MasterCard Prepaid Monitoring

Providing an additional layer of security and prevention

In a class by themselves, catastrophic attacks can be devastating for issuers

Catastrophic Attacks, are often highly sophisticated, precisely planned, and aimed at rendering issuer systems defenseless

By their design, they are difficult to detect in real-time—which can have devastating effects

Unlike traditional fraud prevention tools most issuers do not have global network-level monitoring capabilities to detect and stop these types of attacks in real-time

FRAUD ALERT

In early 2013, a massive attack on a prepaid program resulted in millions of dollars being stolen, in a matter of hours.

In response to this exposed vulnerability in the system, **MasterCard Prepaid Monitoring** was developed —to help stop catastrophic fraud in its tracks

To address these sophisticated attacks, issuers need a sophisticated solution

Complex payment ecosystems—an attractive target for fraudsters

Prepaid programs have an expanded value chain—which criminals see as an opportunity with more potential points of vulnerability to hack into an account system

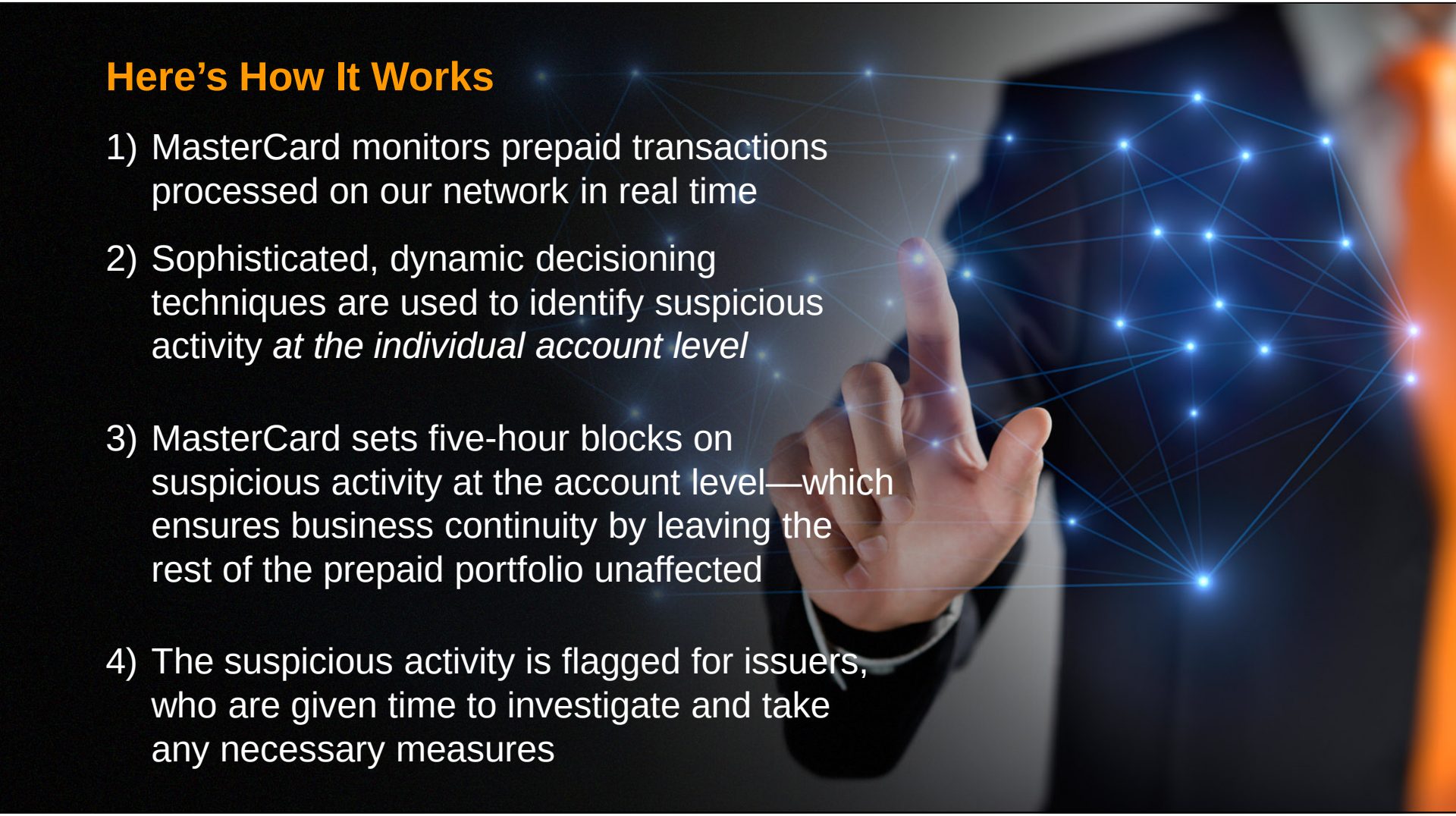
Hackers use sophisticated tactics that typical anti-fraud tools may not be able to quickly detect *(e.g., changing load values, converting cards from closed- to open-loop status, enabling cards for ATM use, and creating duplicate /counterfeit cards for geographically dispersed use)*

Once an account system is compromised, it can be difficult for the issuer to protect against runaway losses

FAST FACT

Leveraging a 24/7 global view, MasterCard Prepaid Monitoring compliments an issuers existing fraud tools—providing an additional layer of security to stop catastrophic attacks.

Identifying activity in real-time and blocking at the account level are essential tactics



Here's How It Works

1) MasterCard monitors prepaid transactions processed on our network in real time

2) Sophisticated, dynamic decisioning techniques are used to identify suspicious activity *at the individual account level*

3) MasterCard sets five-hour blocks on suspicious activity at the account level—which ensures business continuity by leaving the rest of the prepaid portfolio unaffected

4) The suspicious activity is flagged for issuers, who are given time to investigate and take any necessary measures

Prepaid Monitoring has already proven successful—blocking catastrophic fraud

> Fraud prevention never stops. Our ability to monitor suspicious patterns in real-time and immediately act against such activity is essential to the viability of the entire payment system.
>
> - Ron Hynes, Group Executive, MasterCard – Global

Recent catastrophic attacks further demonstrate the value of Prepaid Monitoring

Thwarting a major attack in Middle East/Africa region

In March 2014, MasterCard detected and prevented an attack that had the same patterns associated with potentially catastrophic losses

- MasterCard immediately blocked the attempted transactions and contacted the issuer
- What would have amounted to millions of dollars in losses was limited to just a few thousand

Blocking an attempted “brute force” attack

Prepaid Monitoring recently identified and blocked an attempted CVC2 brute force attack of 46,000 transactions totaling $4.6 billion. This type of attack has historically overwhelmed issuers’ processing systems and resulted in a severe outages and enormous fraud losses.

Prepaid Monitoring acts as a *safety net*— by enhancing existing issuer security tools

Prepaid Monitoring can "step-in" and help issuers:

- Block suspicious activity without impacting the rest of their portfolio
- Protect their business from 'catastrophic' risks
- Support the integrity, reliability and security of their brand
- Demonstrate to stakeholders and regulators an increased ability to combat fraud with additional tools

QUOTE

"Prepaid Monitoring is a like a 'circuit breaker' that automatically responds to suspicious activity and defuses an attack before it can have an impact."

Ron Hynes,
Group Executive
MasterCard - Global

Blocking Options—
What to do if/when an attack occurs

MIP Transaction Blocking

Quickly block an entire BIN for all activity or by broad-level criteria
(e.g., country, region, transaction type, merchant category)

List Manager

Temporarily block or unblock an individual primary account number

Fraud Rule Manager

Selectively block upon variations of sophisticated data elements

Stand-In Range Blocking

Block all transactions during Stand-In processing only

For more information on
MasterCard Prepaid Monitoring,
please contact your
MasterCard representative.