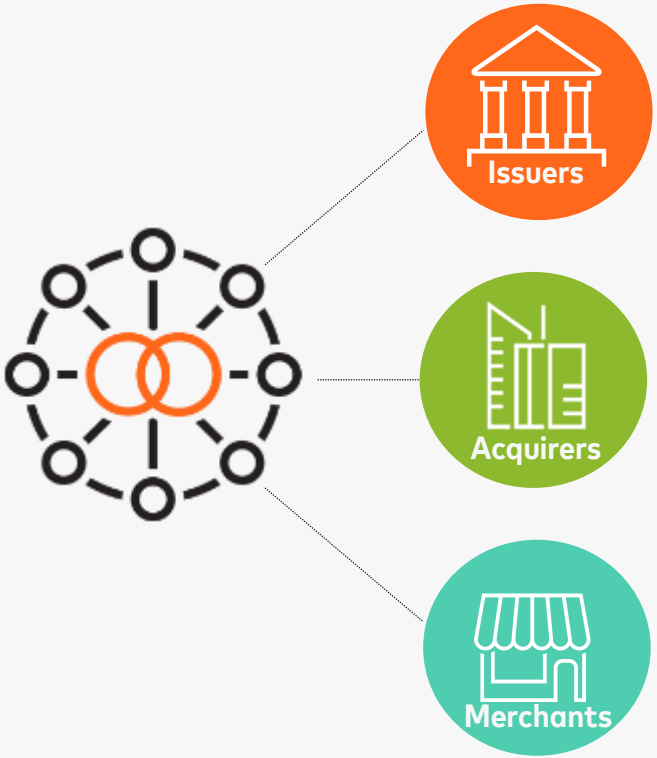
- How deeply have the fraudsters penetrated my defenses?
- How many cards have been compromised?
- How many BINs are impacted?
- What is my real exposure?
- How quickly can I identify and contain the system damage?

Limited Options

Block all activity on one or many BINs

- # of active cards in each BIN
- Lost spend on cards
- Cardholder inconvenience and disruption
- Impact to service center

An extra line of defense against large-scale fraud



- **Real-time visibility and insights into large-scale fraud events** helps to limit losses for issuers, acquirers and processors
- **Network-level transaction monitoring** silently scans global authorization transactions for highly abnormal activity
- **External second layer of defense** independent from but complementary to customer fraud systems and tools
- **Critical protection framework** enables business continuity in the event of issuer/processor system breach
- **Surgical intervention approach** gradually escalates responses to detected threats

Providing real-time visibility outside of impacted systems into large-scale attacks as they occur

BIN Attacks
Brute force, Credit master

ATM Attacks
Cash-out

CNP Attacks
Merchant spoofing

POS Attacks
Duplicate card accounts

Merchant Misuse
Credentials misuse to issue reversals

Authorization Anomalies
Terminal malware manipulation

System Failure
Excessive authorization system maintenance exploitation

Complementing your fraud controls with a secondary level of protection

Mastercard Network Monitoring Level	Enterprise-level Security Standards		**Information Security**		**Cyber Security**		
Safety Net Monitoring Level	Network-level Fraud Monitoring	**Spend/Velocity Thresholds**	**ATM Terminal Monitoring**	**Authorization Integrity**	**Account Profiles**	**Artificial Intelligence**	**Spend Policies**
Issuer/Acquirer Monitoring Level	Transaction-level Fraud Detection		**Fraud Rules**		**Fraud Scoring**		

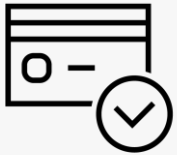
Safety Net at work for issuers

SAFETY NET GLOBAL MONITORING

Silently monitors global auth. for highly abnormal activity

Monitoring criteria is variable and adapted by Mastercard as needed; including but is not limited to:

- Spending patterns across channels, cards and BINs
- Spend amounts over time
- Known anomalies in authorization data
- Location and velocity indicators
- Profiling across transaction channels



TRANSACTION DECLINE

No block—typically just one transaction

- Advice message with declined transactions
- Transaction & List Management utilities
- Dedicated Customer Support

ACCOUNT BLOCK OR ALERT

5-hour temporary block on transactions in channel

- Advice message w/ declined transactions OR
- Alert-only email notification to Auth/Security MIM contacts
- Transaction & List Management utilities
- Dedicated Customer Support

MULTIPLE PANS/BINS

Mastercard Tactical Response Team (TRT) investigation

- Emergency investigation initiated across full response team
- Fraud and authorization experts
- Triage evaluation
- Issuer contacted
- Emergency rules/blocks deployed as needed

1 Reacts upon behavior indicating a potential large-scale attack

2 Gradual response escalation as threat increases

3 Surgical intervention to mitigate attack across multiple cards/BINs

4

Safety Net at work for acquirers

SAFETY NET GLOBAL MONITORING

Silently monitors global auth. for highly abnormal activity

Monitoring criteria is variable and adapted by Mastercard as needed; including but is not limited to:

- Spending patterns across channels, cards and BINs
- Spend amounts over time
- Known anomalies in authorization data
- Location and velocity indicators
- Profiling across transaction channels

ACCOUNT ALERT

Email alert notification

- For a broad array of unusual activity requiring urgent follow-up with merchants
- Dedicated Customer Support

MULTIPLE PANS/BINS

Mastercard Tactical Response Team (TRT) investigation

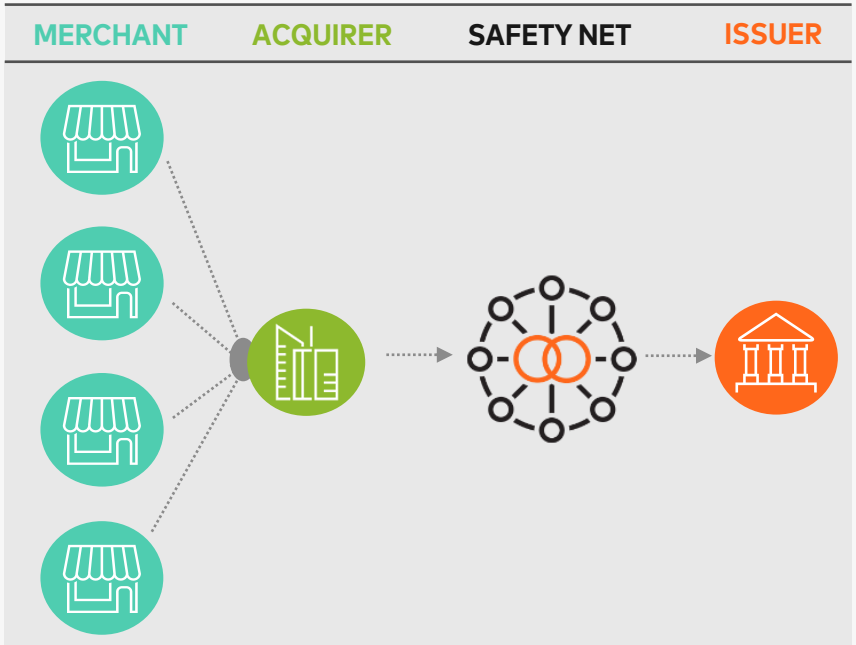
- Emergency investigation initiated across full response team
- Fraud and authorization experts
- Triage evaluation
- Acquirer contacted
- Emergency rules/blocks deployed as needed

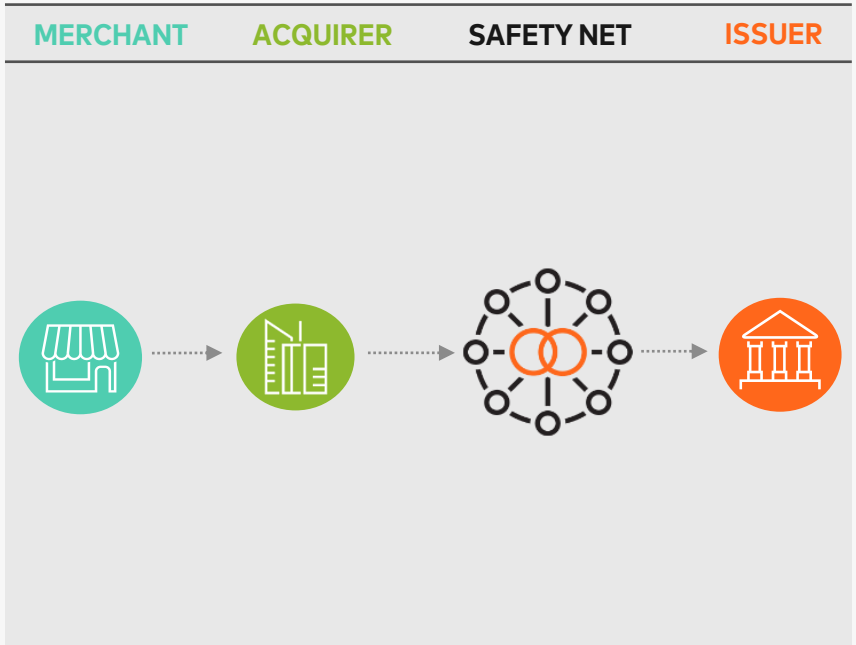
1 Reacts upon behavior indicating a potential large-scale attack

2 Surgical intervention to mitigate attack across multiple cards/BINs

3

Safety Net works differently for issuers and acquirers, even when they are the same organization





An integral part of issuer risk management strategies

1. **Financial Protection**
   Provides a second line of protection when issuer fraud defenses are compromised and can't detect the threat

2. **Regulatory Protection**
   Assists with regulatory concerns about data breaches and network exposure

3. **Reputational Protection**
   Safeguards from reputational damage associated with large-scale fraud attacks

4. **Fast Response**
   Deploys network security quickly against emerging threats across the ecosystem

5. **Turnkey Participation**
   Requires no coding or enrollment forms

Extending security across the network for acquirers

1. **Financial Protection**
   Provides a second layer of protection should criminals disable or compromise first-level fraud defenses

2. **Regulatory Protection**
   Helps avoid certain compliance fines related to fraudulent merchant activities (i.e., ECP)

3. **Reputational Protection**
   Provides real-time insights into merchants impacted by large scale fraud events as they are occurring

4. **Fast Response**
   Enables immediate action, working in combination with merchants and payment processors to stop attacks—including real-time rules to block fraudulent activity if necessary

5. **Turnkey Participation**
   Requires no coding or enrollment forms

Helping issuers avoid over $46 billion in potential fraud losses across markets and channels

Safety Net detected an issuer who had inadvertently disabled chip cryptogram validation, blocking **$11K** in potential fraud losses for a MEA issuer.

System Failure

Safety Net detected an attack resulting from criminals finding a gap in chip validation, blocking **$400K** in potential fraud losses for an LAC issuer.

System Weakness

Safety Net detected an ATM cash-out attack, blocking **$500K** in potential fraud losses for EUR issuers.

ATM Cash-Out Attacks

Safety Net detected a merchant spoofing attack, blocking **$26M** in potential fraud losses for about issuers globally.

CNP Attacks

Safety Net detected a POS attack, and would have blocked **$995K** in fraud losses for an AP issuer who opted out of Safety Net participation.

POS Attacks

Safety Net outperforms the competition

Differentiator	Mastercard SAFETY NET	OTHERS
Globally integrated network-level fraud monitoring across all markets	Provides global fraud monitoring for every market around the world from a single integrated network visibility into global fraud trends and new attack vectors.	Are limited by the markets in which they can provide monitoring or by a non-integrated, multi-platform network which inhibits a holistic view of global activity.
Network-level fraud monitoring for all transaction types and channels	Monitors fraud across all channels for ATM, POS, CNP and Quasi-Cash.	Do not monitor across all channels and transaction types for potential large-scale fraud events (i.e. may only monitor ATM transactions in AP region).
Precise tactical blocking of suspicious transactions	Detects and blocks suspicious spend within a specific channel without impacting issuers' other business areas.	Have limited ability to block transactions; can only block transactions under select conditions.
Blocking activity alerts	Provides automated alerts on blocking activity within 24 hours for immediate assessment, enabling blocks to expire automatically in 5 hours without issuer intervention.	Cannot provide automated alerts and blocking expirations.
Self-service management of blocked transactions	Provides self-service utilities to view blocked transactions in real time and list exceptions to blocking rules.	Do not provide customers with the ability to view and manage blocked transactions via web interface.

Participating in Safety Net is easy for issuers and acquirers

- **Required participation:** Mastercard requires Issuer and Acquirer participation in Safety Net.
- **No enrollment forms:** Mastercard automatically enrolls all BINs in Safety Net.
- **No coding required:** Participate immediately.
- **Update contacts:** Ensure all Security and Authorization contacts are updated in the Member Information (MIM) application.

Participation is monitored by FFIEC order of the White House Summit Cybersecurity and Consumer Protection to advance consumer financial protection and launched the Buy Secure Initiative.

A roadmap for innovation

2017

Artificial Intelligence

Creating dynamic, multi-layer rule strategies beyond business rules alone to ensure Safety Net unpredictability and enable more sophisticated decisions.

2018

Extended Coverage

Utilizing Safety Net in new ways for new payment products such as domestic activity.

Beyond

Enhanced Monitoring

Monitoring at a macro vs. PAN level across all channels using profiles to enhance threshold decisions and evolve single card thresholds.

Mastercard continues to invest **millions** in the deployment and continual advancement of Safety Net around the world.

Issuer Case Studies

Safety Net helps large regional issuer avoid millions in potential fraud losses

In Context

Large issuer experienced sophisticated ATM cash-out attack impacting thousands of accounts across their region.

Situation

A large regional issuer was targeted with an extremely well-organized and sophisticated ATM cash-out attack during weekend off hours. Using a few cards at multiple terminals, fraudsters impacted thousands of accounts with relatively low dollar amounts in a matter of hours.

Solution

Safety Net detected the attack within minutes and started declining transactions on behalf of the issuer while simultaneously alerting issuers of the attack. Mastercard technical teams gathered and implemented controls to minimize the financial and reputational damage to the issuer.

Results

$35M

in estimated fraud losses prevented by Safety Net without impacting the issuer's business and cardholders.

Safety Net alerts issuers to attacks on other networks and brands

In Context

Russian issuers experienced ATM cash-out attacks resulting in substantial fraud loss.

Situation

Over a one-month period, two ATM cash-out attacks on domestic transactions occurred in Russia. Criminals had infiltrated issuer systems, rendering them unable to detect the attacks.

Solution

Safety Net identified and alerted issuers to the abnormal activity, enabling them to respond to the domestic ATM cash-out attacks.

Results

Millions USD lost domestically and on other global brands

In response, Safety Net is now available for domestic transactions not switched by Mastercard.

Monitoring against attacks exploiting system failures

THREAT System maintenance exploitation

1. Fraudsters exploit defects that issuers may inadvertently introduce into system maintenance releases—such as failing to restore spend policy controls after a maintenance window.
2. Issuers can lose millions of dollars quickly to these attacks as they may lack the insights to identify and quickly respond.
3. Safety Net may recognize unusual spend behaviors that issuers cannot detect as a result of the defect. While issuers restore their systems, Safety Net can limit their exposure by isolating suspicious behavior while enabling genuine cardholder spend.

RESULTS

Who	Issuers	Issuer
When	2016	March 2017
Where	LAC and MEA	MEA
Attack	Exploited maintenance releases that introduced system defects disabling internal spend policies	Issuer inadvertently disabled chip cryptogram validation
Result	Safety Net blocked **$250K** in potential fraud losses	Safety Net detected attack and blocked **$11K** in fraud losses

Monitoring against attacks exploiting system weakness

THREAT Authorization parameter manipulation

1. Fraudsters manipulate authorization data to exploit known defects in issuers' processing capabilities resulting in fraudulent or counterfeit transactions being approved.
2. Issuers can lose millions of dollars in a matter of hours from attacks that occur as a result of exploiting system weaknesses, because they may lack the ability to see these attacks as they are occurring and/or the capability to respond quickly.
3. Mastercard continually embeds additional network level protections that help quickly detect large-scale attacks.

RESULTS

Who	Issuers	Issuer
When	January 2016	February 2017
Where	Global	Brazil
Attack	Approval of counterfeit transactions due to invalid authorization data	Criminals exploited vulnerability in chip validation
Result	Safety Net quickly detected the attack and blocked **$3M** in potential fraud losses	Safety Net detected attack and blocked **$400K** in potential fraud losses

Monitoring against cash-out attacks in the ATM channel

THREAT Cash-out attacks

1. Fraudsters infiltrate issuer's system, duplicating a handful of card accounts. In the duplicate accounts, fraudsters disable velocity checks, change available dollar limits on card accounts, etc.
2. The duplicate cards are then distributed to an organized team of mules who use the cards simultaneously at various ATMs in markets globally; the leader continually replenishes card limits.
3. Issuers can lose millions of dollars in a matter of hours from these types of attacks.

RESULTS

Who	Issuer	Issuer
When	August 2016	March 2017
Where	MEA	EUR
Attack	ATM cash-out attack	ATM cash-out attack
Result	Safety Net detected attack within minutes, blocking **$35M** in potential fraud losses	Safety Net detected attack and blocked **$500K** in fraud losses (competitor brand losses totaled $2M)

Monitoring against service attacks in the CNP channel

THREAT CNP attacks

1. Fraudsters hijack eCommerce merchant details to establish themselves as seemingly legitimate online merchants—known as merchant spoofing.
2. Using the stolen merchant credentials, fraudsters submit large quantities of high-dollar transactions in rapid succession.
3. Issuers can lose millions of dollars in a matter of hours by approving transactions from seemingly genuine merchants.

RESULTS

Who	850+ issuers
When	March 2016
Where	Global
Attack	Spoofing merchant credentials for over 6K PANs/9K transactions
Result	Safety Net detected attack at $101K and blocked **$26M** in potential fraud losses

Monitoring against attacks in the POS channel

THREAT POS attacks

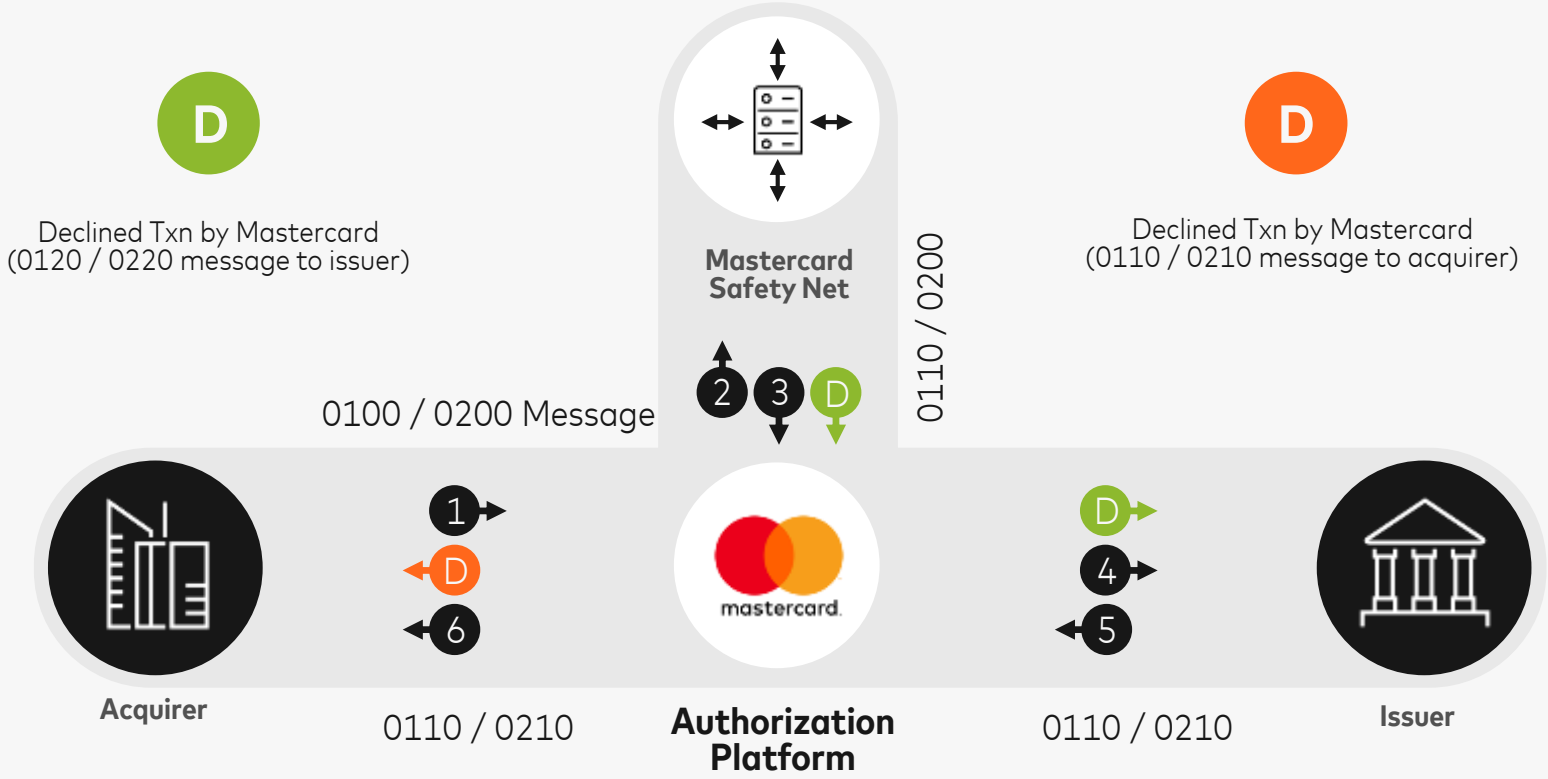
1. Fraudsters infiltrate issuer's system, duplicating a handful of card accounts. In the duplicate accounts, fraudsters disable velocity checks, change available dollar limits on card accounts, etc.
2. The duplicate cards are then distributed to an organized team of mules who use the cards simultaneously at various POS merchants in markets globally; the leader continually replenishes card limits.
3. Issuers can lose millions of dollars in a matter of hours from these types of attacks.

RESULTS

Who	95+ issuers	Issuer
When	April 2016	March 2017
Where	Global	AP
Attack	POS attack from merchants in Brazil	POS attack
Result	Safety Net detected attack at $650K and blocked **$340M+** in potential fraud losses	Safety Net detected attack and would have blocked **$995K** in fraud losses if issuer had not opted out of Safety Net participation

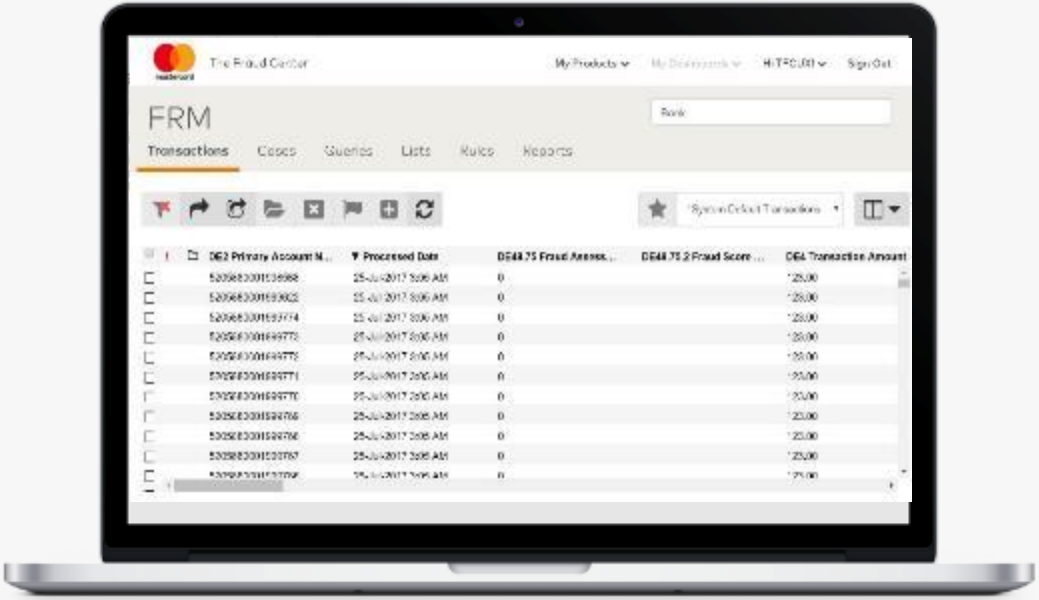
Issuer Security Solutions Utilities

View declined transactions via the advice message



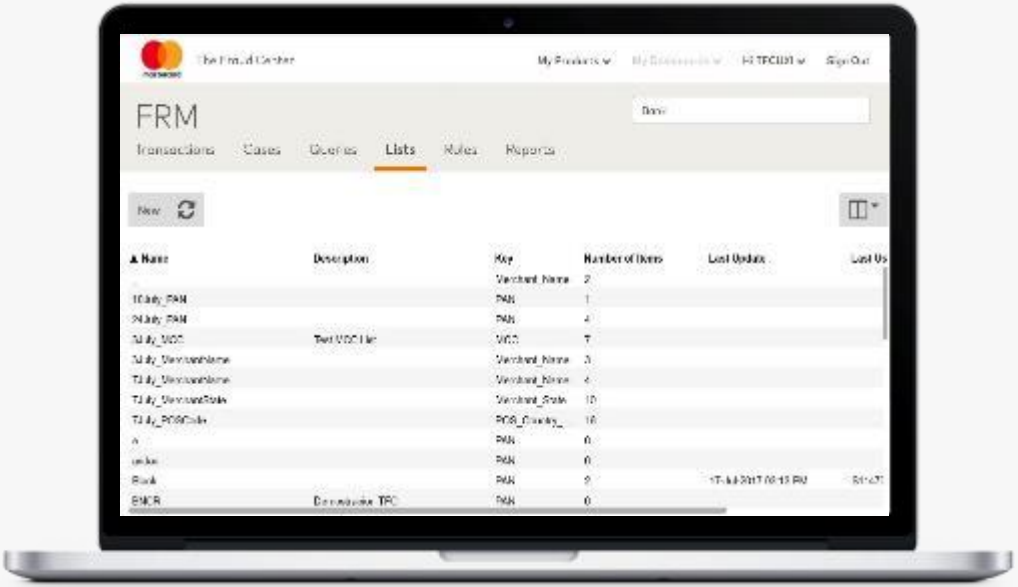
View transactions declined or alerted by Safety Net via Transaction Management

- Real-time access to see any transactions that have been declined or alerted by Fraud Rule Manager, Safety Net, Mastercard Prepaid Monitoring, Decision Intelligence or Mastercard Network Defense
- Access online within seconds of transaction occurrence
- Up to 30 days of data can be accessed
- Available via the Fraud Center on Mastercard Connect®



List accounts to be exempt from Safety Net blocking via List Management

- List criteria you want to include or exclude from rules driven by Safety Net, Fraud Rule Manager or Network Defense
- Add or remove one or more criteria from user-defined lists (i.e. merchants, countries, PANs, etc.)
- Set start/expiration dates for exception
- Access audit history to track activity/use
- Available via the Fraud Center on Mastercard Connect®



NEXT STEPS

Let's get started

For more information on Safety Net, contact your Mastercard representative.