2014 MasterCard Global Risk Conference: *Asia Pacific*

Academy of Risk Management | Innovate. Collaborate. Educate.

Statement of Confidentiality and Disclaimer

The information provided herein is strictly confidential. It is intended to be used internally within your organization and cannot be distributed nor shared with any other third party, without MasterCard's prior approval. This proposal is intended solely to facilitate discussion between the parties. This proposal only sets forth a general description of the financial terms that are anticipated to be included in a proposed agreement between the parties and shall not create a legally binding or enforceable agreement or offer. The parties acknowledge that other terms and conditions are also anticipated to be included in the proposed agreement. Except for the confidentiality obligations stated above, neither party shall be liable to the other party as a result of the failure to fulfill any obligation described in this proposal or the failure to enter into any agreement contemplated by this proposal.

Information in this presentation or in any report or deliverable provided by MasterCard in connection herewith relating to the projected impact on your financial performance, as well as the results that you may expect generally are estimates only. No assurances are given that any of these projections, estimates or expectations will be achieved, or that the analysis provided is error-free. You acknowledge and agree that inaccuracies and inconsistencies may be inherent in both MasterCard's and your data and systems, and that consequently, the analysis may itself be somewhat inaccurate or inconsistent. The information, including all forecasts, projections, or indications of financial opportunities are provided to you on an "AS IS" basis for use at your own risk. MasterCard will not be responsible for any action you take as a result of this presentation, or any inaccuracies, inconsistencies, formatting errors, or omissions in this presentation.

Matthew Parciak, Deputy Chief Information Security Officer, MasterCard
Pee-Beng Ong, Business Leader, Information Security Engineering, MasterCard
Michael Petitti, Executive Director – Asia Pacific, Trustwave

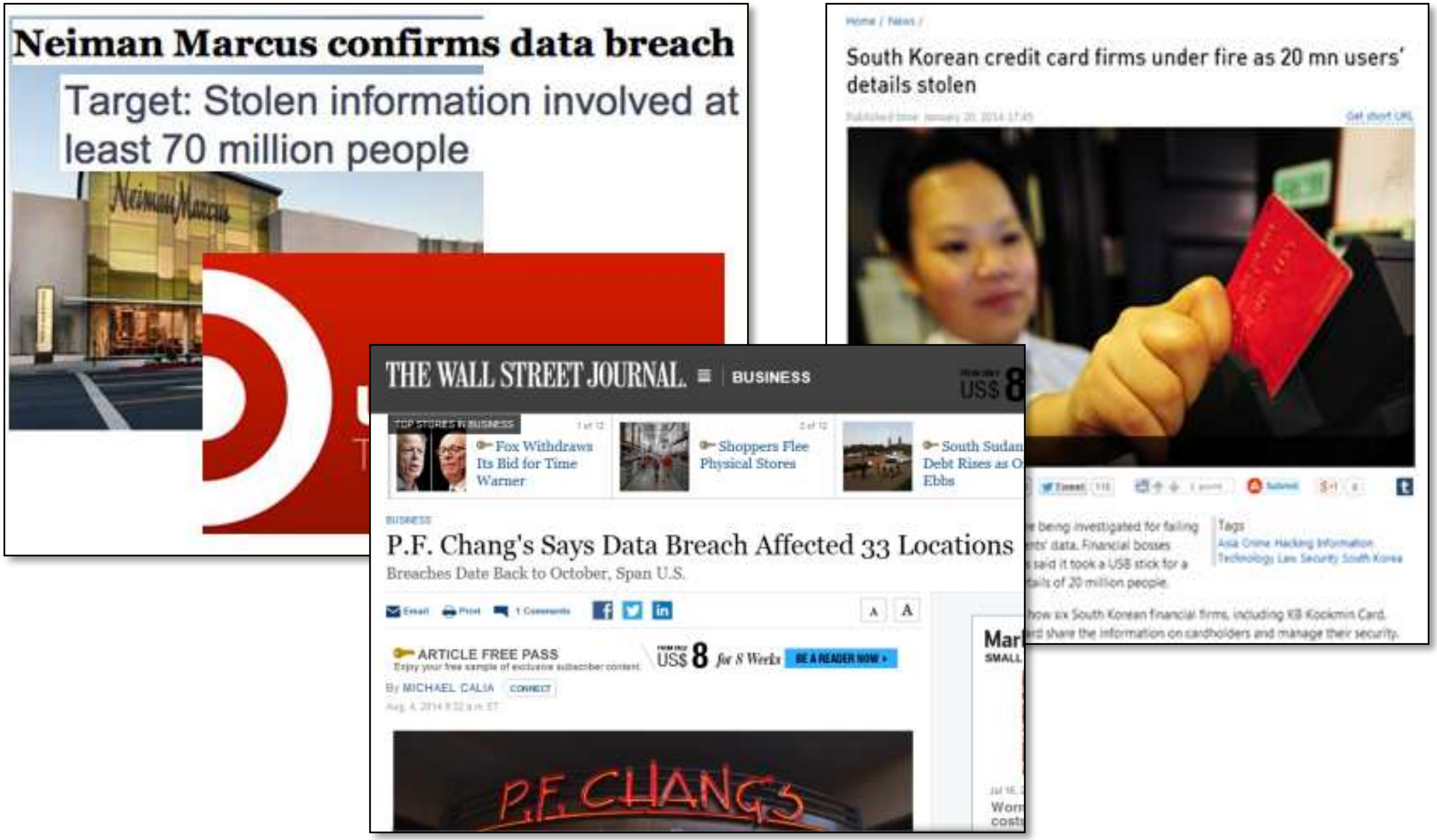
Real-World Strategies to Avoid Cyber Crime

Real-World Strategies to Avoid Cyber Crime

- The Reality
- Best Practices and Strategies
- Q&A

The Reality: Hackers' Success

MasterCard



Neiman Marcus confirms data breach

Target: Stolen information involved at least 70 million people

Home / News /

South Korean credit card firms under fire as 20 mn users' details stolen

Published time: January 20, 2014 17:45

Get short URL

e being investigated for failing
nts' data. Financial bosses
s said it took a USB stick for a
ails of 20 million people.

Tags
Asia Crime Hacking Information Technology Law Security South Korea

how six South Korean financial firms, including KB Kookmin Card,
rd share the information on cardholders and manage their security.

THE WALL STREET JOURNAL. | BUSINESS

TOP STORIES IN BUSINESS

Fox Withdraws Its Bid for Time Warner

Shoppers Flee Physical Stores

South Sudan Debt Rises as O Ebbs

BUSINESS

P.F. Chang's Says Data Breach Affected 33 Locations

Breaches Date Back to October, Span U.S.

Email Print 1 Comments

ARTICLE FREE PASS
Enjoy your free sample of exclusive subscriber content.

FROM ONLY US$ 8 for 8 Weeks BE A READER NOW ›

By MICHAEL CALIA CONNECT

Aug. 4, 2014 8:32 a.m. ET

The Reality – Average Detection Time

INTRUSION TO DETECTION MEDIAN:

87 DAYS

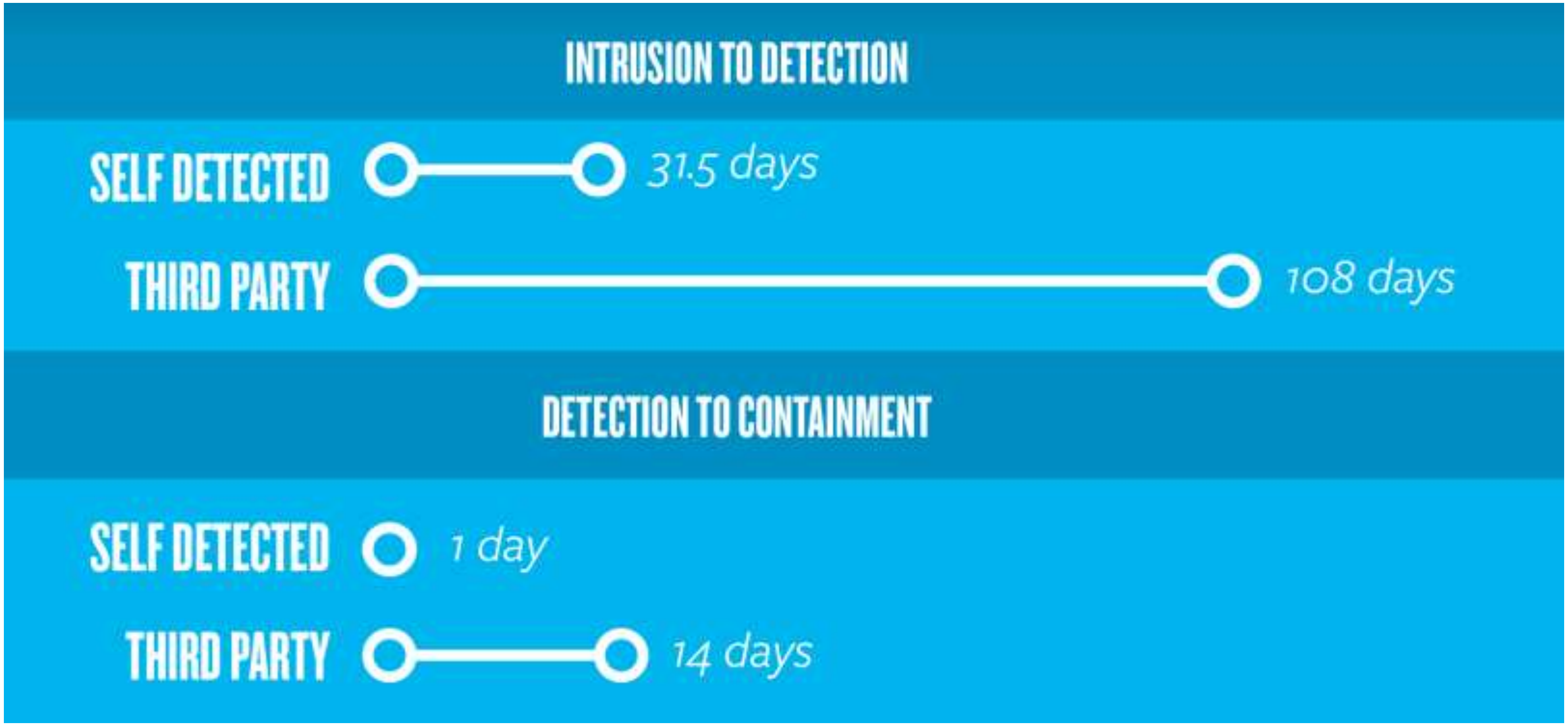
2012 mean: 210 days
2013 mean: 134 days

DETECTION TO CONTAINMENT MEDIAN:

7 DAYS

Source: 2014 Trustwave Global Security Report 2014

The Reality – Duration to detection

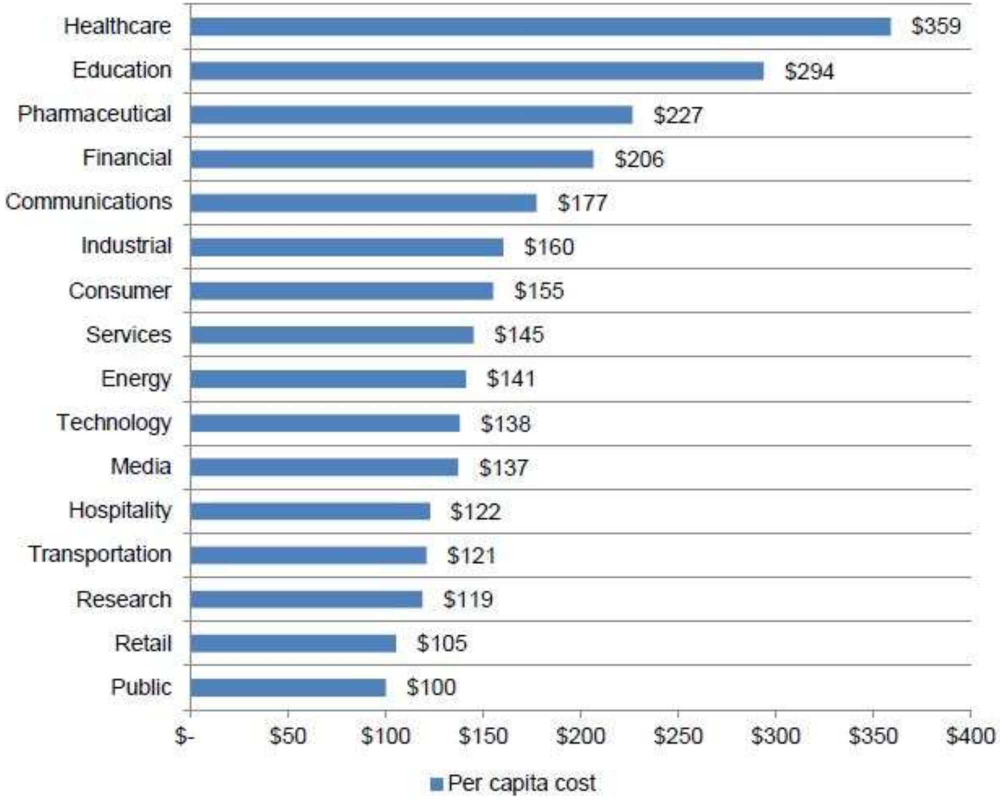


Source: 2014 Trustwave Global Security Report 2014

The Reality – Breaches are expensive!

MasterCard

2014 Cost of Data Breaches by Industry



Source: 2014 Cost of Data Breach Study: Global Analysis. Ponemon Institute LLC.

The Reality - Hacker Motivation

- A business venture = Seeking profits $$$$

- Primary Methodologies:
  - Opportunistic:
    - ✓ high volume, low sophistication, low margin
    - ✓ = Majority of compromises
  - Targeted:
    - ✓ low volume, high sophistication, high margin
    - ✓ = Majority of losses

The Reality - Geography

Origin of Attack

19% - United States

18% - China

16% - Nigeria

5% - Russia

5% - Korea

4% - Germany

4% - United Kingdom

4% - Japan

3% - France

3% - Taiwan

Location of Victims

59% - United States

14% - United Kingdom

11% - Australia

2% - Hong Kong

2% - India

1% - New Zealand

1% - Mauritius

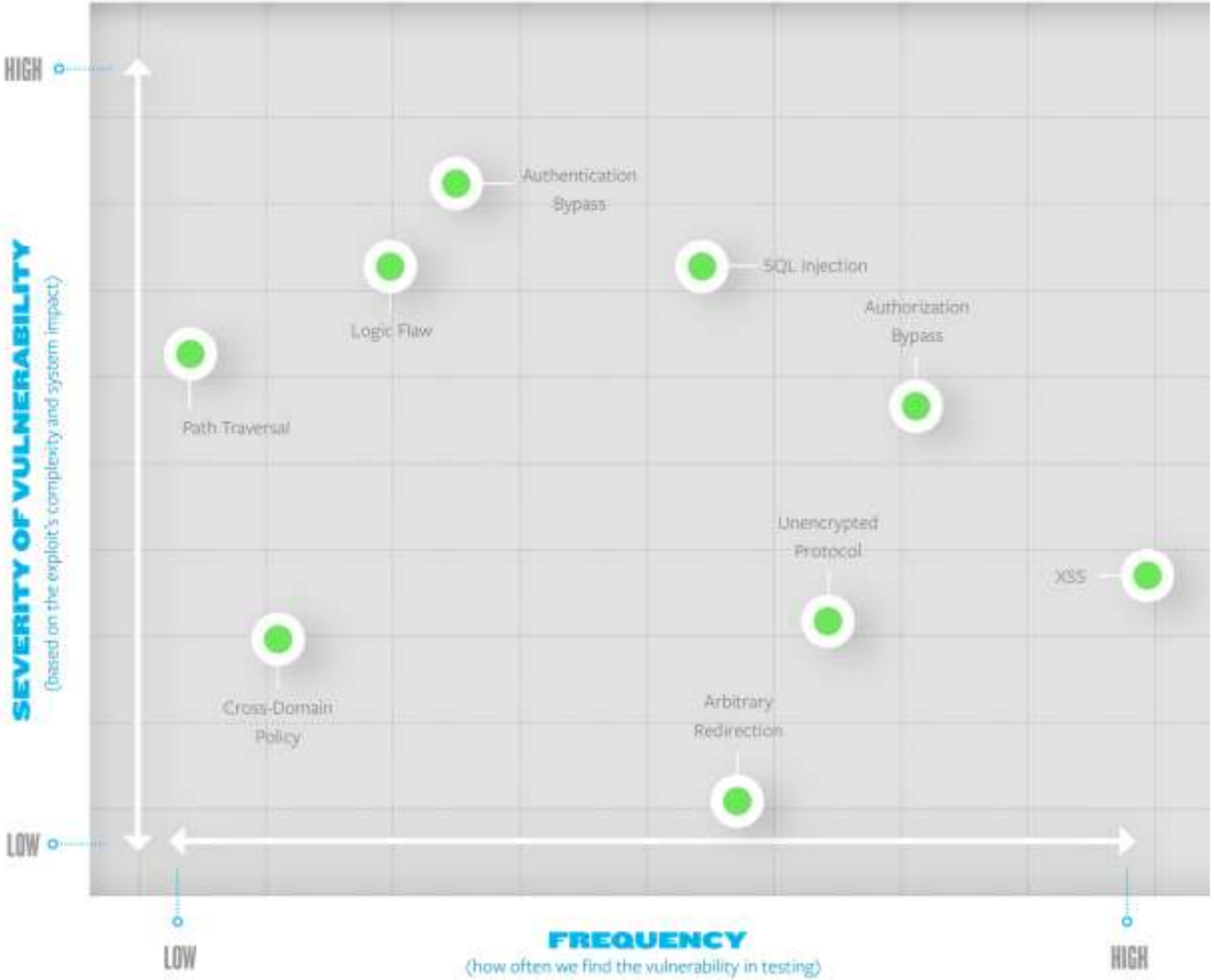
1% - Ireland

1% - Belgium

1% - Canada

Source: 2014 Trustwave Global Security Report 2014

The Reality – Common Exploits



Source: 2014 Trustwave Global Security Report 2014

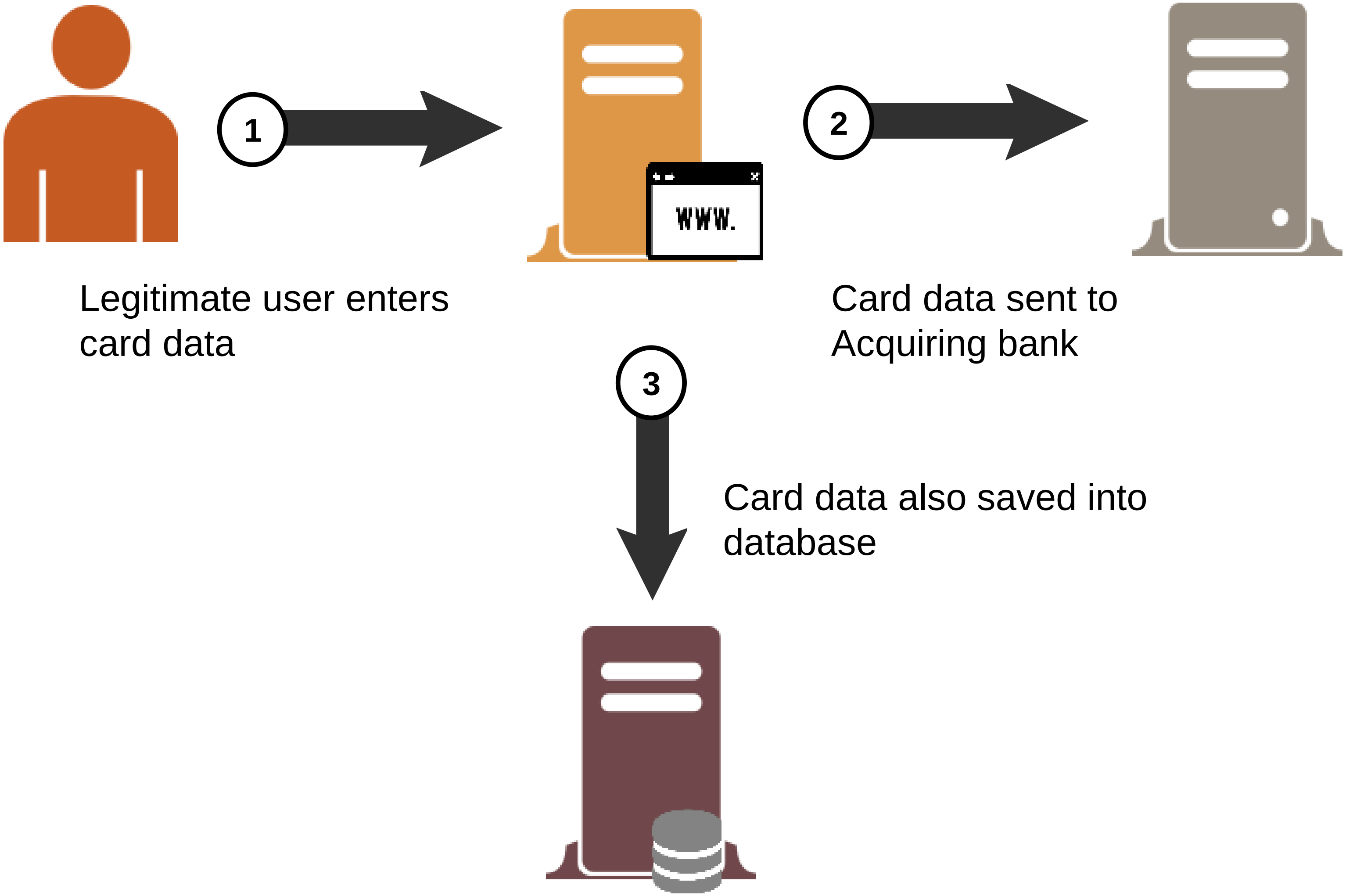
The Reality – Opportunistic Attacks

- Attacker identifies a problem (i.e. Heartbleed)
- Has working exploit developed
- Scans internet for all possible victims
- Compromises systems, then identifies valuable data
  - Stored data = low hanging fruit
  - No stored data = In-transit attacks
- Repeat until no longer cost effective

The Reality – Targeted Attacks

- Attacker profiles target & Identifies employees
- Sends targeted malware to employees
- Begins monitoring employee activity
- Captures login credentials to systems
- Quiet, careful, cautious

The Reality – Ecommerce stored data

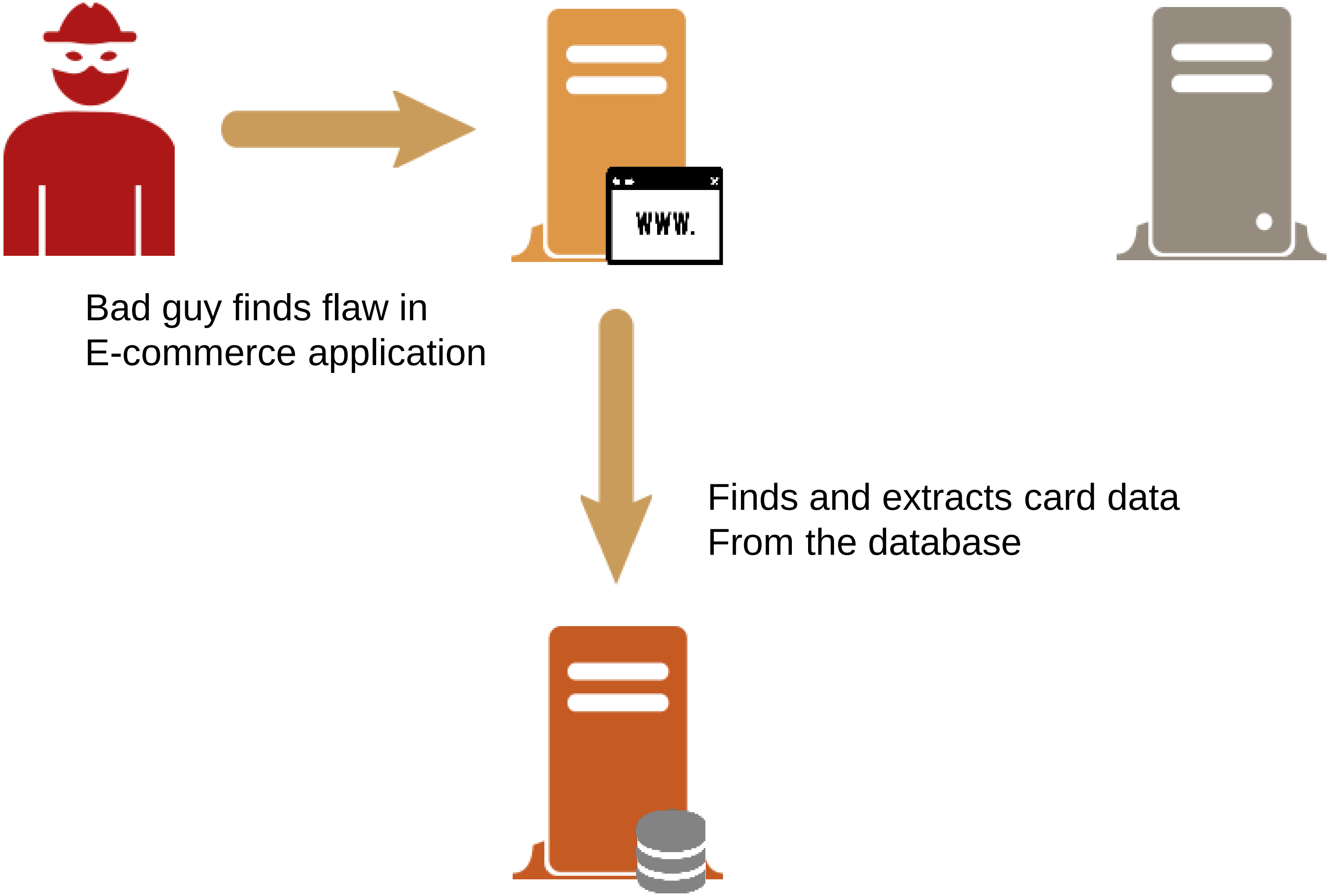


Legitimate user enters card data

Card data sent to Acquiring bank

Card data also saved into database

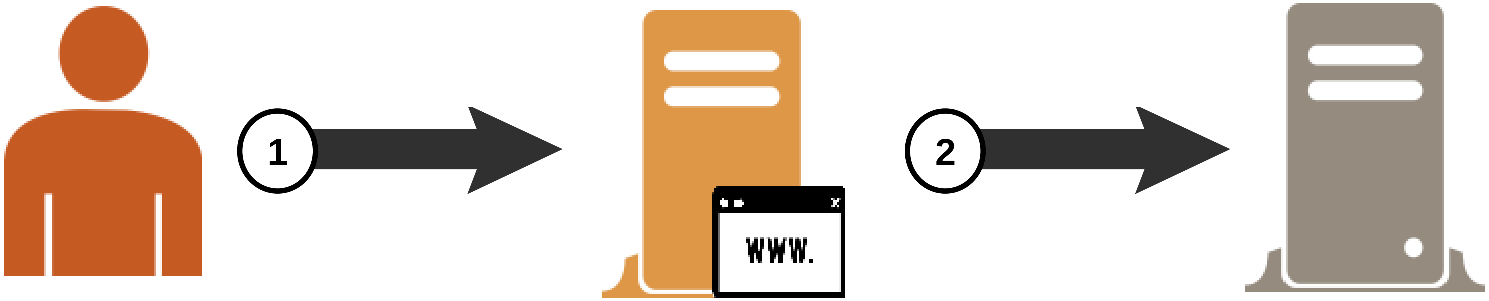
The Reality – Ecommerce stored data



Bad guy finds flaw in
E-commerce application

Finds and extracts card data
From the database

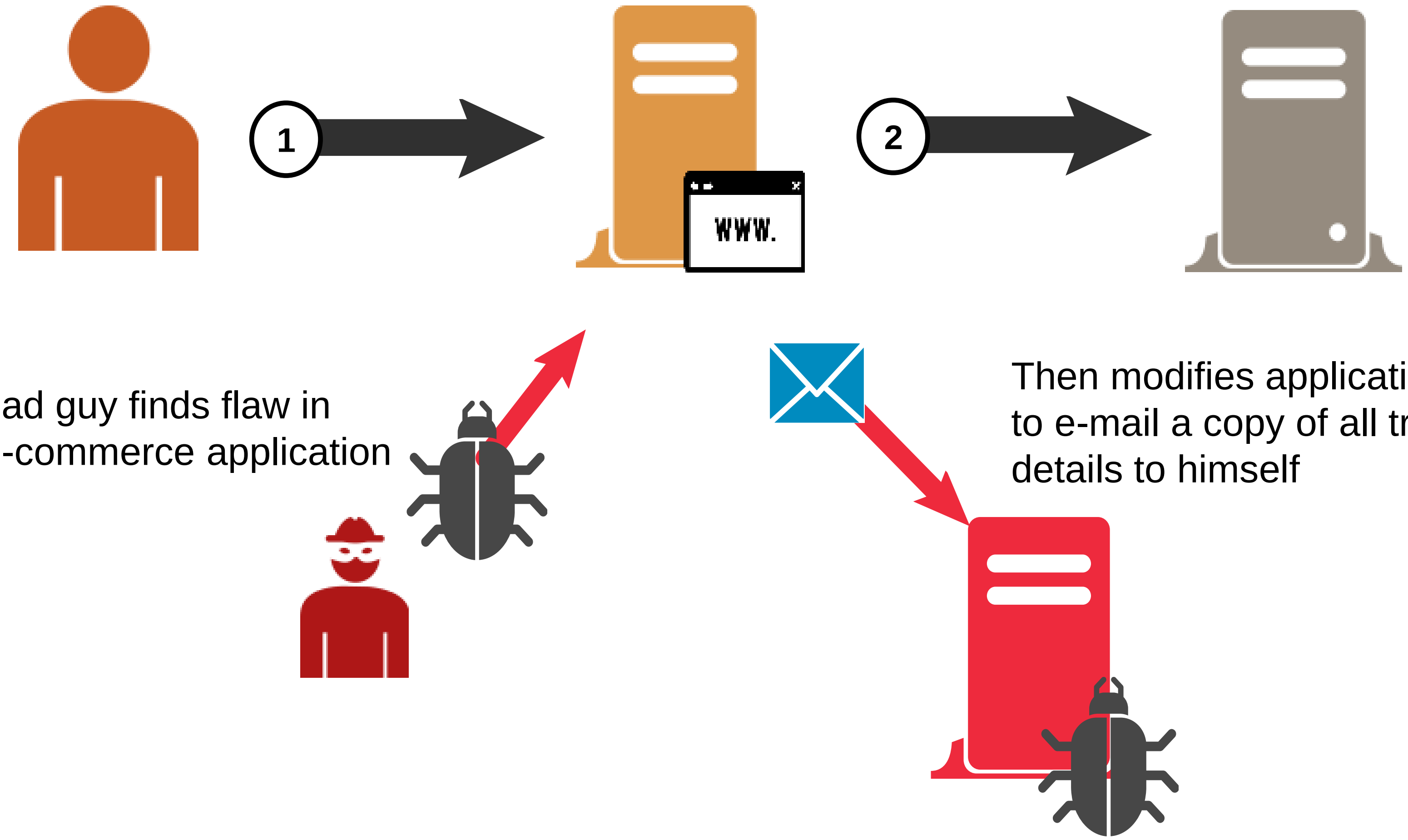
The Reality – Ecommerce in-transit data



Legitimate user enters card data

Card data sent to Acquiring bank

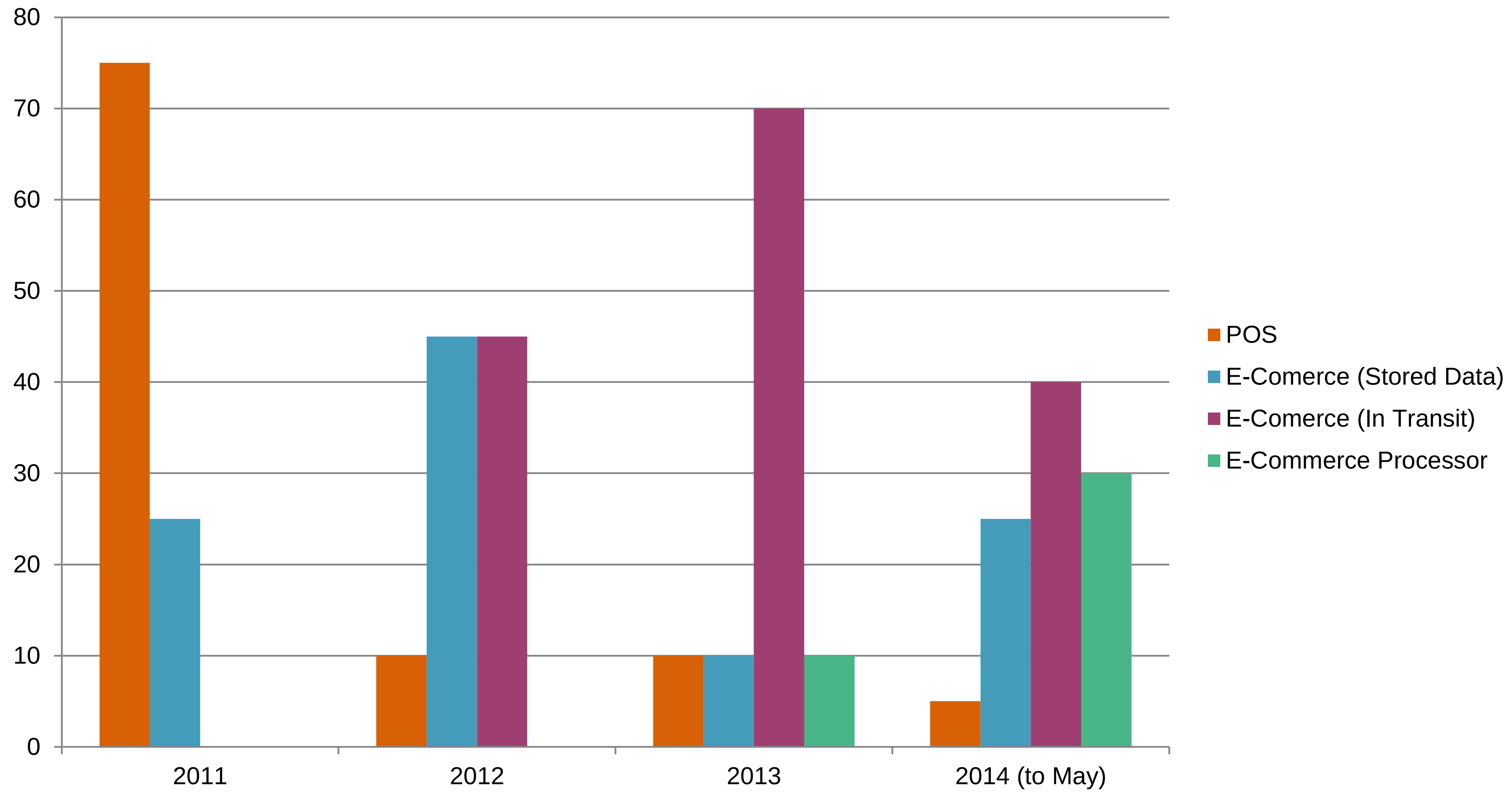
The Reality – Ecommerce in-transit data



Bad guy finds flaw in E-commerce application

Then modifies application to e-mail a copy of all transaction details to himself

Hacker Profiles – Trends



Source: 2014 Trustwave Global Security Report 2014

The Reality – We can be better at this!

MasterCard

BY COUNT

Password1	38.7%
password	34.5%
Welcome1	16.0%
123456	12.6%
P@ssw0rd	11.8%
Passw0rd	10.9%
Password123	10.9%
Password2	10.1%
Summer12	10.1%
password1	10.1%

12345678	9.2%
Welcome2	7.6%
Spring2012	6.7%
Summer2012	6.7%
Password3	6.7%
Hello123	5.9%
Welcome3	5.9%
Fall2012	5.9%
Spring12	5.9%
pa$$w0rd	5.9%
p@ssw0rd	5.9%
p@ssword	5.0%
p@ssword1	5.0%
Summer11	5.0%
password9	5.0%

Source: 2014 Trustwave Global Security Report 2014

Best Practices & Strategies

Do your homework!

✓Firewalls and antivirus software = effective defense

✓Review/replace EOL security devices and apps

✓Maintain patch levels on infrastructure and applications.

✓Protect and defend your “crown jewels” – Your Data!

✓Understand “cloud” risks

✓Incident Management Process is very important

Best Practices & Strategies

Continuous Monitoring

✓Do you know what is happening on your network 24x7?

✓Are privileged users monitored?

✓Who/what is coming in/going out of the network?

✓Are ex-employees still active on your network?

✓Monitor in accordance with policies and applicable laws

Best Practices & Strategies

Manage Vendor / Outsourcing Risk

✓Know your vendors and their capabilities.

✓Are they able to support your PCI-DSS compliance efforts?

✓Do they further outsource the work?

✓**Accountability cannot be outsourced!**

Best Practices & Strategies

Validate Your Internal Controls

✓Regular audit of:

- Access controls,
- System configurations
- Device settings

✓Will help identify internal weaknesses, unauthorized changes, threats or detect signs of intrusions

Best Practices & Strategies

Do not brag, be humble!

✓Do not “advertise” yourself on the news or social media

✓Beware of unintentional “leaks” via social media

✓Monitor “underground” chat rooms (if you can)

✓Learn from the mistakes made by the others

Welland Chu, Regional Sales Director,Thales

David Chan, Group Head, SEA Market Development, MasterCard

Simplifying Mobile NFC Payments

Lessons learned from security assessment

Objectives & Results

By the end of the session, you will:

- Understand the ecosystem of NFC-Mobile payment
- Appreciate the security issues being faced by your users
- Benefit from lessons learned

What is NFC

Near Field Communications (NFC)

- **Allows exchange of data wirelessly**
- **Requires close contact between devices (< 4cm)**
- **Very common in our daily lives :**

Works like an Touch n’ Go cards

Sharing information (eg. photos) with other NFC devices; and

Reader/Writer to another device

What is NFC-Mobile Payment

Combination of

- NFC technologies
- Mobile communications
- Payment cards

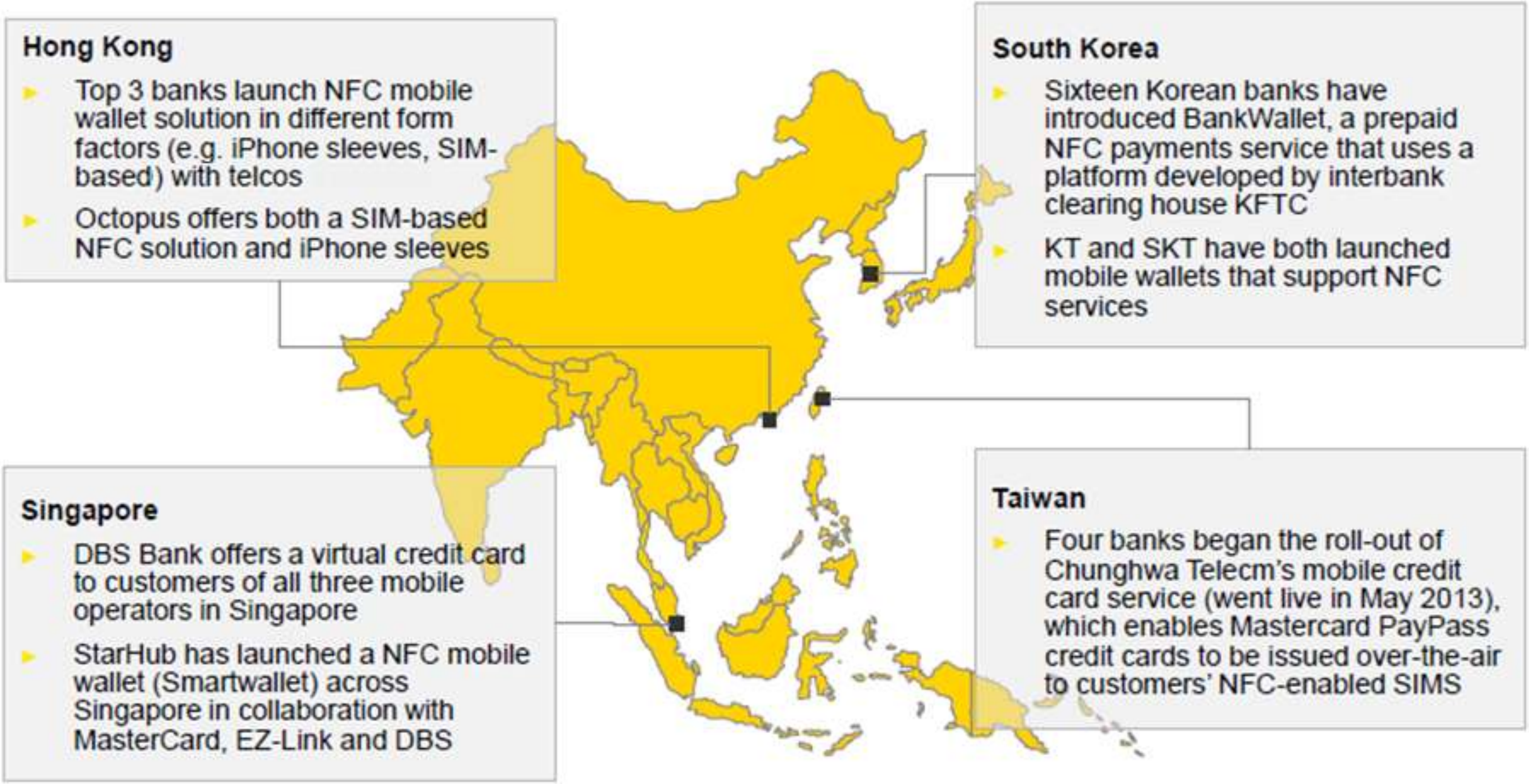
Allows more benefits, such as

- Consumers have options to check available balances, discounts, and other incentives
- Merchants may benefit from geolocation functionality of customers’ smart phones
- Credit card issuers save on cost by not issuing plastic cards

Bigger sales; Higher profitability

Mobile Market Analysis

- The Market



Hong Kong

- Top 3 banks launch NFC mobile wallet solution in different form factors (e.g. iPhone sleeves, SIM-based) with telcos
- Octopus offers both a SIM-based NFC solution and iPhone sleeves

South Korea

- Sixteen Korean banks have introduced BankWallet, a prepaid NFC payments service that uses a platform developed by interbank clearing house KFTC
- KT and SKT have both launched mobile wallets that support NFC services

Singapore

- DBS Bank offers a virtual credit card to customers of all three mobile operators in Singapore
- StarHub has launched a NFC mobile wallet (Smartwallet) across Singapore in collaboration with MasterCard, EZ-Link and DBS

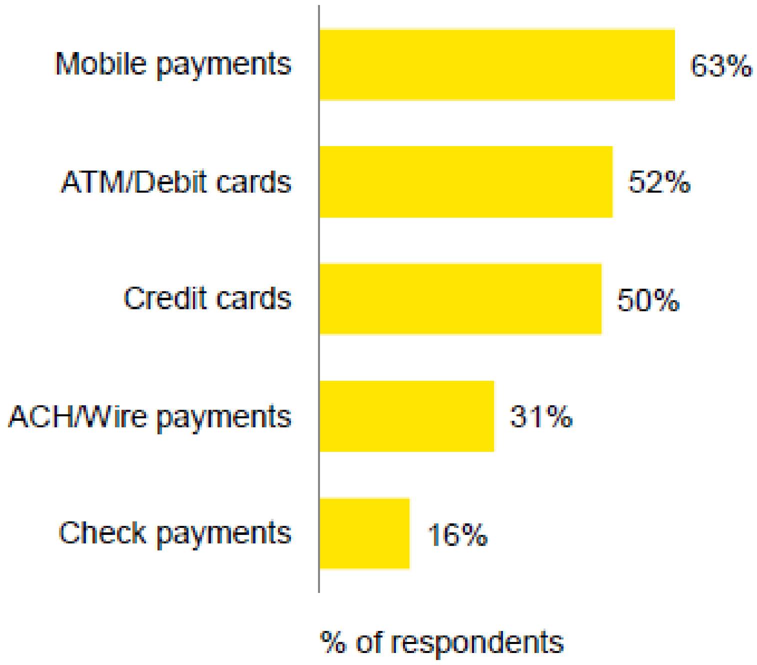
Taiwan

- Four banks began the roll-out of Chunghwa Telecm's mobile credit card service (went live in May 2013), which enables Mastercard PayPass credit cards to be issued over-the-air to customers' NFC-enabled SIMS

Source: GSMA Mobile Commerce

Growth on Mobile Payment

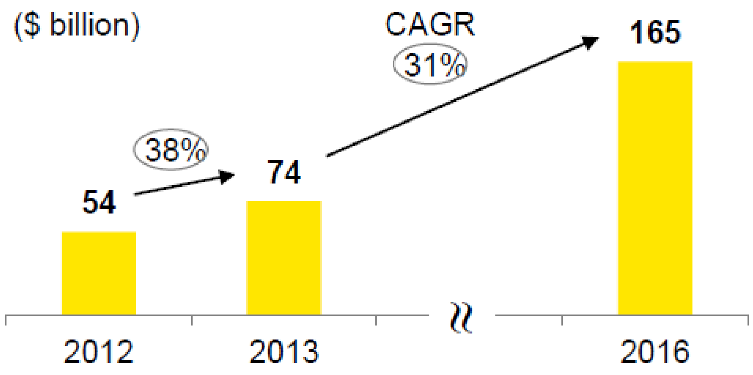
Asian banks' planned payment investment in next 12-18 months



Ovum, 'The strategic implications of mobile on the payments market', Sep 2013

US$165B = 53% of Malaysia GDP (US$312B)

NFC transaction value in Asia-Pacific

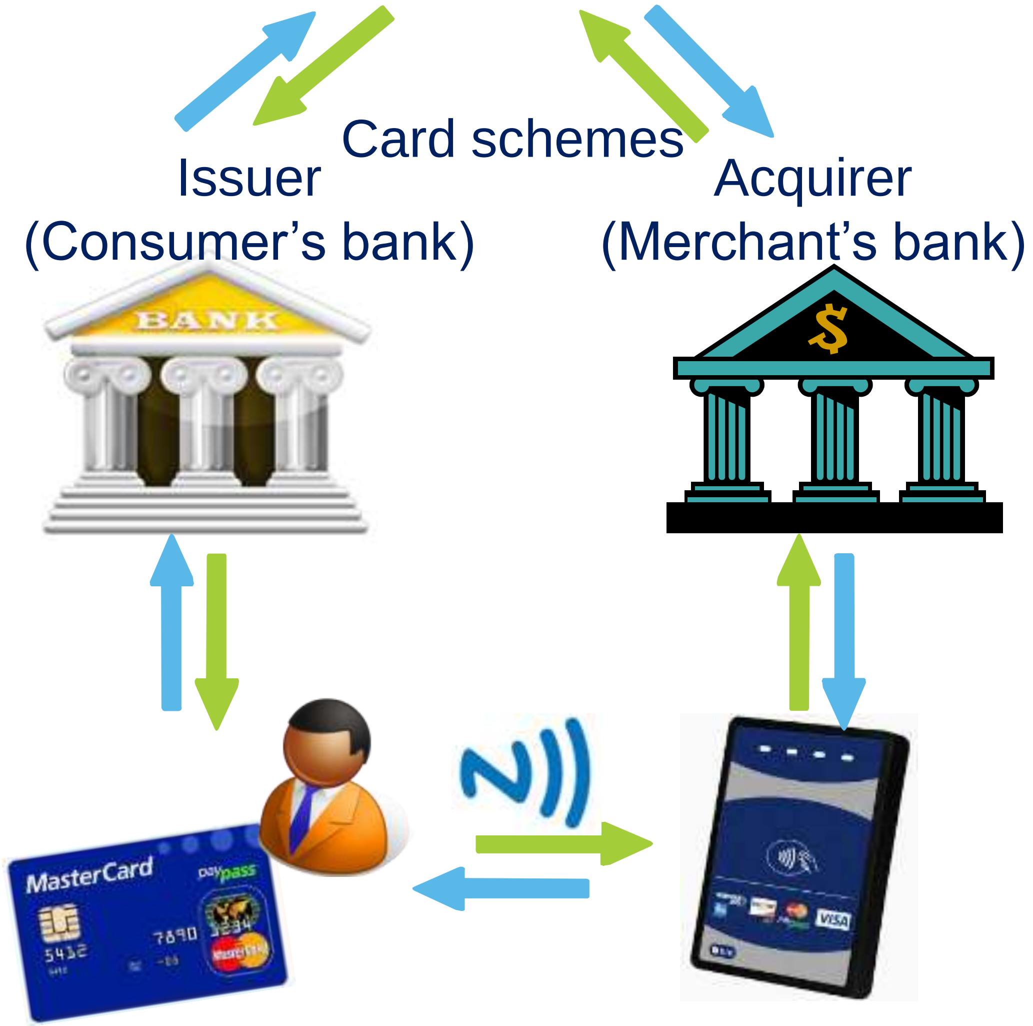


Gartner press release June 4, 2013:
'AP mobile payment transaction value in 2013 will grow by more than 100% and reach US$165 billion in 2016'

Contactless Payment

- Security risks controlled under card schemes' standards, etc
- Subject to PCI Security Standards Council regulations
- Both local & international usage

- **Four-party model**
- Consumer receives credit from issuer
- Merchant receives payment through acquirer



Card schemes

Issuer (Consumer's bank)

Acquirer (Merchant's bank)

Consumer

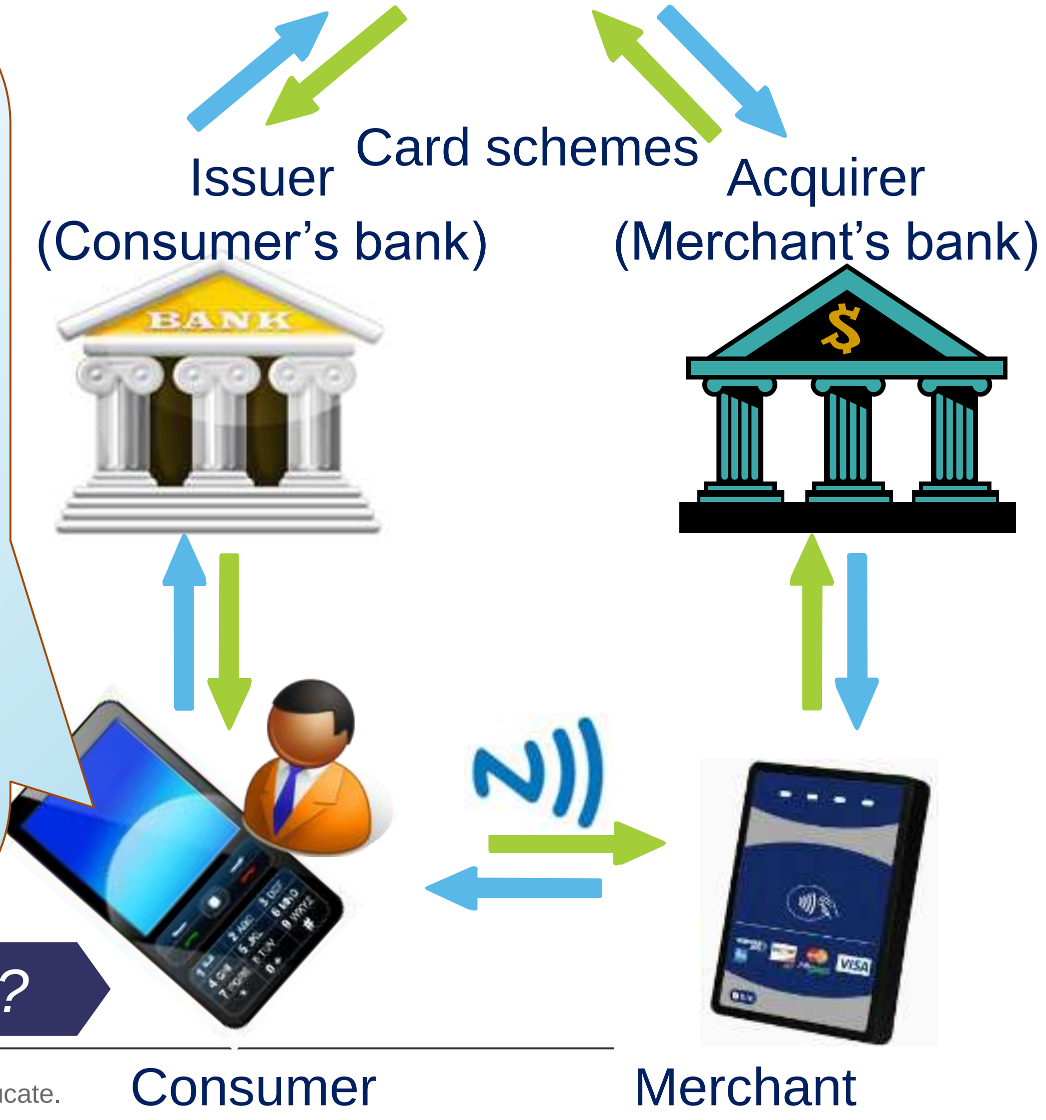
Merchant

Comparison with NFC Mobile Payment

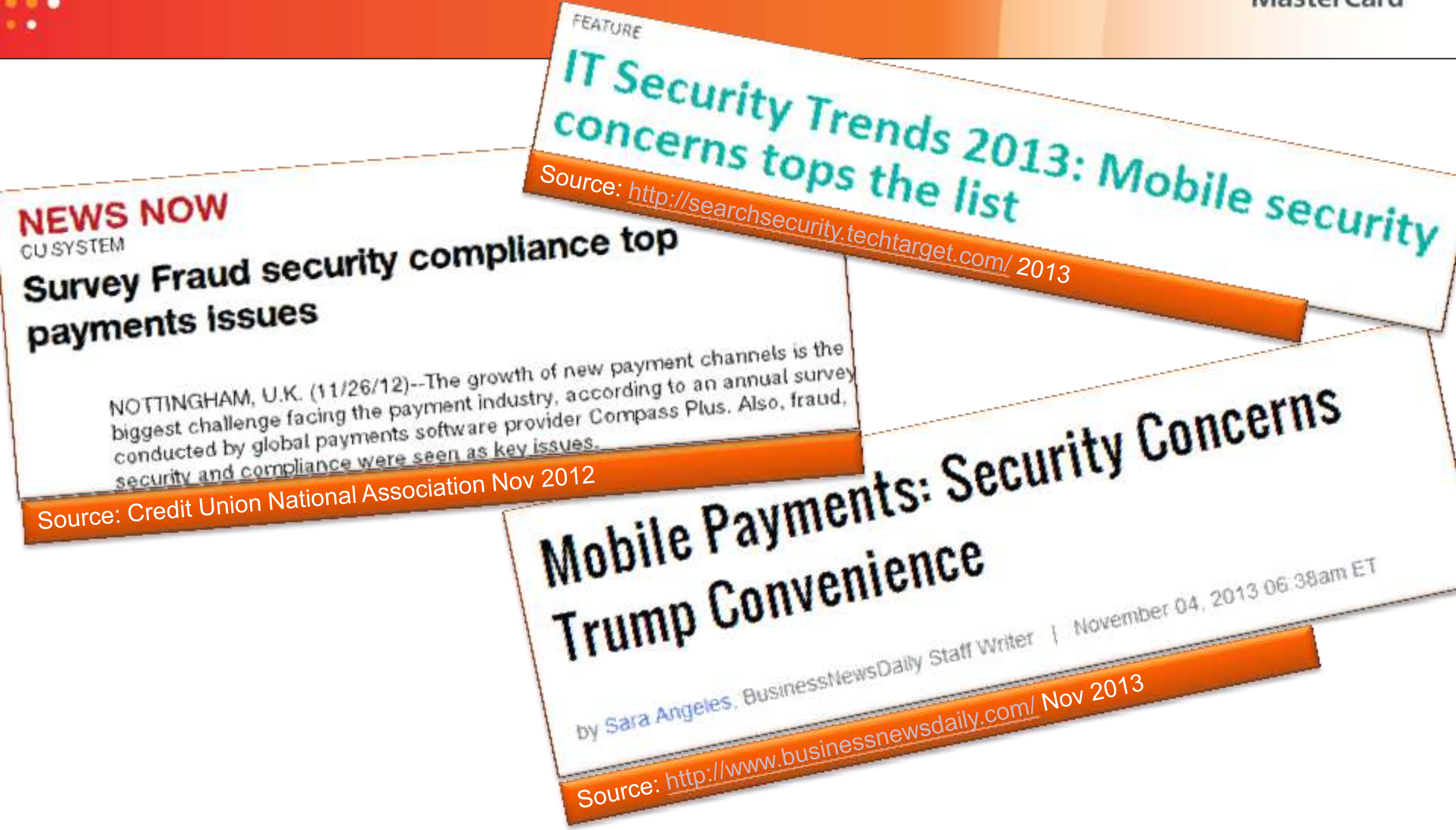
Everything stays almost the same as PayPass, but…

- Phones are insecure
- Consumer’s bank does not have control over the phone
- The sensitive credit card data are not pre-installed, as is done with traditional credit cards
- Sensitive data is downloaded over the air (OTA)

What is the greatest concern ?



Security: Consumers' Biggest Concern



FEATURE

IT Security Trends 2013: Mobile security concerns tops the list

Source: http://searchsecurity.techtarget.com/ 2013

NEWS NOW

CU SYSTEM

Survey Fraud security compliance top payments issues

NOTTINGHAM, U.K. (11/26/12)--The growth of new payment channels is the biggest challenge facing the payment industry, according to an annual survey conducted by global payments software provider Compass Plus. Also, fraud, security and compliance were seen as key issues.

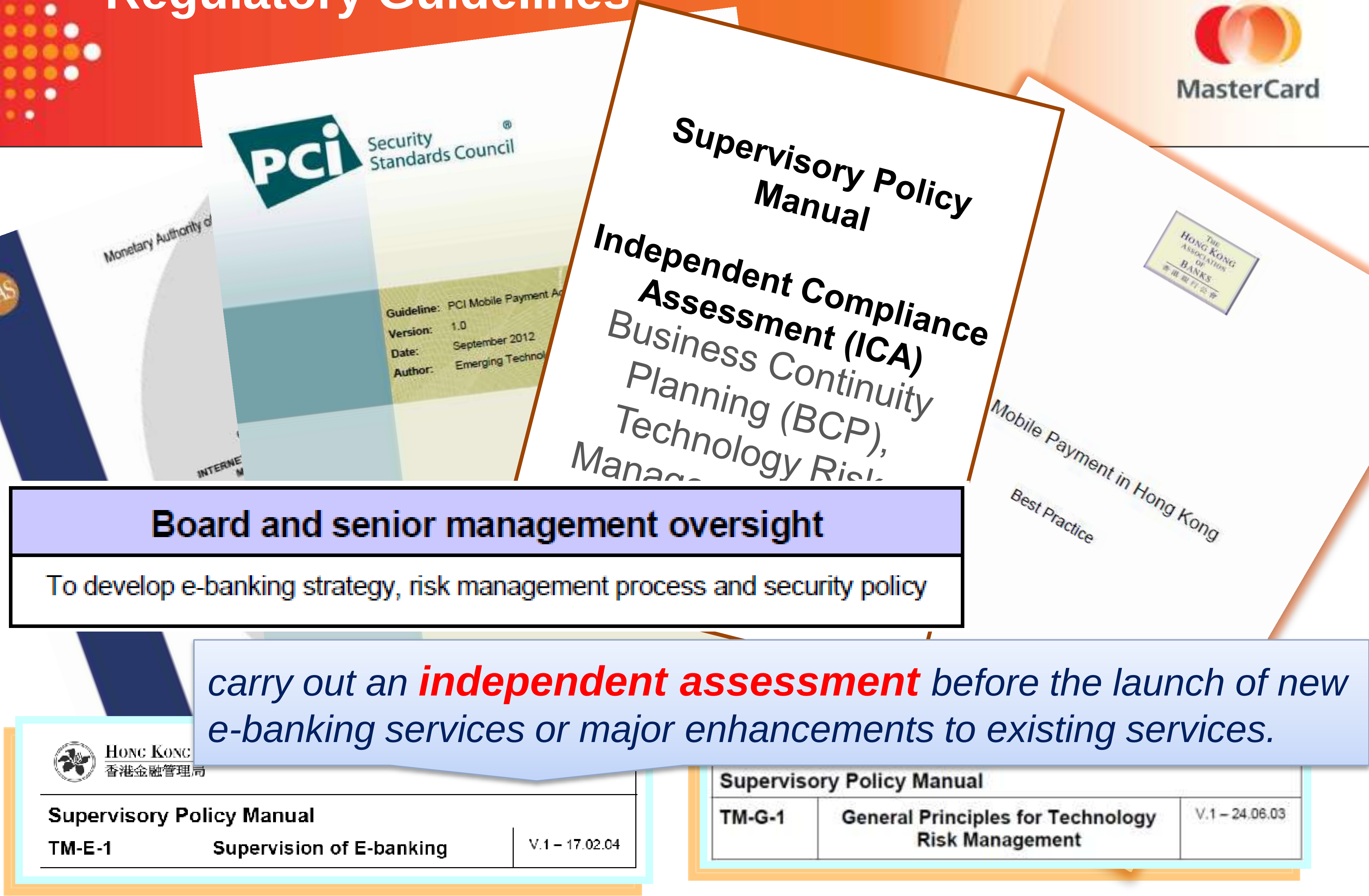
Source: Credit Union National Association Nov 2012

Mobile Payments: Security Concerns Trump Convenience

by Sara Angeles, BusinessNewsDaily Staff Writer | November 04, 2013 06:38am ET

Source: http://www.businessnewsdaily.com/ Nov 2013

Regulatory Guidelines



Monetary Authority of

INTERNE
M

PCI Security Standards Council®

Guideline:	PCI Mobile Payment Ac
Version:	1.0
Date:	September 2012
Author:	Emerging Technol

Supervisory Policy Manual

Independent Compliance Assessment (ICA)

Business Continuity Planning (BCP), Technology Risk Manag

The Hong Kong Association of Banks 香港銀行公會

Mobile Payment in Hong Kong

Best Practice

Hong Kong
香港金融管理局

Supervisory Policy Manual		
TM-E-1	Supervision of E-banking	V.1 – 17.02.04

Supervisory Policy Manual		
TM-G-1	General Principles for Technology Risk Management	V.1 – 24.06.03

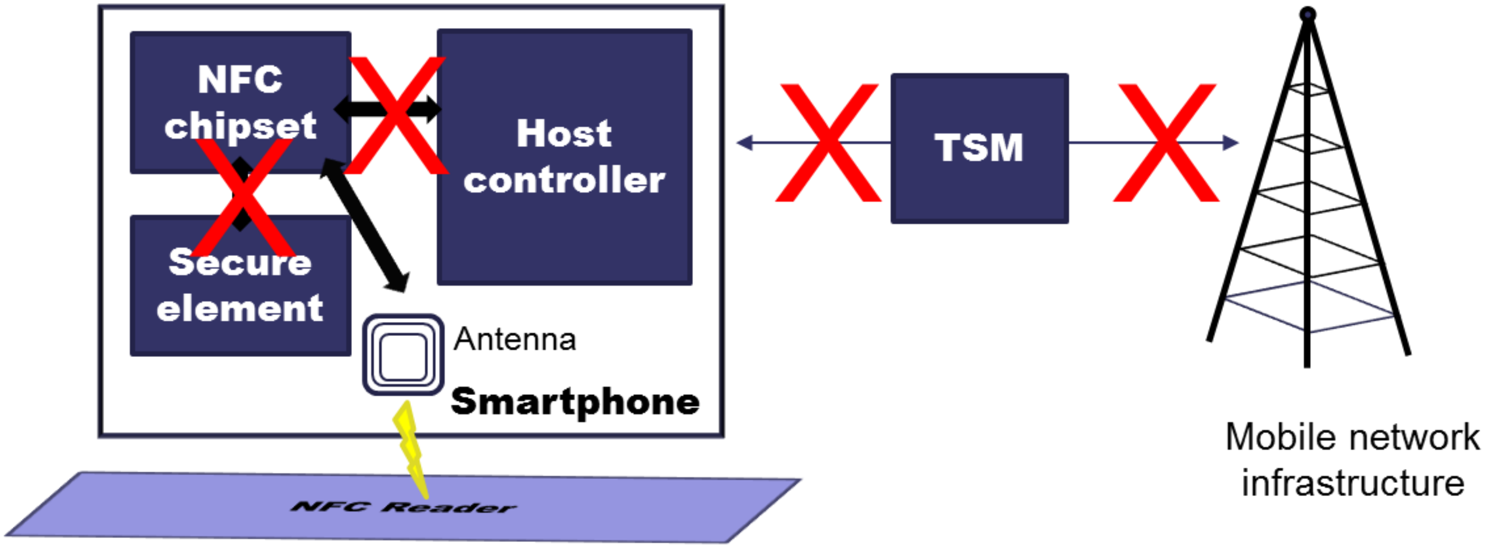
Board and senior management oversight

To develop e-banking strategy, risk management process and security policy

carry out an ***independent assessment*** *before the launch of new e-banking services or major enhancements to existing services.*

Source: Hong Kong Association of Banks, Hong Kong Monetary Authority, Monetary Authority of Singapore, PCI Security Standards Council

NFC Threat Scenarios and Modeling



Hardware, Software, Platforms and their Interfaces

- Attack by disturbances (faults)
- Attack by side channels
- Attain certification to meet EMVCo and Common Criteria standards

Users and Service Providers

- Data protection in transit, in use and at rest
- Malware
- Social engineering, trojans, phishing
- Theft and loss of devices
- Weak security controls , eg. no PIN lock

Lesson Learned (1): Mobile Device Strategy

Assured data in transit protection

Assured data at rest protection

Platform integrity and application sandboxing

Incident response

Authentication

1. user to device
2. user to service
3. device to service

Secure boot

Application whitelisting

Device update policy

External interface protection

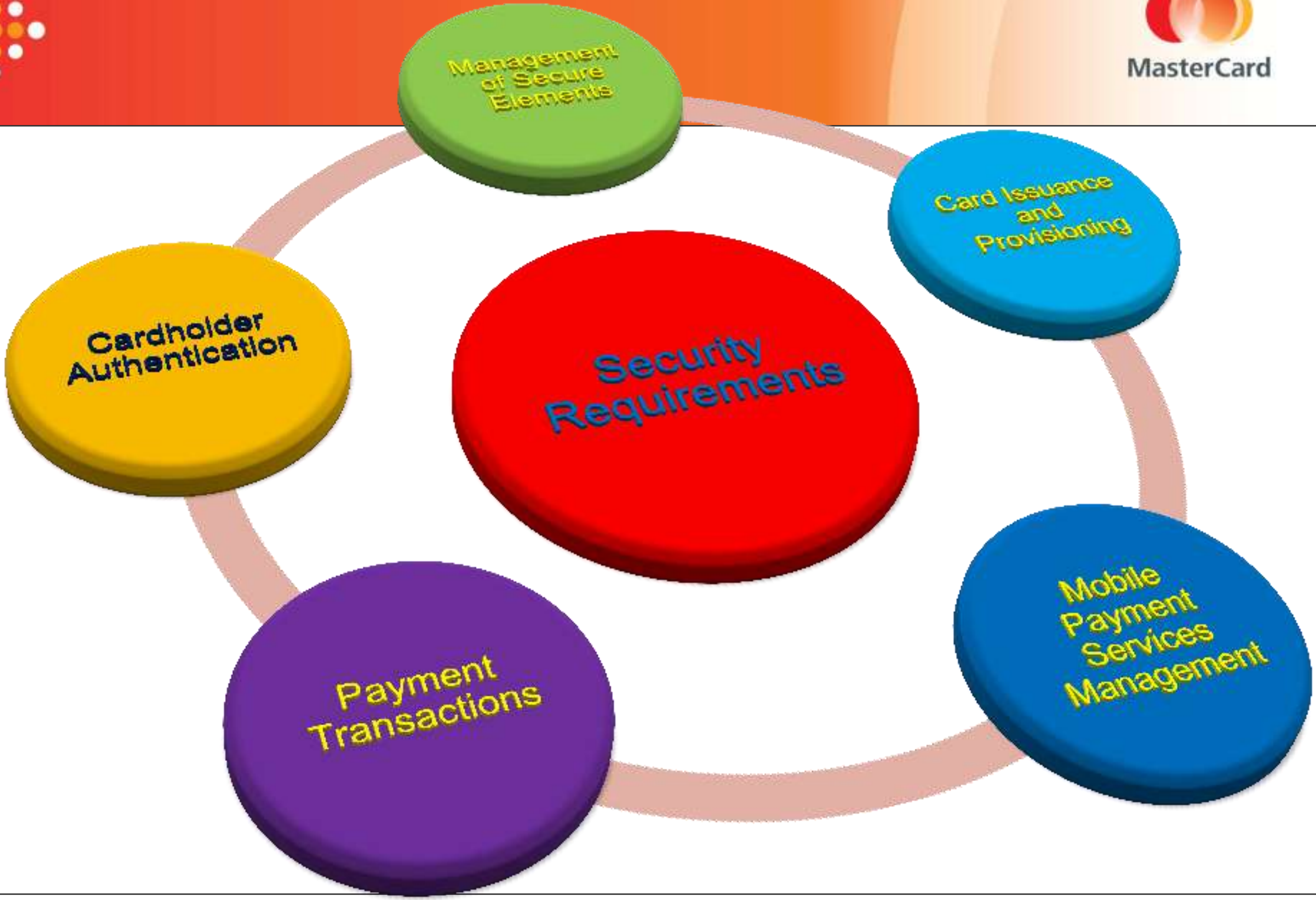
Malicious code detection and prevention

Security policy enforcement

Event collection for enterprise analysis

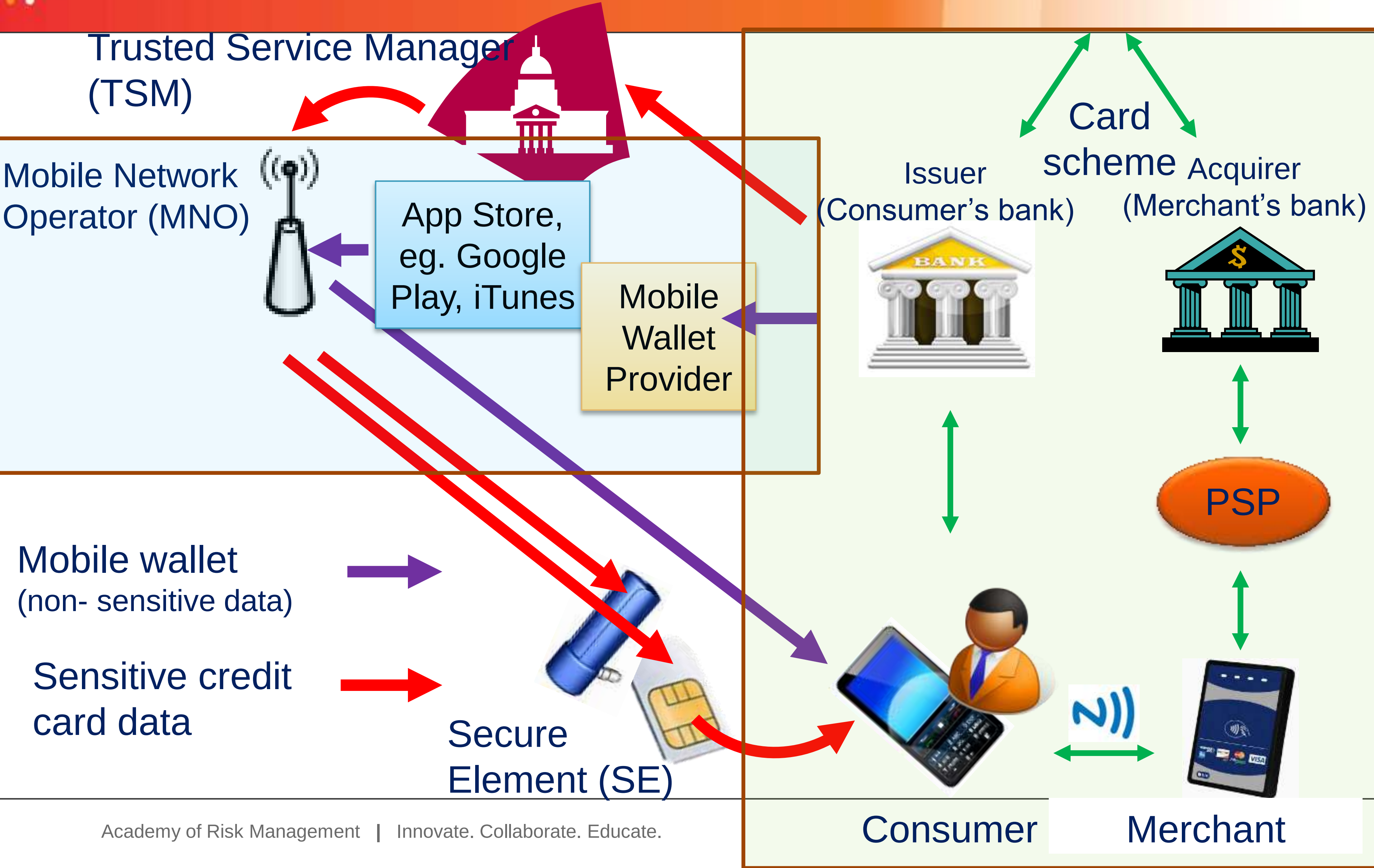
Source: UK CESG 2013

Lesson Learned (2): NFC Security Requirements


Management of Secure Elements
Card Issuance and Provisioning
Cardholder Authentication
Security Requirements
Mobile Payment Services Management
Payment Transactions

Source: Hong Kong Association of Banks 2013

Lesson Learnt (3): Mobile Security Assessment



Trusted Service Manager (TSM)

Mobile Network Operator (MNO)

App Store, eg. Google Play, iTunes

Mobile Wallet Provider

Card scheme

Issuer (Consumer's bank)

Acquirer (Merchant's bank)

PSP

Mobile wallet (non- sensitive data)

Sensitive credit card data

Secure Element (SE)

Consumer

Merchant

Lesson Learned (4): Security Review for TSM

Customer requests

- A security review on the infrastructure and operation of the TSM that covers
  - Card personalization preparation process
  - Credential data downloading through over-the-air (OTA)
  - Mobile card life cycle management
  - Mobile wallet

Assessment approach and response

- TSM is provided with findings and practical recommendations
- Examine whether sufficient controls are in place to meet the security requirements as laid out by the local monetary authority and association of banks

Benefits

- Obtain an assurance that the TSM is secure in protecting sensitive customer data

The TSM is a first in North Asia that incorporates multi-modal secure elements (the SE can exist in dongle, SIM card, SD card, embedded in phone) and multi-wallets (different banks will join the same scheme)

Lesson Learned (5): Security Review for Mobile Payment Card Issuer

MasterCard

Customer requests

- Security review covering the confidentiality, integrity and availability of customer sensitive data within the mobile wallet and IT infrastructure
- Vulnerability assessment on internet-facing servers and internal IT

Bank

Assessment approach and response

- Security review that include context analysis, technical assessment and interviews
- The final report is written in a format that conforms to the guidelines of regulatory bodies

Benefits

- Meeting the compliance requirements of regulatory bodies
- Getting an assurance that the mobile wallet and the bank’s IT infrastructure is secure in protecting sensitive customer data

Sample Security Risk Assessment Report

THALES

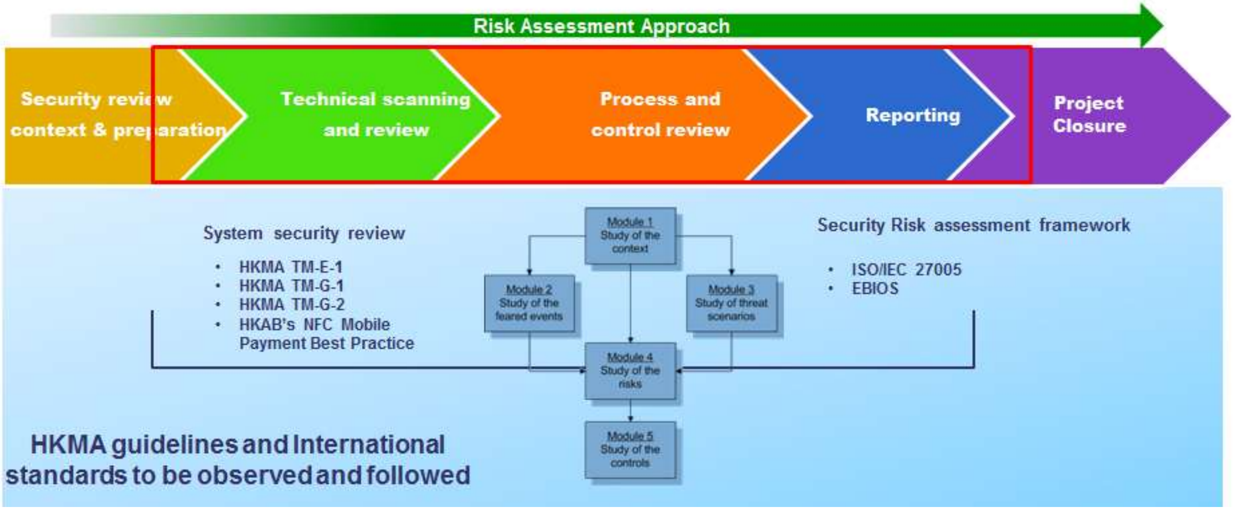
MOBILE PAYMENT SERVICE
SECURITY REVIEW
FINAL REPORT – ADDENDUM

MOBILE PAYMENT SERVICE LTD.
JUNE 2014

CONFIDENTIAL DOCUMENT

Reference	Mobile Payment Service Security Review Report

This document is classified as confidential. It contains significant information related to th
& Security (Hong Kong) Ltd.



Risk Assessment Approach

Security review context & preparation → Technical scanning and review → Process and control review → Reporting → Project Closure

System security review

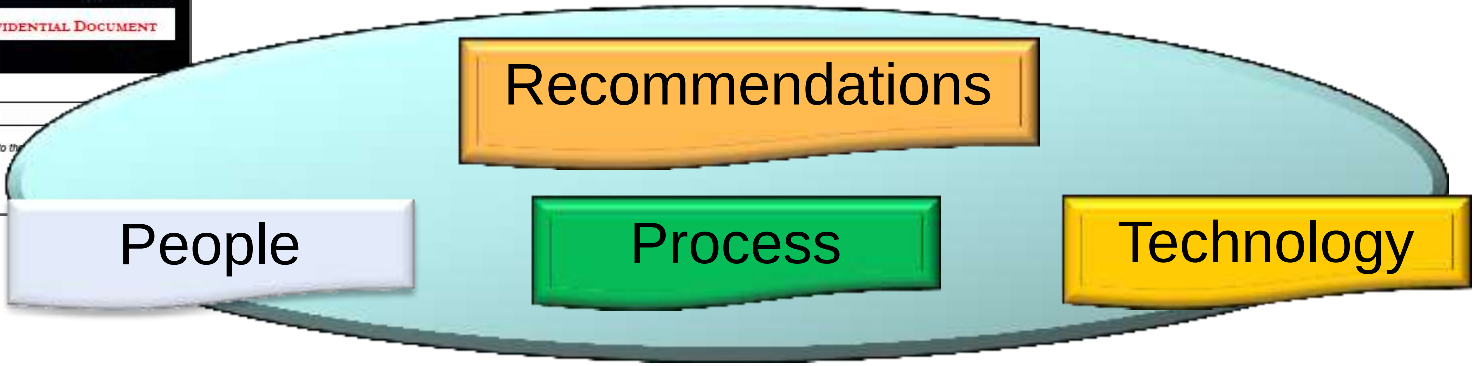
- HKMA TM-E-1
- HKMA TM-G-1
- HKMA TM-G-2
- HKAB's NFC Mobile Payment Best Practice

Module 1 Study of the context
Module 2 Study of the feared events
Module 3 Study of threat scenarios
Module 4 Study of the risks
Module 5 Study of the controls

Security Risk assessment framework

- ISO/IEC 27005
- EBIOS

HKMA guidelines and International standards to be observed and followed



Practical recommendations to help clients prioritize in fixing vulnerabilities and achieving compliance most effectively !

Thank You

THALES

Welland Chu
Welland.Chu@thales-esecurity.com

Tel : +852-28158633

David Chan
Group Head, SEA Market Development
MasterCard

Simplifying Mobile NFC Payments

Using MasterCard Cloud Based Payment (MCBP) and MasterCard Digital Enablement Service (MDES)

Consumers are increasingly using their smart mobile devices for shopping

MasterCard

USD $235B

Estimated payments
via mobile devices
in **2013**[1]

USD $721B

Projected payments
via mobile devices
by **2017**[1]

22%

Consumers would like to use their phones to buy things at the point of sale[2]

Number of mobile contactless transactions by 2018[3]

10,000,000,000

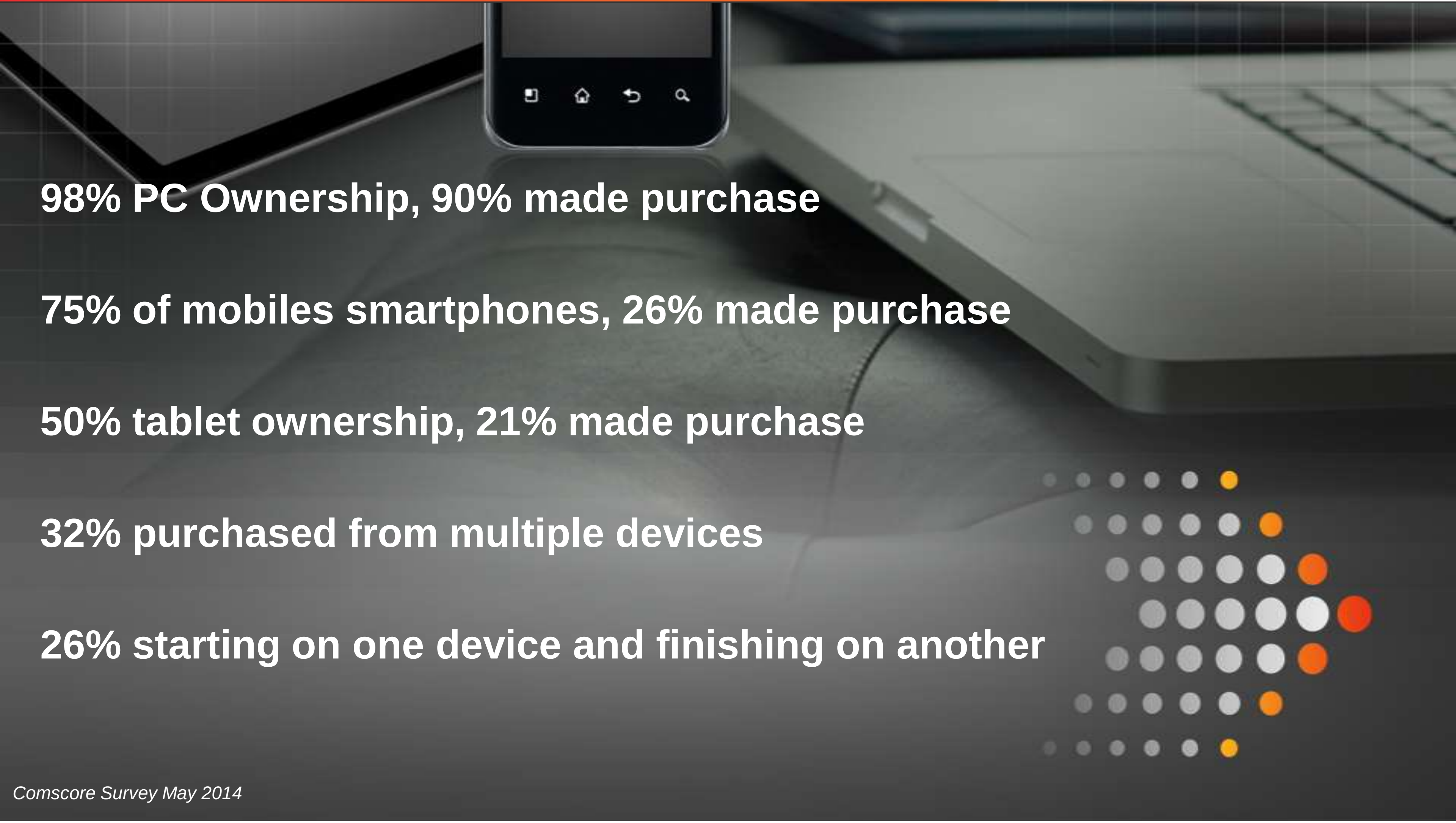
[1] Gartner, Inc., "Gartner Says Worldwide Mobile Payment Transaction Value to Surpass $235 Billion in 2013," June 2013.

[2] Board of Governors of the Federal Reserve System, "Consumers and Mobile Financial Services 2013," March 2013.

[3] Juniper Research

Proliferation of smart devices is helping to drive this change in consumer behavior

MasterCard



98% PC Ownership, 90% made purchase

75% of mobiles smartphones, 26% made purchase

50% tablet ownership, 21% made purchase

32% purchased from multiple devices

26% starting on one device and finishing on another

Comscore Survey May 2014

MasterCard's digital vision is to enable richer shopping experiences

MasterCard

Issuer

A streamlined payment experience, both online and in-store, that brings global acceptance, security and simplicity across all channels and devices

Consumer

A richer shopping experience that is accessible across all channels, more secure, and provides access to more benefits than traditional methods and from my main bank

Merchant

A seamless 'omni-channel' commerce experience providing a better retail experience for consumers and generating increased sales

… by integrating a number of products and platforms to deliver…

Safe, Simple and Smart payments

- **MasterPass** delivers the wallet and merchant acceptance framework
- **Digital Secure Remote Payment (DSRP)** provides the mechanism to secure remote payments using EMV based cryptography
- **MasterCard Cloud-Based Payment (MCBP)** provides a mechanism for enabling contactless and DSRP transactions without a hardware Secure Element in the mobile device
- **MasterCard Digital Enablement Service (MDES)** provides issuer on-boarding and tokenization services

How MCBP and MDES will simplify Mobile NFC payments

Success in Mobile NFC payments requires us to do 3 things well

1

Contactless Acceptance

2

Scale Participation & Reduction in Costs

- More Issuers
- More Devices

3

Consumer & Merchant Education

Successful contactless payments are paving the way for Mobile NFC payments

Contactless has helped drive cashless payments in Australia

Proliferation of Contactless Cards

66% consumers have a contactless card

Greater Usage

~50% F2F debit transactions are contactless

Proliferation of Smartphones

76% consumers have a smartphone

Setting the stage for Mobile NFC

$3B in contactless mobile payments forecast for 2015

Sources: WestPac Bank Australia, MasterCard, Statistica.com

But existing Mobile NFC payment programs have a number of pain points

… Issuer & Mobile Network Operator effort, lead time and costs

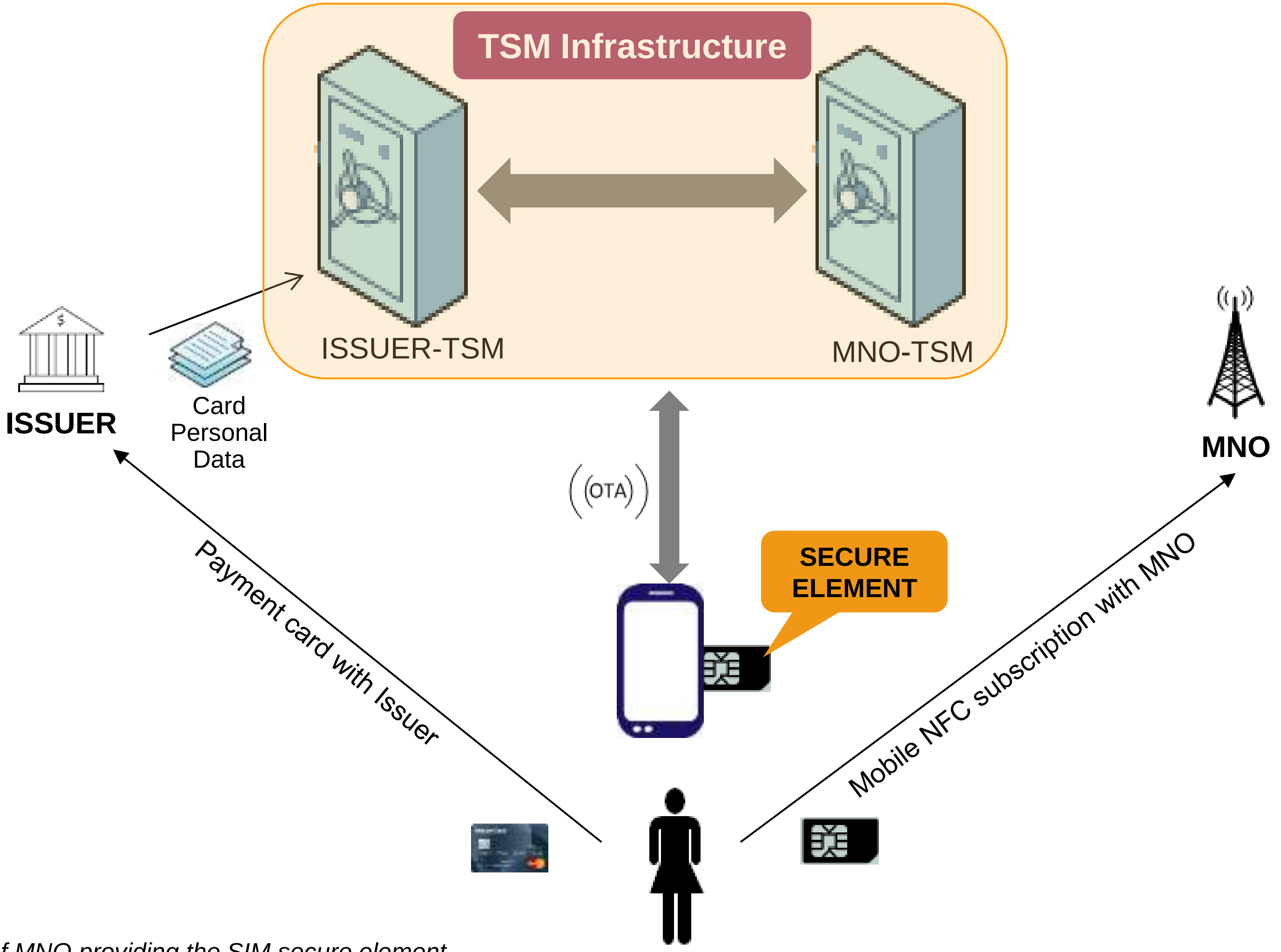


Illustration of MNO providing the SIM secure element

Faster Mobile NFC deployment and lower costs with MCBP and MDES

- **MCBP** for Mobile NFC payments leverages HCE specifications that do not require a secure element (SIM or Embedded SE) or associated TSM

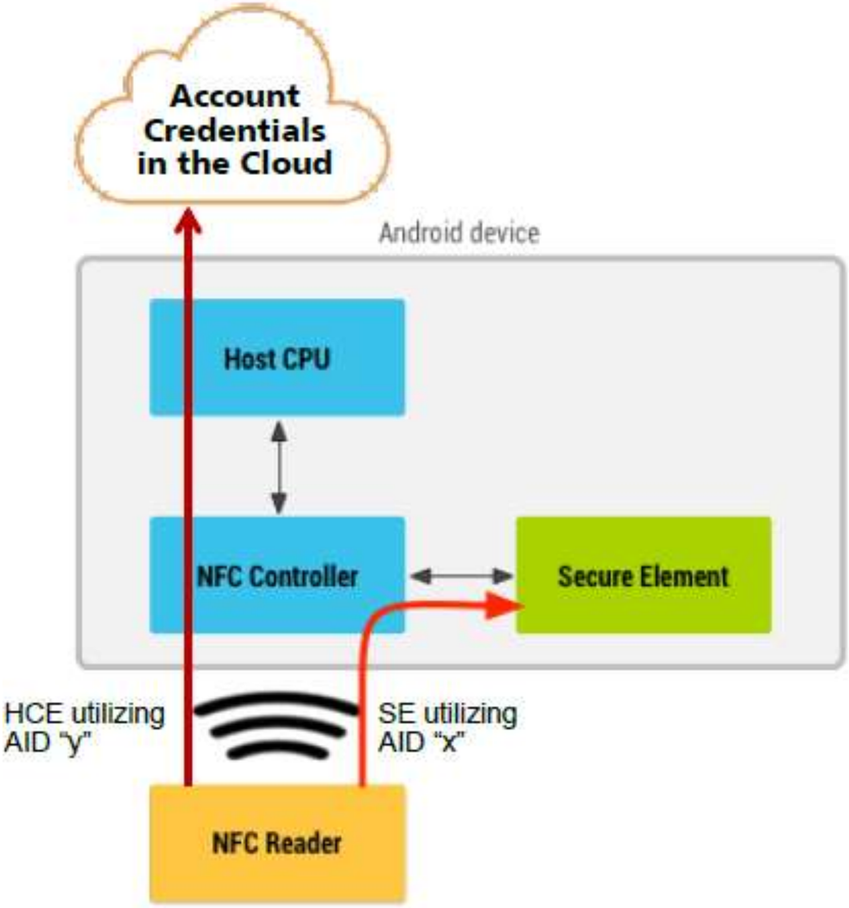
- **MDES** provides Tokenization and Digitization service and removes need for issuer TSM

MCBP leverages HCE specifications to enable Mobile NFC payments

MasterCard

HCE is a specification for contactless transactions performed on a device without using a Secure Element (SE)

- Implemented in Android v4.4 or above
- Contactless payments are now enabled using credentials stored on the SE or in the cloud via HCE
- Reduces go-to-market complexity and costs for mobile NFC payments. SE and TSM no longer required



MDES

Tokenization

And

Digitization

Tokenization

Tokenization is the replacement of the card primary account number (PAN) with an alternative card number that is used in a mobile or digital device.

MasterCard tokenization secures consumer account credentials

In the cloud

Or

From a device

Digitization

Digitization is the loading and personalization of card details into mobile devices or onto servers enabling simpler and more secure payments

MasterCard digitization enables simpler payment experiences

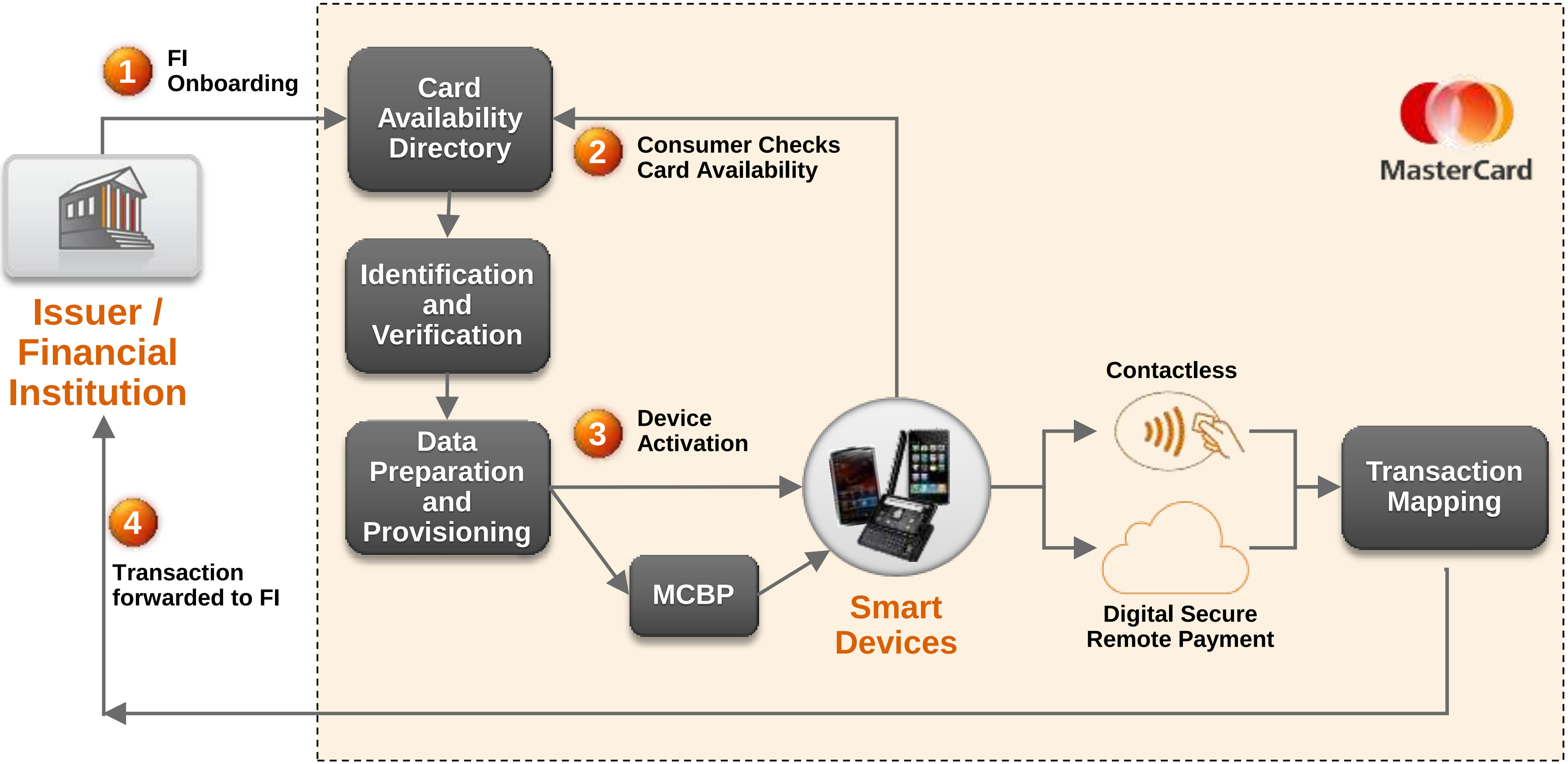
On the web

Or

From a device

MCBP and MDES will together address a number of Mobile NFC pain points

- **MDES tokenizes card credentials and digitizes / provisions the tokens onto devices for Mobile NFC payments**


1
FI Onboarding
Card Availability Directory
2
Consumer Checks Card Availability
MasterCard
Issuer / Financial Institution
Identification and Verification
3
Device Activation
Data Preparation and Provisioning
MCBP
Smart Devices
Contactless
Digital Secure Remote Payment
Transaction Mapping
4
Transaction forwarded to FI

Derek Ho
Senior Counsel, Privacy & Data Protection, APMEA
MasterCard

The Evolving Privacy Landscape in Asia

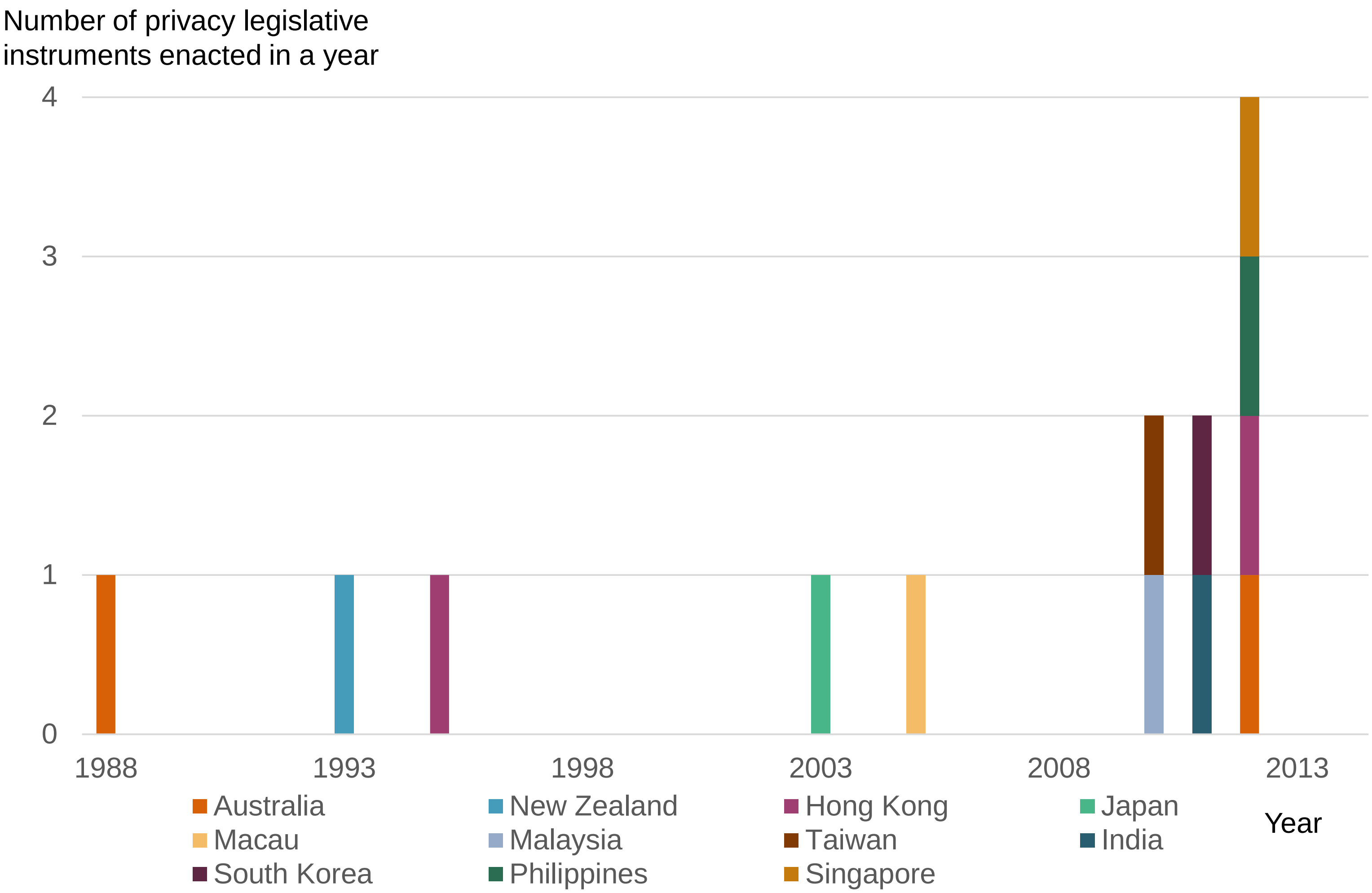
An Update on Recent Changes in Privacy Regulations

Introduction

Overview of changes in the privacy landscape

Some key themes driving change

Overview of AP Privacy Laws



On the cards

Japan

New Zealand

Australia (breach notification)

India (omnibus)?

Thailand (omnibus)?

Overview of AP Privacy Laws

- No unified privacy and data protection law across AP countries
- Each country has its own privacy and data protection regime (some omnibus, some sector specific)
- Privacy law evolving at different speeds in different countries

The Data Economy

The Data Economy

MasterCard & Syniverse
Secure Experience **for Mobile Consumers**

75 million mobile phone users travel outside their home country each month[1], yet today **70 percent** of people switch off their mobile data when they arrive[1], disconnecting them from all the **convenient benefits** that mobile provides – including the ability to safely and **securely shop on the go**.

2 Nearly BILLION payment cards in circulation

Processing 65,000 TRANSACTIONS EVERY MINUTE

MasterCard

5 Reaching more than BILLION mobile devices globally via...

...relationships with 1,000 MOBILE NETWORK OPERATORS

Syniverse

MasterCard & Syniverse are collaborating to make shopping easier and more secure than ever before, enabling your MasterCard to uniquely work where you and your phone are – anywhere in the world.

For consumers who opt-in, they'll be able to have:

Peace of Mind When Shopping
"ON THE GO"

Today, between **50-80 percent** of declined transactions abroad are actually legitimate, creating a real travel headache for consumers[2].

Through this collaboration, consumers will now be able to have an **extra layer of security** over their finances abroad through **geo-tagging**.

This means that no matter where you are in the world, when your card and your mobile device are in the same place, you're less likely to encounter the frustrations associated with unqualified card cancelations or blocked transactions.

In addition to this new security functionality, this collaboration will also create better options for roaming consumers to receive personalized offers and rewards whether they are at home or across the globe.

Improved Transparency and Choices for Roaming

70 percent of consumers switch off their mobile data when arriving in another country[1] – likely in an effort to avoid roaming charges. Through this collaboration, consumers will have a choice of prepaid data packages that they can purchase directly from their phone when they arrive in another country – meaning no more bad surprises on your phone bill down the road.

Relevant Offers and Rewards Anywhere Around the Globe

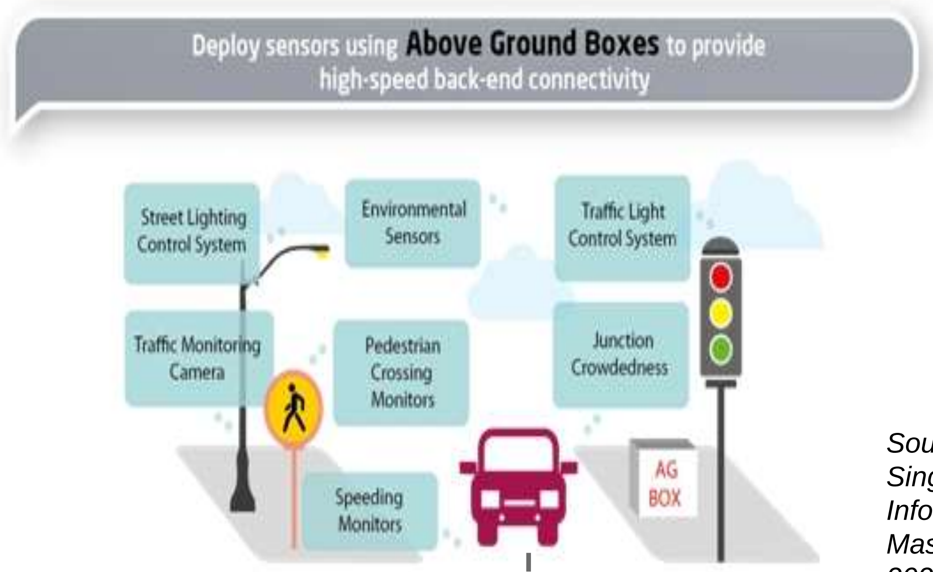
Consumers will be able to receive personalized rewards when they're away from home such as coupons and special geo-based offers. This means getting access to deals and discounts that matter most to you whether you're in London or Los Angeles.

The Data Economy

Issues lurk in the Internet of Things:

- Security risks?
- Is the use always for the benefit of the individual?
- Does the individual have control over the decisions being made?

The Data Economy


Deploy sensors using Above Ground Boxes to provide high-speed back-end connectivity
Street Lighting Control System
Environmental Sensors
Traffic Light Control System
Traffic Monitoring Camera
Pedestrian Crossing Monitors
Junction Crowdedness
Speeding Monitors
AG BOX

Source: Singapore Infocomm Media MasterPlan for 2025

Insurance Provider?

Other service providers?

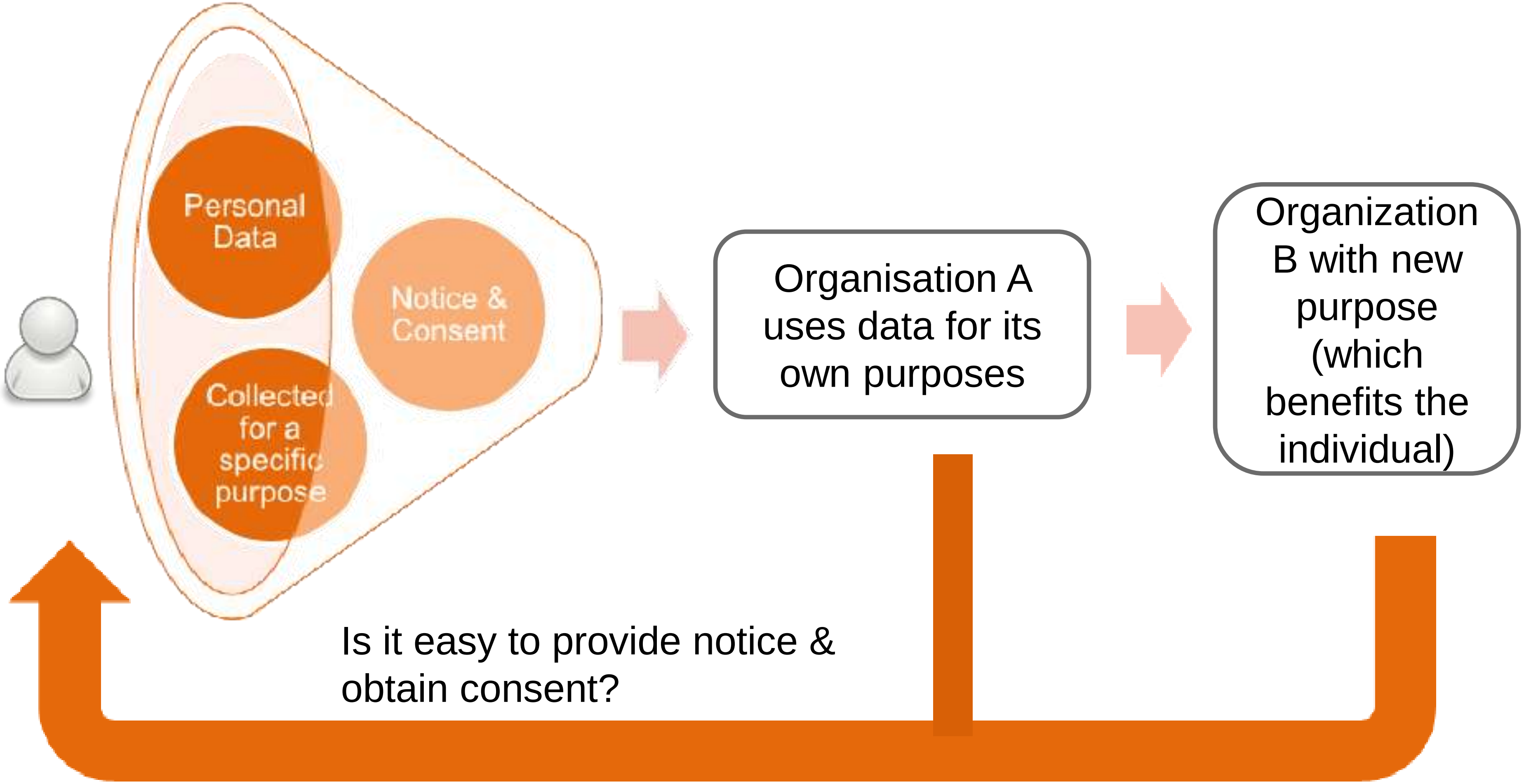
Value

- Reduced pollution
- Reduction in wastage of time / money

Issues

- Sharing data with other providers?
- Is the data attributed correctly?
- Where do you draw the line?

Privacy Law in the IoT and the Big Data world



Organisation A uses data for its own purposes

Organization B with new purpose (which benefits the individual)

Is it easy to provide notice & obtain consent?

The Data Economy

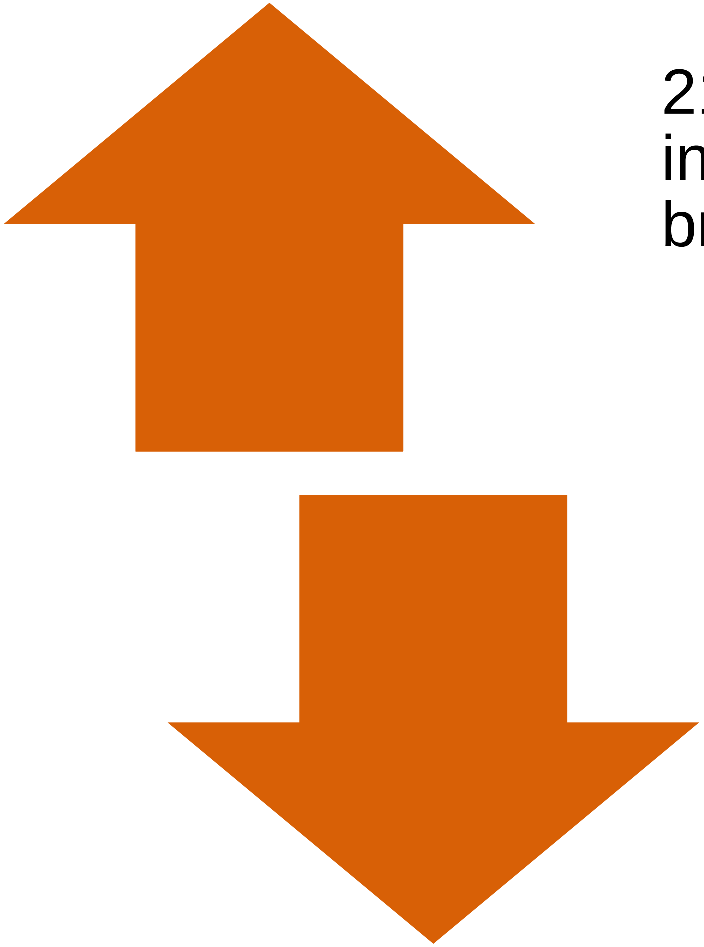
The Regulatory Response

Most laws in the region still apply Notice, Consent and Specific Purpose requirements

Japan: Institutional Revision for the Utilization of Personal Data

Greater consumer awareness … more laws

Data Breach



21% of 500 (i.e. 105) companies in Australia experienced a data breach

The State of Privacy Awareness in Australian Organisations (April 2013)

The OAIC received:

56 breach notifications in 2010-2011

46 breach notifications in 2011-2012

71 breach notifications in 2013-2014

The Regulatory Response

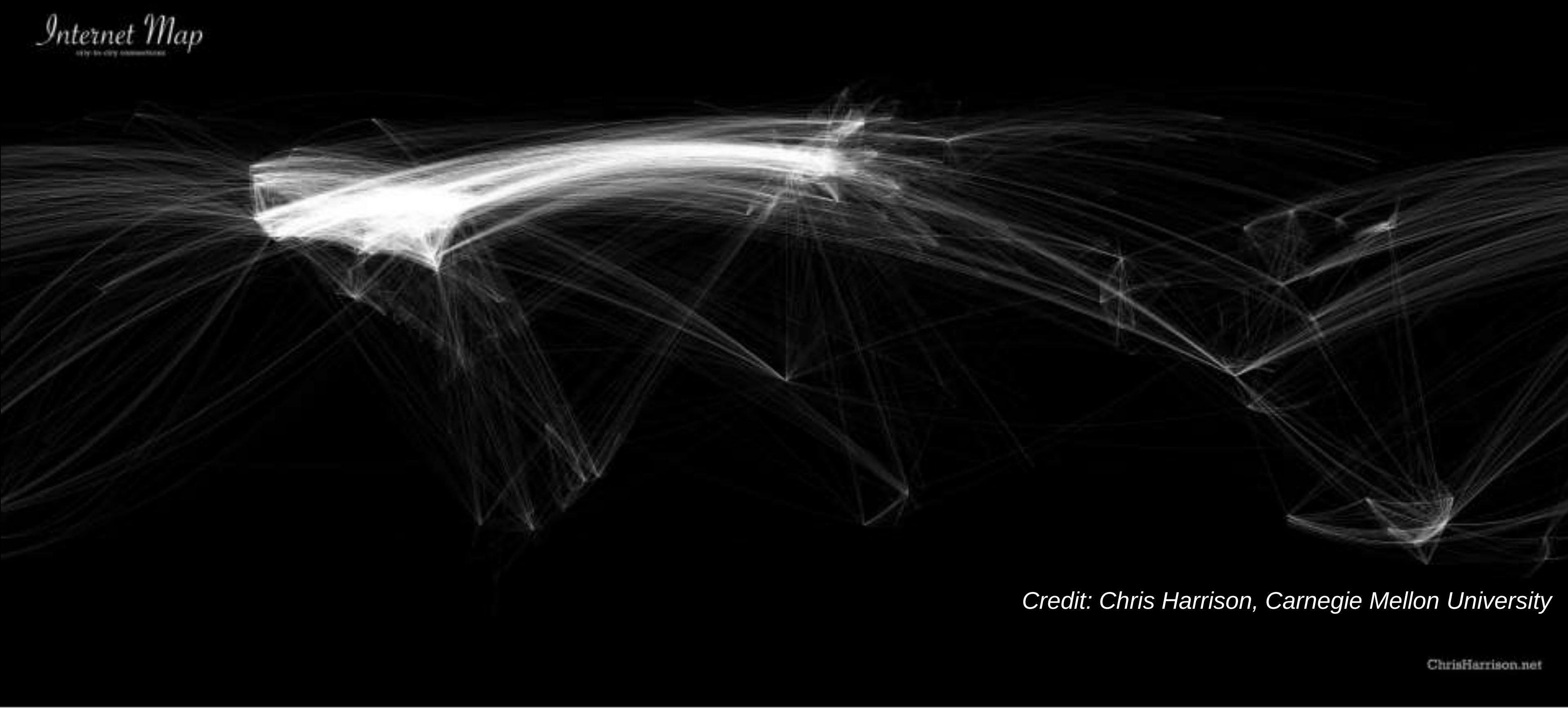
- Mandatory Breach Notification Obligations
  - Existing countries: China, Japan, India, Philippines, South Korea and Taiwan
  - On the horizon: Australia, New Zealand
- Stricter Penalty Frameworks
  - Australia, Singapore
  - Hong Kong, Malaysia

Data Breach

Country	Financial penalty	Imprisonment
Malaysia	Up to RM500,000 fine Up to RM200,000 fine for direct marketing	Up to 3 years Up to 2 years for direct marketing
Singapore	Up to S$1 million Up to S$10,000 for failure to check DNC registry requirements	Generally none
Australia	Up to A$340,000 for individuals Up to A$1.7 million	Generally none
Taiwan	Up to NT$1,000,000	Up to 5 years
South Korea	Varies depending on gravity of breach: from KRW 10 million to KRW 50 million	Varies: up to 5 years
Philippines	A range of penalties from PHP500,000 to PHP5 million	1 to 3 years 3 to 6 years for sensitive personal data
Hong Kong	HKD50,000, with additional penalty on a daily basis if the penalty continues	Up to 2 years for contravention of enforcement notice Up to 3 years for direct marketing offences
India	Company has to pay compensation to affected individual No limit to amounts recoverable	Up to 3 years for unlawful disclosure
Macau	Up to MOP 80,000 to MOP 100,000	Up to 1 year
Japan	Up to ¥300,000	Up to 6 months (for failure to follow corrective order)

Data Sovereignty Concerns

Interconnectedness and data flows are at their highest but some countries are imposing cross-border data restrictions (such as data localization)



Credit: Chris Harrison, Carnegie Mellon University

Data Sovereignty Concerns

Data localization will *not* help the economy; it will harm the local economy

	Effect of proposed or enacted data localization requirements		
	GDP	**Investment**	**Welfare Loss (USD)**
China	-1.1%	-1.8%	61.6 bn
India	-0.1%	-1.4%	3.1 bn
Indonesia	-0.5%	-2.3%	2.7 bn
Korea	-0.4%	-0.5%	5.3 bn
Vietnam	-1.7%	-3.1%	1.5 bn

Bauer, Lee-Makiyama, Marel, Verschedle, The Costs of Data Localisation: Friendly Fire on Economic Recovery (ECIPE) 2014

Data Sovereignty Concerns

Data localization does *not* increase security or protect the privacy of individuals' data or protect against government surveillance; it may weaken security and privacy

Data localization *will* introduce risk if both production and DR sites are in the same country

Data localization does *not* result in the creation of many jobs

A better regulatory response to cross-border data flows: the accountability model in Australia, the Philippines and Singapore

Key Takeaways

- A lot of new laws, and more laws on the way
- These are driven by various reasons including increased use of data for varied purposes; data breaches
- Keep an eye on countries like Japan which are trying to figure out the right balance between using data in a Big Data world and respecting the individual's right to control the use of data – a very tricky balancing act
- Keep an eye out for restrictions on cross-border data transfers which may introduce risks to your systems

Tony Pereira, Business Leader,
Product Management, MasterCard

Brian McCormack, , Senior Business Leader,
Fraud Management Solutions, MasterCard

DATACASH
A MASTERCARD COMPANY

MasterCard

Confronting Fraud from All Angles: Risk-Based Solutions

Risk Angles

	ISSUING	ACQUIRING
Lost and Stolen	✓	✓
Account Takeover	✓	✓
Counterfeit	✓	
Card Not Present	✓	✓
Card Never Received	✓	

Card Fraud Tools Comparison

Risk Portfolio	Acquiring	Issuing	Online Merchants
Risk Group Focus	Acquirers	Cardholders – CP (Liability)	Merchants (Liability)
Decision Data	Settlement	Authorization and Cardholder (if available)	Authorization, CRM, Shopping Cart, Shared Data
Predominant Method	Historical Averages	Cardholder spend attributes and portfolio	Transaction analysis good/bad based on attributes and velocities
Tools	SQL, db	Statistical Approaches (Neural) Rules	Rules, db (+ & -)
Timing	Batch	Near Real Time	Near Real Time, Real Time Batch

MasterCard Issuing Fraud Tools

- Issuers’ wish list
- Our solution

Issuers' wish list

Pre- Authorization

Real- time decisioning

Artificial Intelligence

Business rules

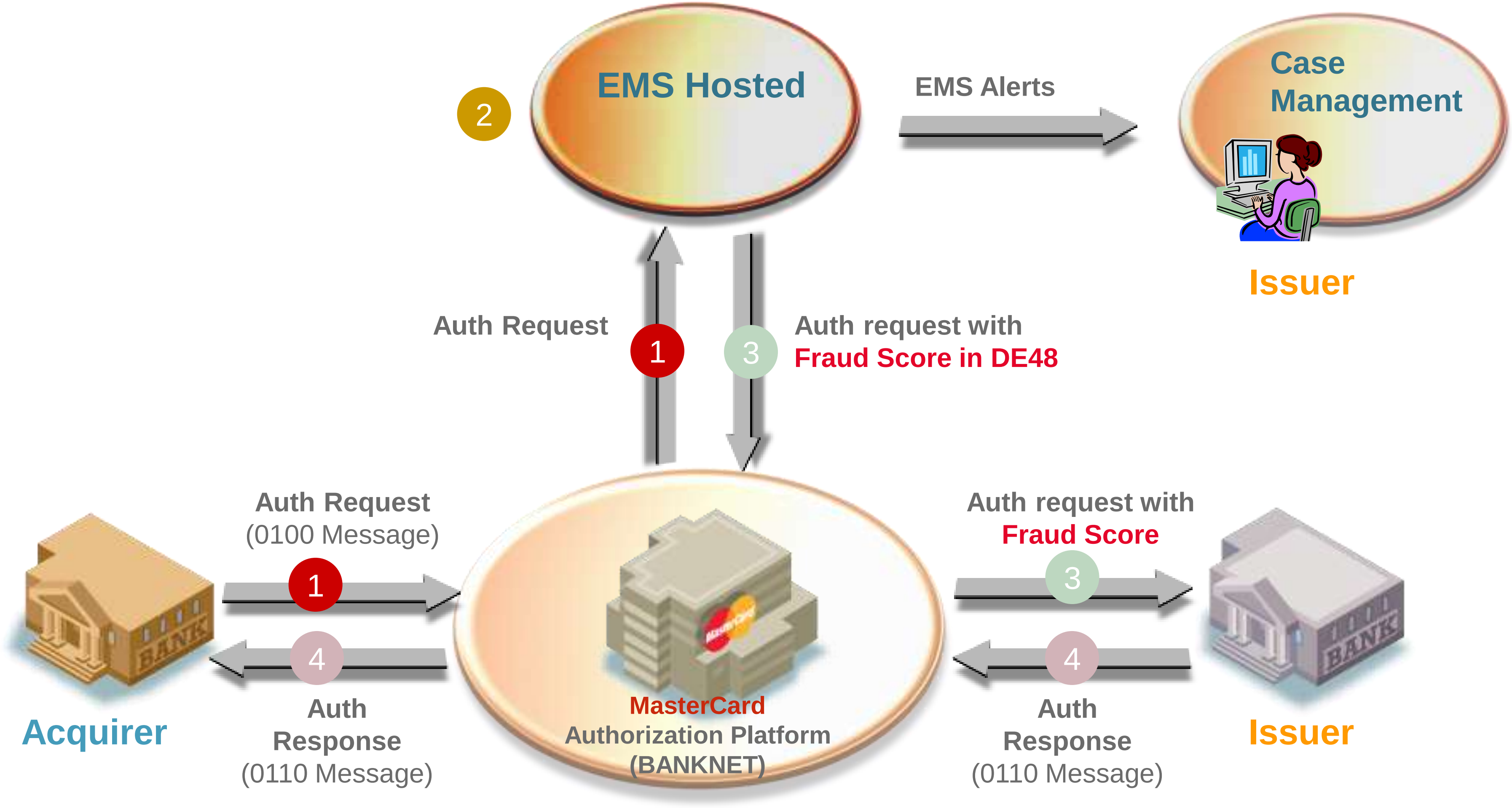
Real-time Blocking

Fraud Score in message

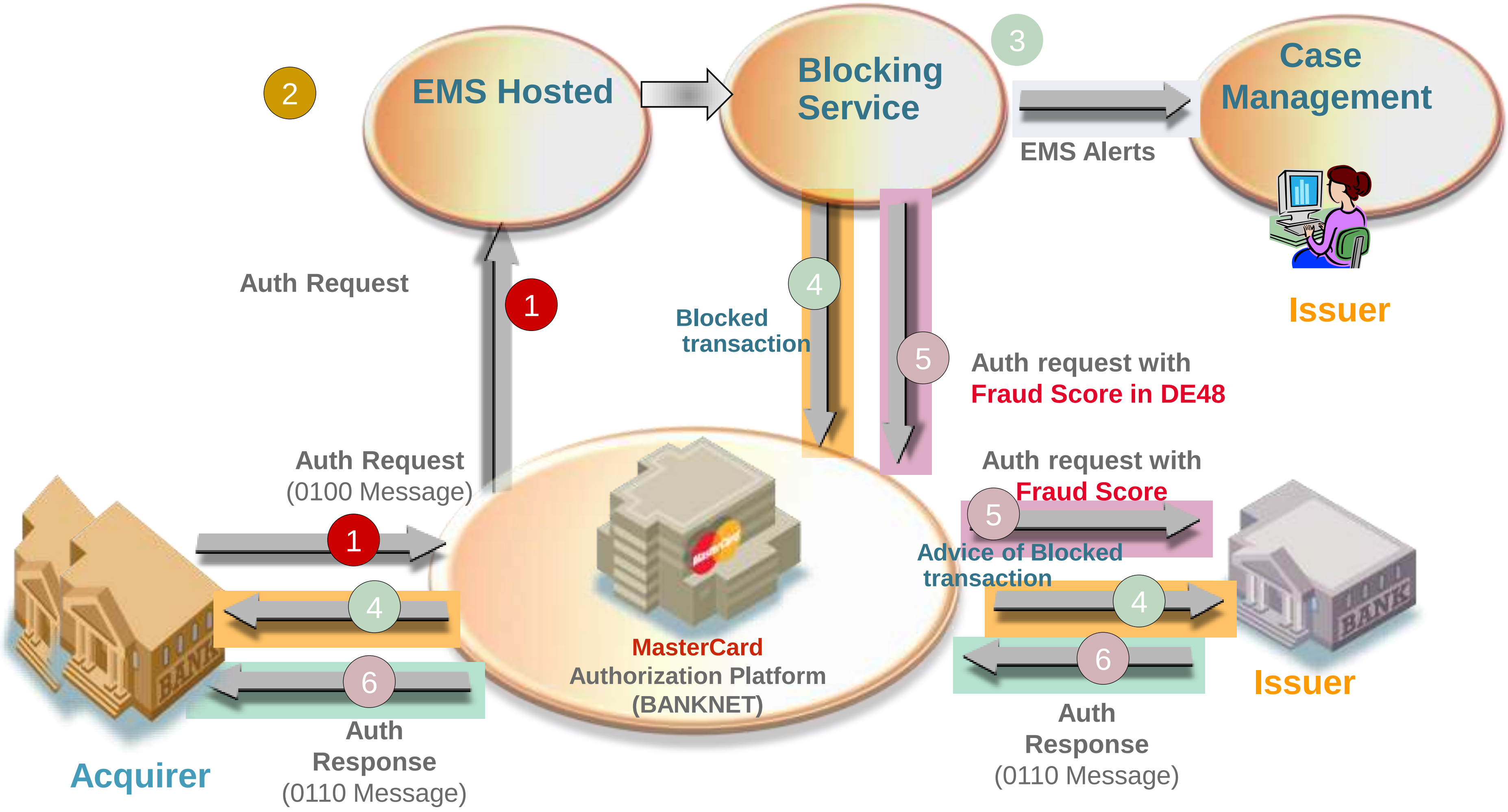
Case Manager

Analytical reports

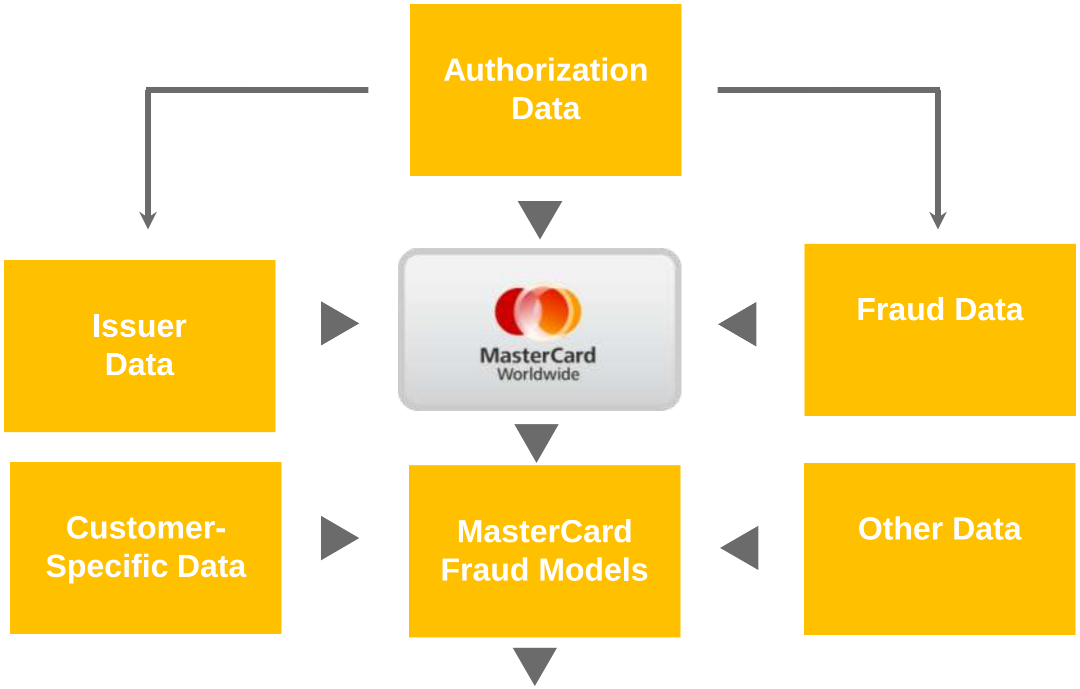
Transaction scoring in Real-Time (during Authorization process prior to Auth decision)



Transaction scoring & transaction blocking in Real-Time (during Authorization process prior to Auth decision)



MasterCard’s unique wealth of data - globally integrated fraud data yields invaluable insight



Authorization Data

Issuer Data

MasterCard Worldwide

Fraud Data

Customer-Specific Data

MasterCard Fraud Models

Other Data

Data–Driven Scoring Solutions

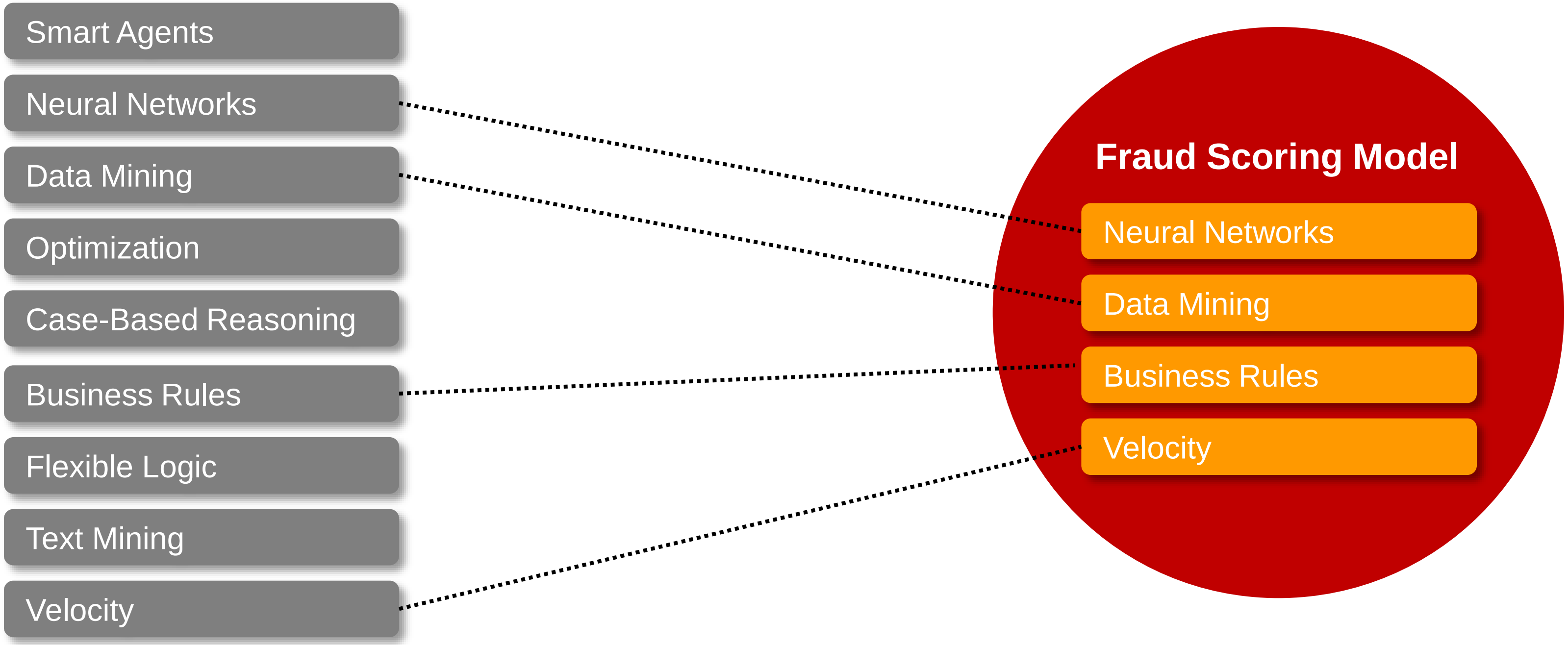
`

- Geographically–Specific Models
- Transaction–Specific Models
- Product–Specific Models
- Custom Models

Components of EMS - state-of-the-art analytics enable targeted fraud scoring models

The **power of numerous modeling technologies** applied to MasterCard’s vast transaction and fraud data yields highly predictive fraud scores.

Expert Monitoring Technologies

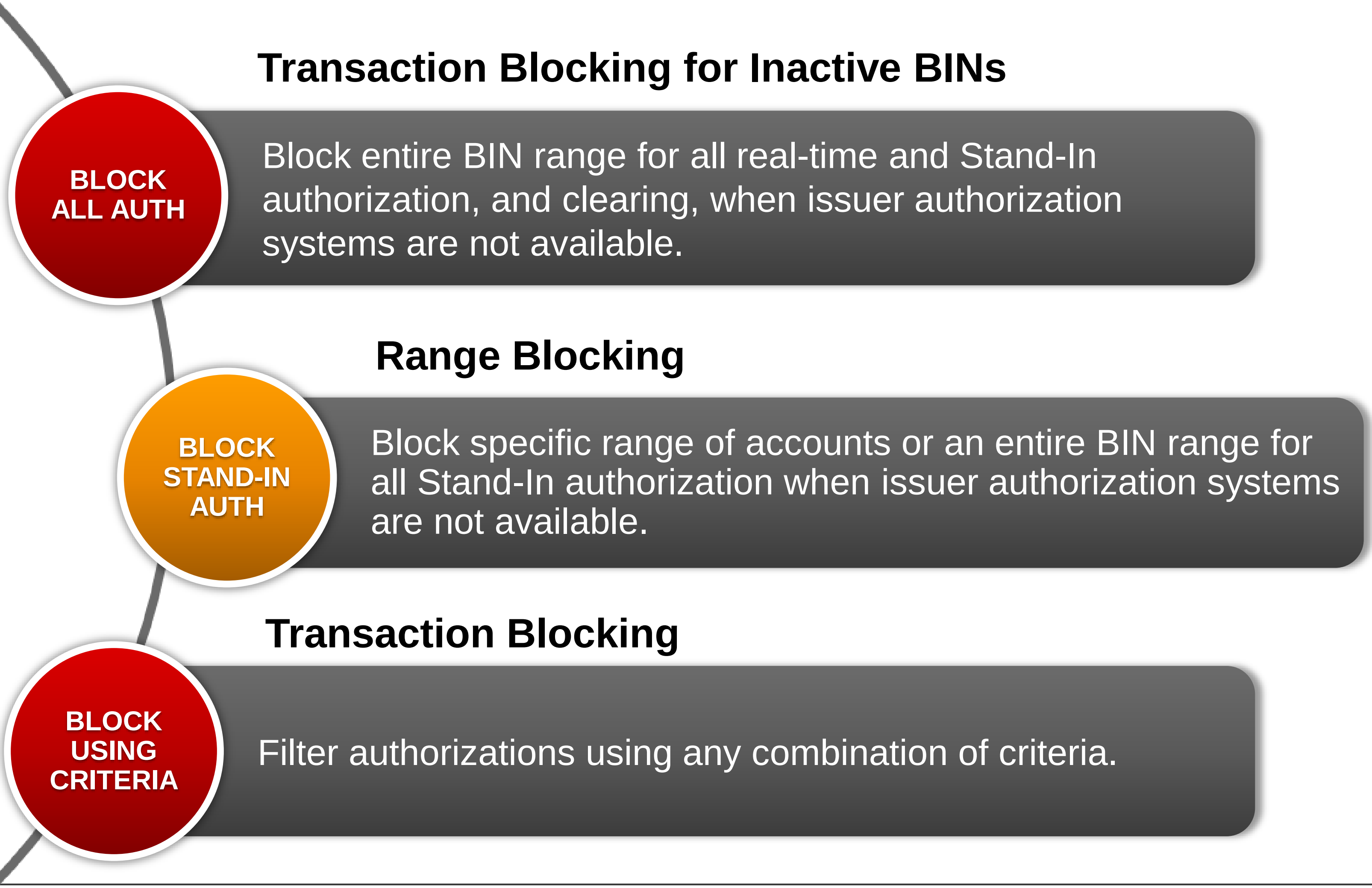


- Smart Agents
- Neural Networks
- Data Mining
- Optimization
- Case-Based Reasoning
- Business Rules
- Flexible Logic
- Text Mining
- Velocity

Fraud Scoring Model

- Neural Networks
- Data Mining
- Business Rules
- Velocity

Protect new payment programs and inactive accounts from fraud attacks



Transaction Blocking for Inactive BINs

BLOCK ALL AUTH

Block entire BIN range for all real-time and Stand-In authorization, and clearing, when issuer authorization systems are not available.

Range Blocking

BLOCK STAND-IN AUTH

Block specific range of accounts or an entire BIN range for all Stand-In authorization when issuer authorization systems are not available.

Transaction Blocking

BLOCK USING CRITERIA

Filter authorizations using any combination of criteria.

GateKeeper:2.0

Merchant fraud prevention systems: Tools and technologies

There are a number of tools and technologies on the market today. Merchants may choose to assemble a suite of these tools themselves or use more advanced fraud prevention solutions from an outsourced provider

Examples of tools & technologies used today:

- ○ I.P. Geo-location
- ○ Business Rules Engines
- ○ Negative Databases – Per merchant, per industry
- ○ Address Validation Tools – Post office address tools
- ○ Personal/Identity Validation Tools – Facebook, LinkedIn
- ○ Device Identification/PC Fingerprinting
- ○ Public Records Validation – Telephone Book, Electoral Roll
- ○ Other types of "transaction intelligence": Card BIN analysis, Customer history analysis
- ○ Generally-available Internet Tools (Google Maps, Whitepages.com, etc.)

Key solution aspects for eCommerce fraud prevention

Integration flexibility

Solution must work with existing client practices

Workflow integration – minimize the total cost of fraud management:

Solution rather than product focus

Real-time, pre/post authorisation batch submission

DataCash GateKeeper:2.0

DATACASH
A MASTERCARD COMPANY

MasterCard

- Merchant facing fraud prevention and investigation toolkit
- 450 Business Rules, real time and offline – up to 150 fields of data
- Use of confidence indexing uniquely offered by DataCash

Transactions from over 180 countries analysed

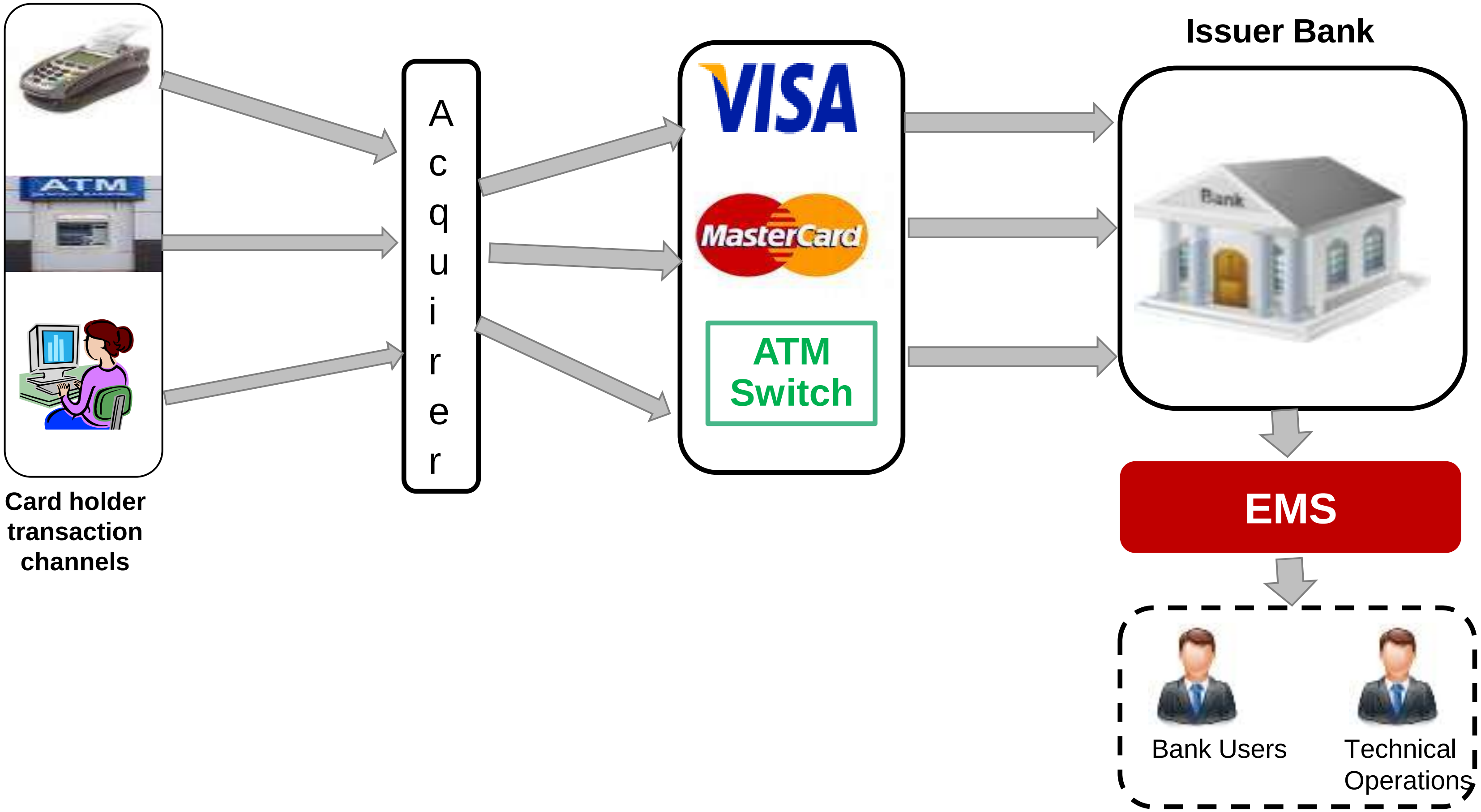
30,000 merchants actively using service

Over £1 million of attempted fraud prevented each day

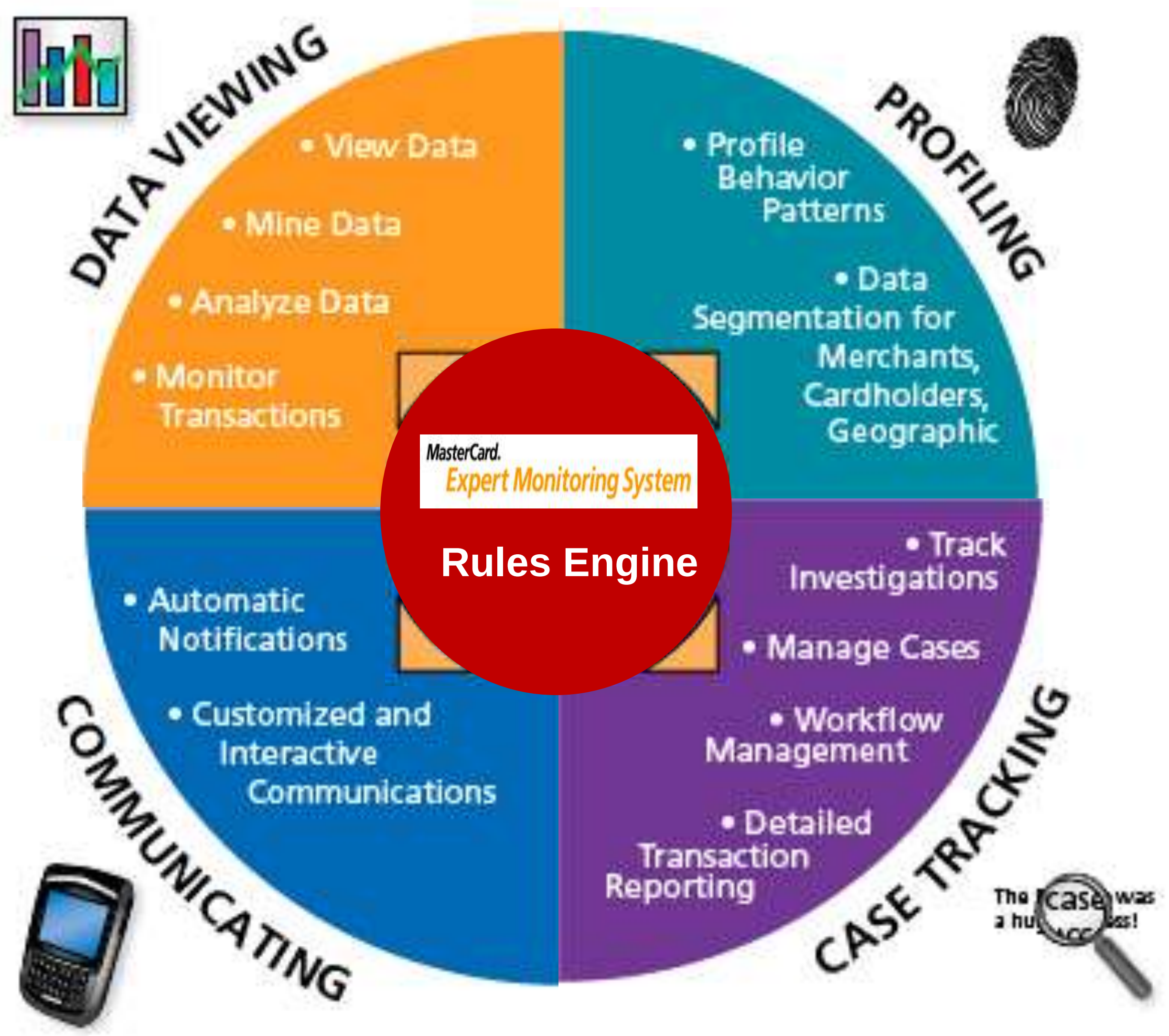
- Proprietary shared positive and negative databases
- Over 200 staff dedicated to:
  - Support, development, analysis of fraud patterns
  - Complete back office reviewing transactions on behalf of merchants

EMS Local Software Solution

Normal transaction flow



System implemented by the Bank: EMS local



MasterCard. Expert Monitoring System

Rules Engine

DATA VIEWING

- View Data
- Mine Data
- Analyze Data
- Monitor Transactions

PROFILING

- Profile Behavior Patterns
- Data Segmentation for Merchants, Cardholders, Geographic

COMMUNICATING

- Automatic Notifications
- Customized and Interactive Communications

CASE TRACKING

- Track Investigations
- Manage Cases
- Workflow Management
- Detailed Transaction Reporting

System implemented by the Bank: EMS local

Component	Ownership & Control	Comment
Hardware	Bank	Located in Bank's premises
EMS Local software	MasterCard	Installed on the Bank's hardware
Supporting Software	Bank	Operating System, Java, Database System
Other relevant information		
Channels	All channels	ATM, POS, eCommerce
Brands	All brands	MasterCard, Visa, JCB, Union Pay, Amex
Products	Debit, Credit & Prepaid	
Message Types	Authorization, Clearing, Refunds,	

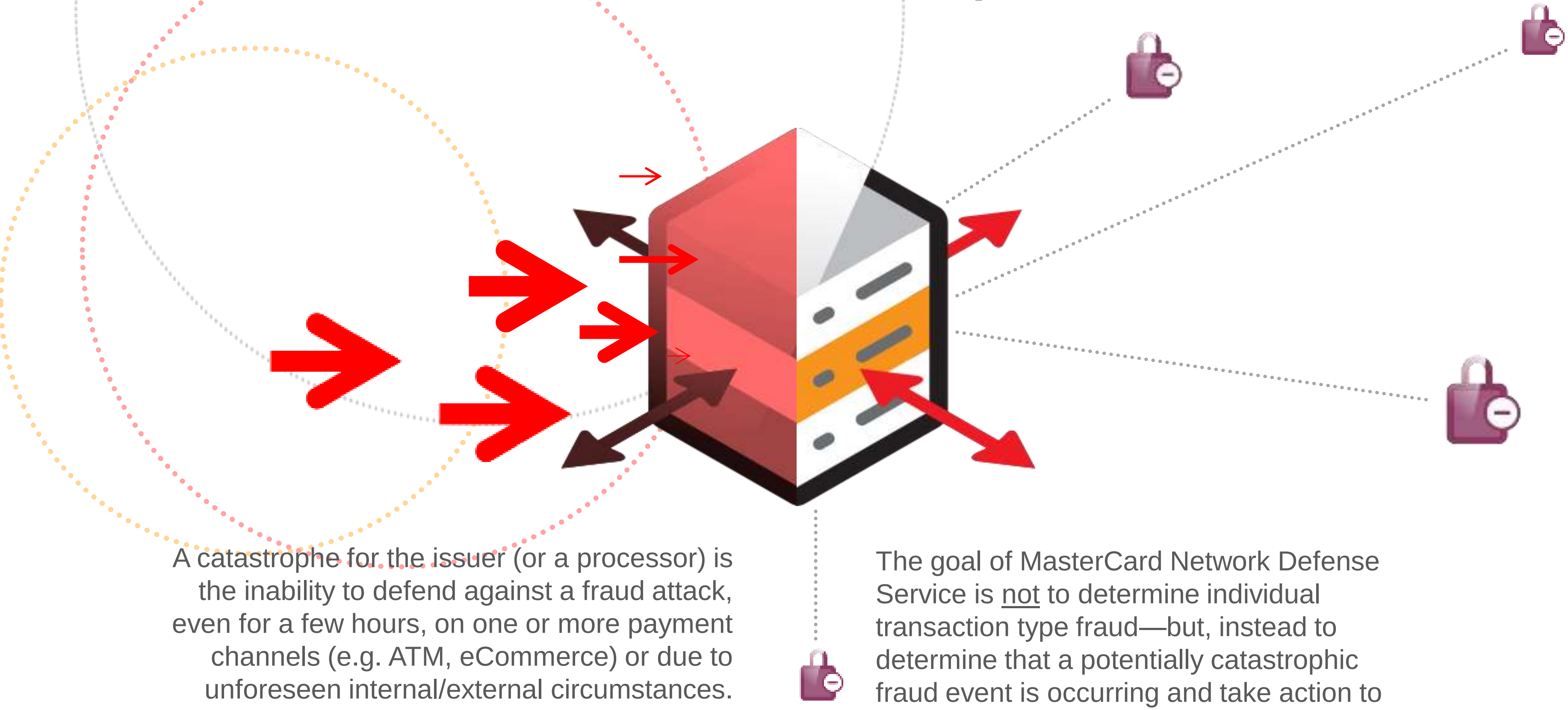
MasterCard Network Defense

MasterCard Network Defense - A Second Line of Defense!

DATACASH
A MASTERCARD COMPANY

MasterCard

MasterCard Network Defense Service helps protect MasterCard customers from *catastrophic* fraud events



A catastrophe for the issuer (or a processor) is the inability to defend against a fraud attack, even for a few hours, on one or more payment channels (e.g. ATM, eCommerce) or due to unforeseen internal/external circumstances.

The goal of MasterCard Network Defense Service is not to determine individual transaction type fraud—but, instead to determine that a potentially catastrophic fraud event is occurring and take action to help prevent further loss.

How does MasterCard Network Defense work? Monitoring process

OCC Activity

- 5 hour block is enabled for account
- OCC receives Alert and transaction detail
- OCC contacts issuer via email to Security contacts in MIM

Monitoring

- Thresholds by channel with velocity in a specific timeframe
- Multi-location monitoring
- ***Result - 2 kinds of declines; individual transaction decline; channel block***

Blocking Criteria

- Sum exceeds the threshold - decline transaction
- Fifth attempt exceeds threshold – block subsequent transactions in that channel for 5 hours

OCC – MasterCard Operations Command Center - http://mccentral.mastercard.com/bu/ot/cno/ocs/occ/Pages/default.aspx

Risk Angles

	MASTERCARD SOLUTIONS PROTECT AGAINST
Lost and Stolen	✓
Account Takeover	✓
Counterfeit	✓
Card Not Present	✓
Card never received	✓

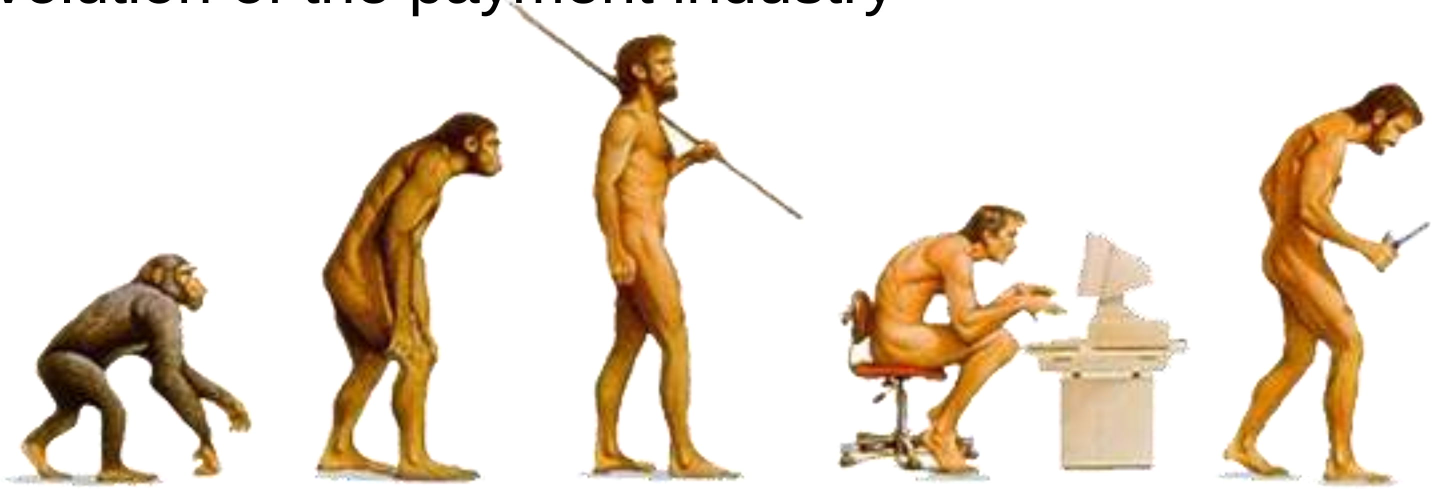
Paul J. Paolucci, Senior Business Leader, MasterCard

Keith Groves, EVP, G2 Web Services

Leveraging Compliance to Optimize Your Business

Leveraging Compliance

- Identify new or existing trends
- Identify challenges and vulnerabilities
- Optimize acceptance and reduce fraud loss
- Evolution of the payment industry



The Here and Now

- *Issuer Monitoring Program (IMP)*
- *Questionable Merchant Audit Program (QMAP)*
- *Updated Chargeback Standards*
- *Payment Facilitator & Digital Wallet Operators*
- *Additional BRAM Categories*

Global Compliance Trends

New high-risk merchant categories emerging

Increased focus from legal, regulatory and law enforcement agencies

Proliferation of eMarketplaces – driving both opportunities and risks

High-risk merchants now leveraging person-to-person money transfer payment options

Identification of load-balancing schemes

Increase in Area of Use infractions

Payment Facilitator and Digital Wallet Operator models becoming more prominent

What’s on the Horizon?

- Enhancements to MATCH
- New Data Integrity Edits
- Continued focus on customer education
- BRAM Monitoring Program review
- Evaluation of aggregation compliance

Who Do You Need To Monitor?

Case Study…

An Acquirer with a very diverse portfolio

But was only monitoring high-risk merchants

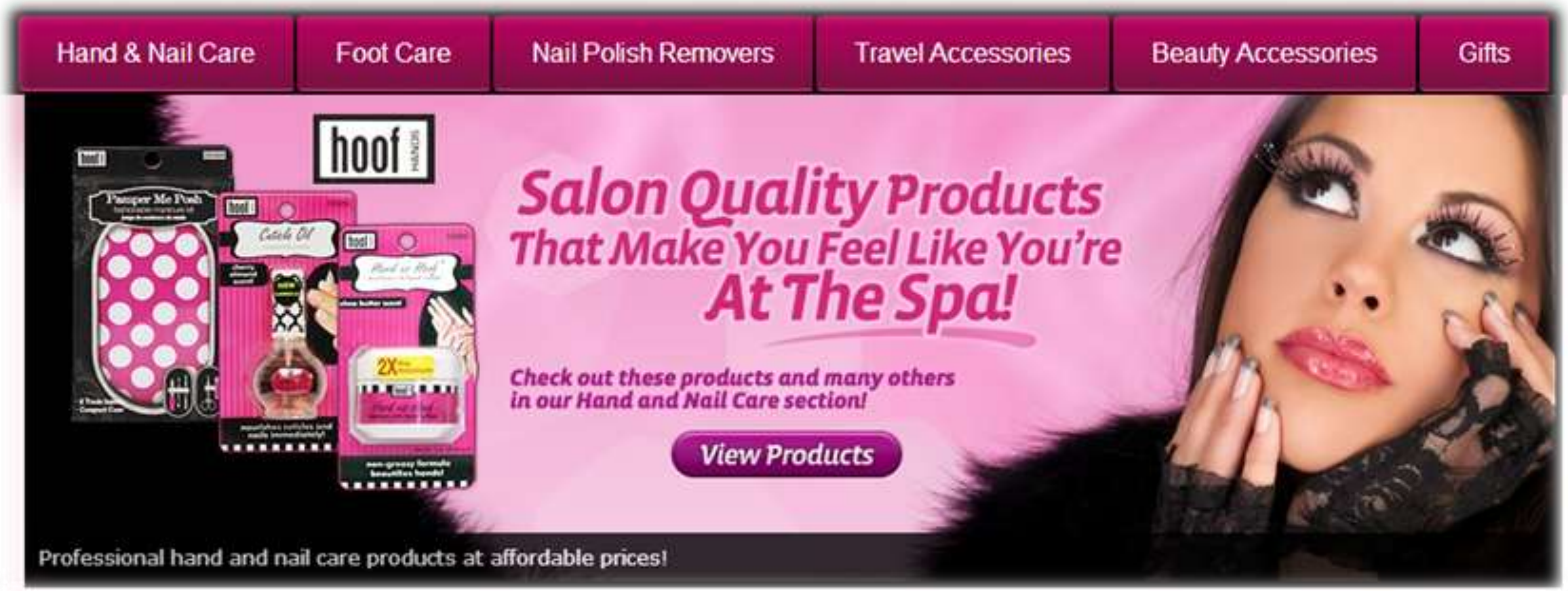
Case Study…

MasterCard

One of their low-risk merchants was selling beauty products

Case Study…

One of their low-risk merchants was selling beauty products



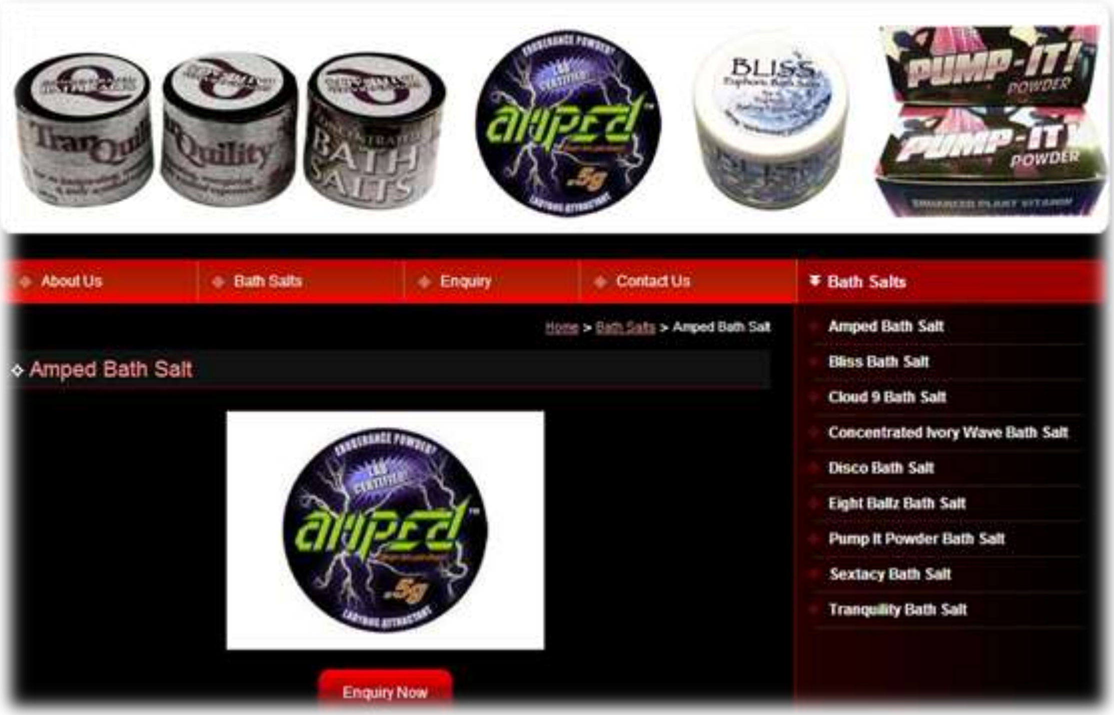
Salon Quality Products That Make You Feel Like You're At The Spa!

Check out these products and many others in our Hand and Nail Care section!

Professional hand and nail care products at affordable prices!

Case Study…

A few months later, they were informed of an alleged violation on the site



They had begun selling illegal "bath salts"

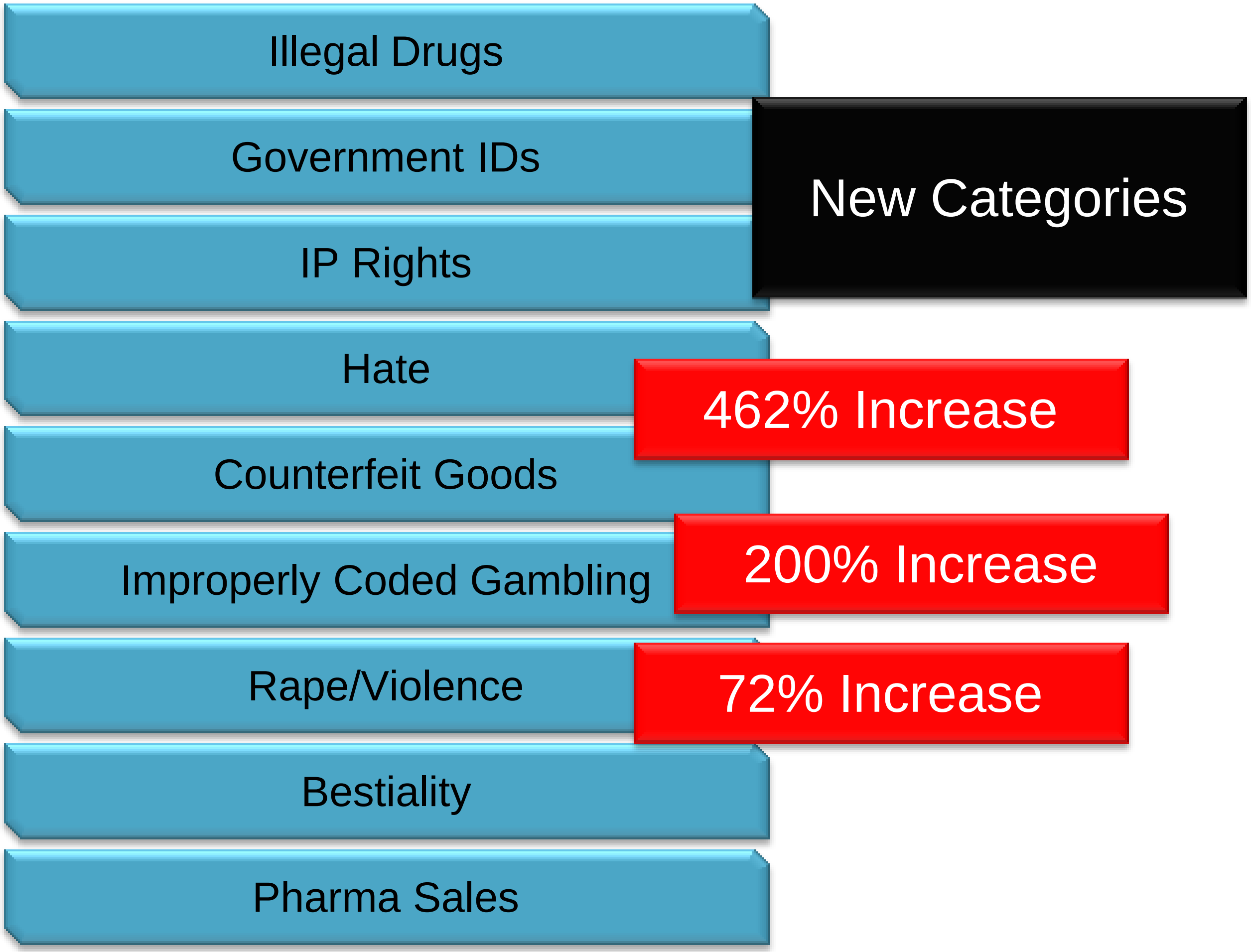
Case Study…

If they had monitored all of their merchants, they would have known about this change and could have handled it

How could it be avoided

- Monitor all merchants
- Review activity regularly
- Communicate with your merchants
- Know your partners

Content Violations



Illegal Drugs

Government IDs

IP Rights

New Categories

Hate

462% Increase

Counterfeit Goods

Improperly Coded Gambling

200% Increase

Rape/Violence

72% Increase

Bestiality

Pharma Sales

Potential Violations

- Counterfeit Goods
- Tobacco

461% Increase

- Bestiality
- Pharma Sales/Info

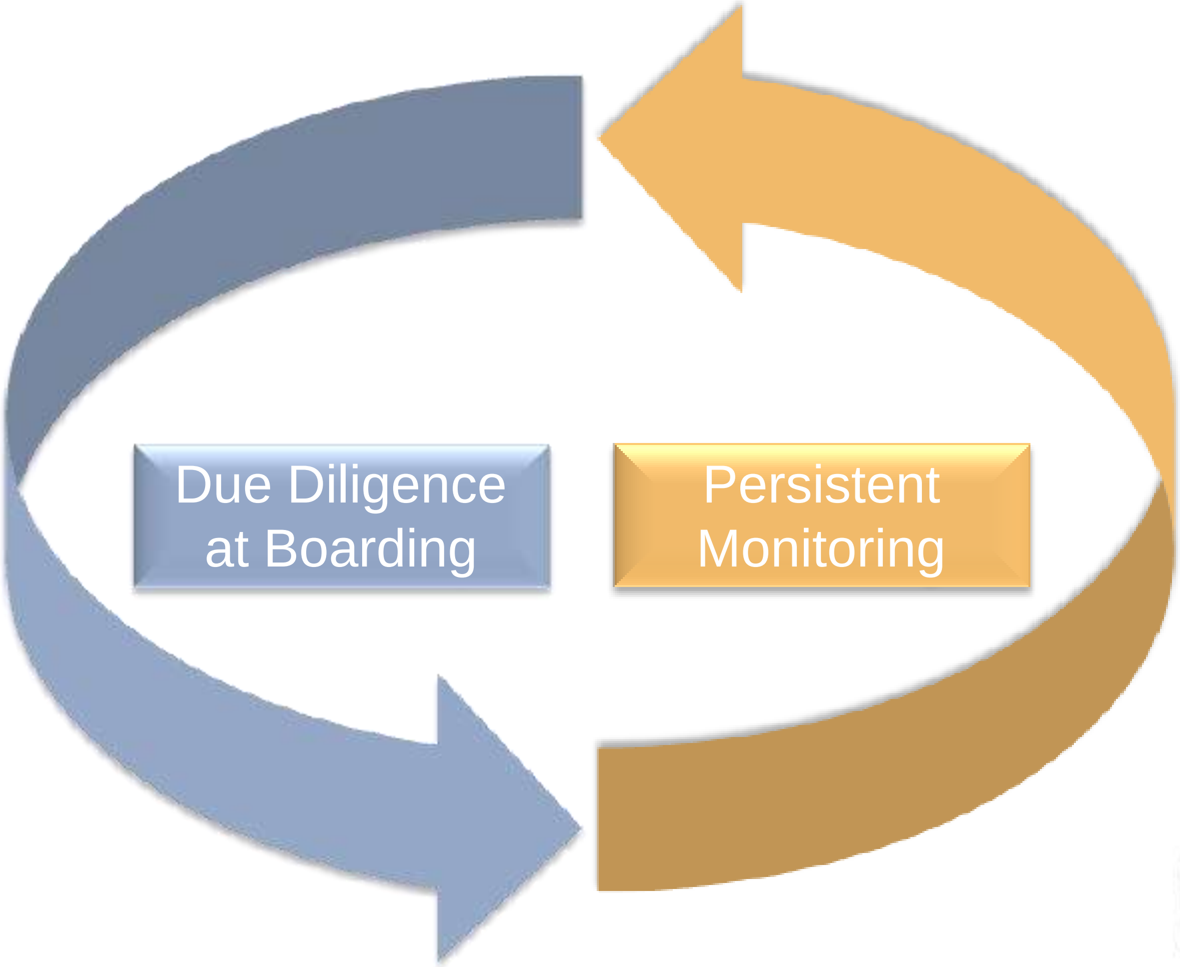
47% Increase

- IP Rights
- Rape/Violence

5% Increase

- Hate
- Improperly Coded Gambling
- Payment Processing
- Aggregation

Prevention



Due Diligence at Boarding

Persistent Monitoring

"I'll have an ounce of prevention."

Merchant Boarding

10% of merchants change acquirers each year

Need for speed conflicts with “Know Your Customer” requirements

Rapidly changing merchant risk makes due diligence difficult for most acquirers

Approving the Good Merchants

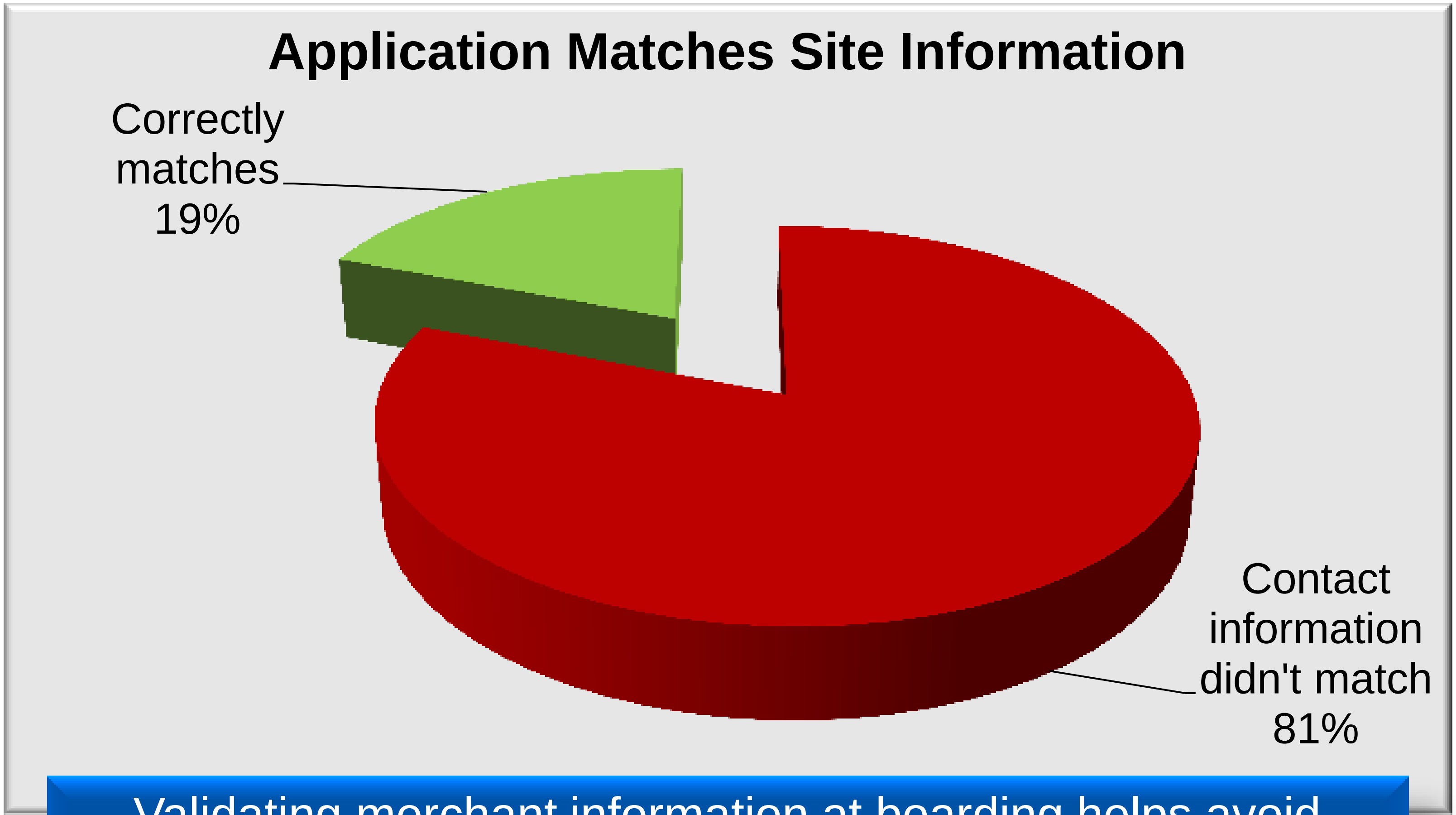
Understand the merchant before it enters your portfolio

Check background and website history

Uncover hidden risks and discrepancies on merchant application

Understand the profitability both today and in the future

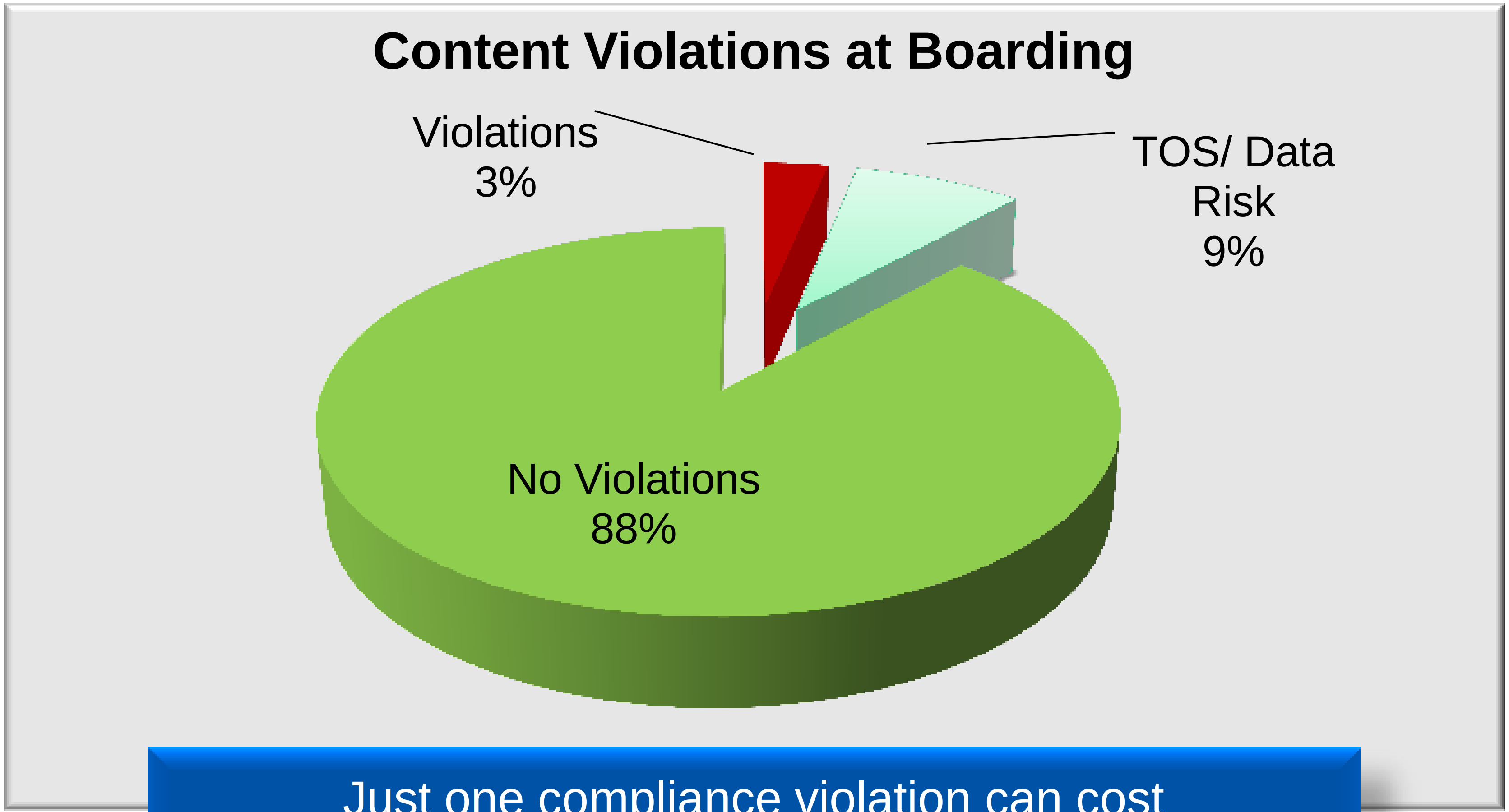
Consistency



Validating merchant information at boarding helps avoid identity theft and unscrupulous merchant fraud.

Compliance

MasterCard

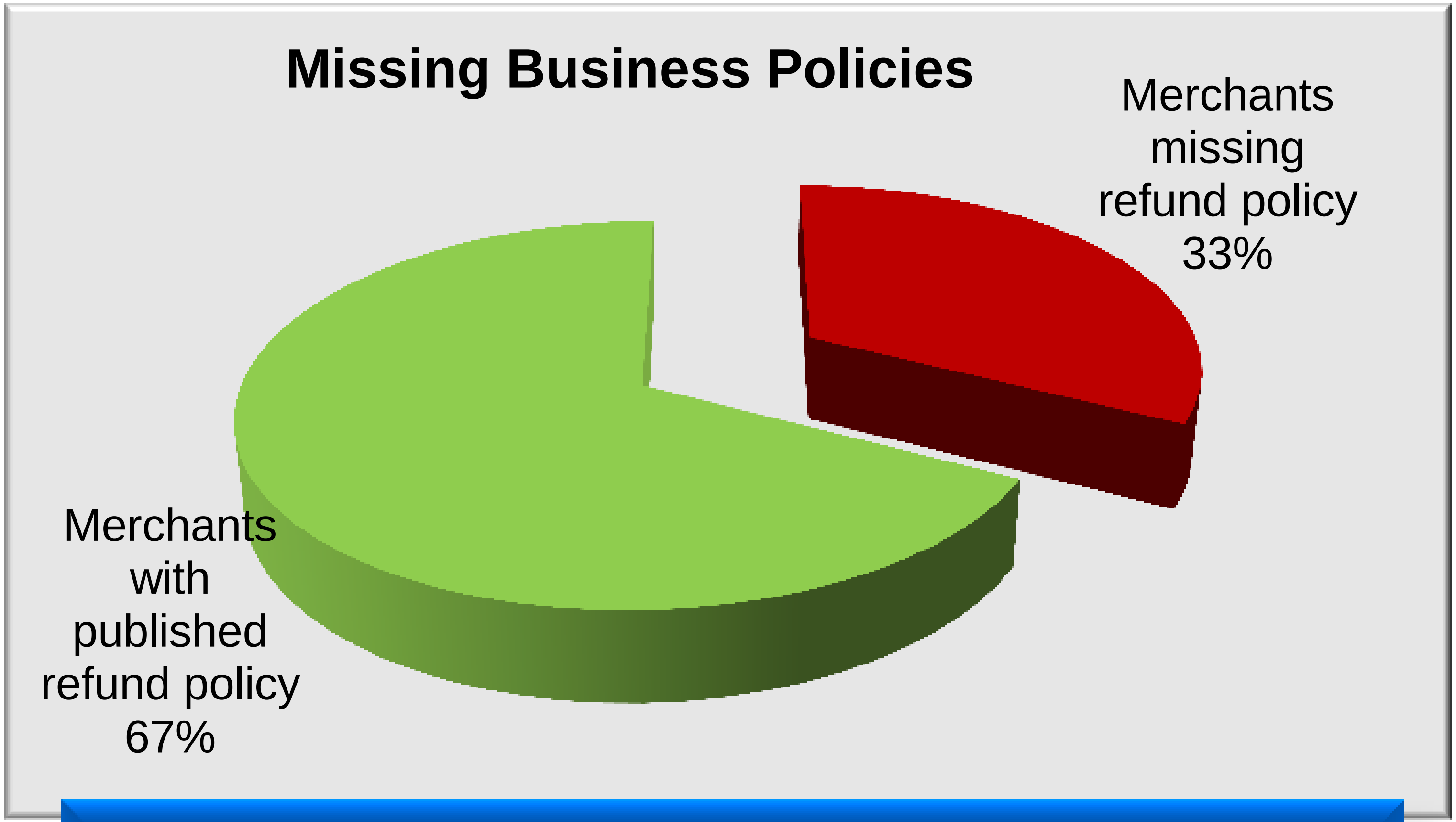


Just one compliance violation can cost hundreds of thousands of dollars.

Evaluate the Merchants Business Policies

Privacy policies and terms & conditions should be one link away from the Home page. They are often much harder to find.

Completeness



Missing refund policies can lead to high chargeback volumes and possible financial loss

Background Checks

Need to understand third parties supporting merchants

Identification of payment facilitators operating in merchant portfolio

Review industry & regulatory watch lists for the website and anyone associated with the merchant

Service Providers

Need to understand third parties supporting merchants

Identification of payment facilitators operating in merchant portfolio

Merchant History

Evaluate previous interaction with payments industry by merchant and principals

Online merchants register their websites as well as host and operate their businesses in acceptable locations

Summary

- Understand merchant history
- Query mandatory watchlists
- Identify and evaluate business policies
- Validate merchant and principal identities
- MATCH inquiries
- Evaluate profitability
- Review merchant business model

Julia Yeo
Vice-President, AP Franchise Development
MasterCard

Franchise Enablement in a Converging World

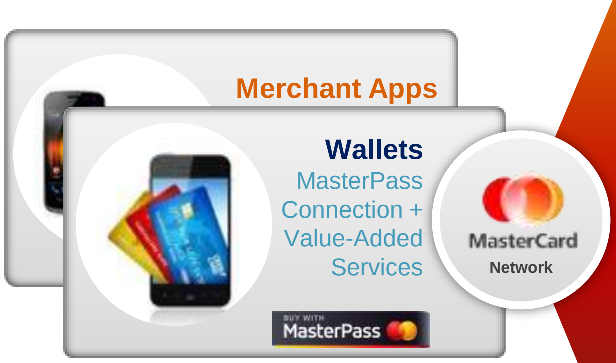
Topics

- Physical-to-digital convergence
- What it means to MasterCard
- What it means for you

Physical & Digital Worlds are Converging

MasterCard

Connected digital wallets/apps from issuers and retailers



Merchant Apps

Wallets
MasterPass
Connection +
Value-Added
Services

MasterCard
Network

At home
Smartphone
Tablet
PC, Laptop
Fridge*
TV*
Game Console*

In store*
Tablet
Kiosk
Mobile in Aisle
POS via NFC, QR

On-the-Go*
Store Window
Bus Stop
Subway Platform
Airport
Anywhere

* Illustrative only, functionality not yet available

Application of Physical to Digital Convergence

MasterCard

Current

Move from paper to plastic, and introduction of digital

Separate experiences in physical and online channels

Primarily payments, limited benefits beyond paper offers

Physical

Shop, pay, and pick up in store

Online

Order, pay, and deliver online

Converging

Inflexion point, gradual transition to digital

Lines blurring between physical and online environments

More than just payments, new experiences are being introduced

Order online and pick up in-store

Shop and price check in store, pay digitally and receive at home

Converged

World beyond plastic; every device is a commerce device

Omni-channel commerce and retailing

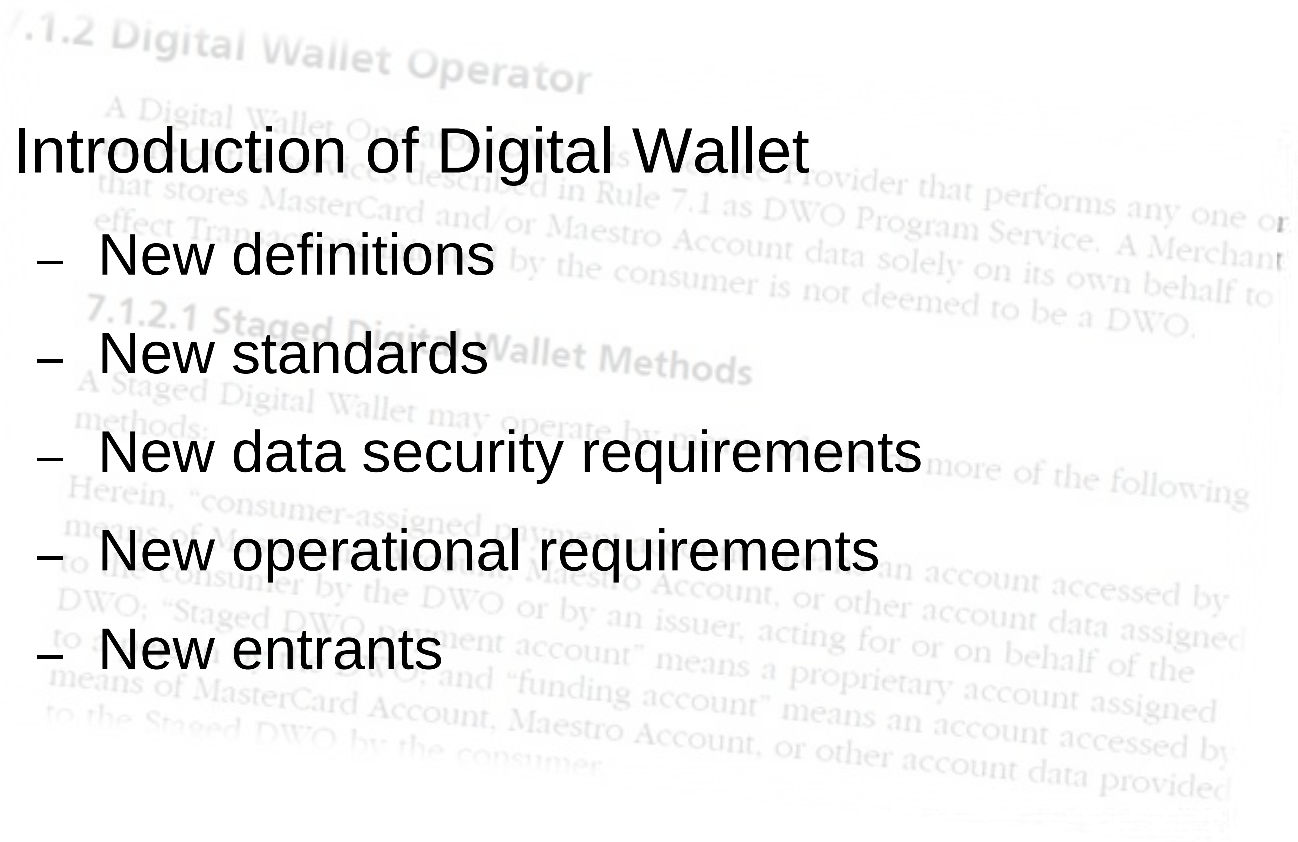
Consumer interaction before, during, and after

Shop, pay, and collect anywhere

Targeted offer instantly redeemed at the POI

Omni Channel

What it means to MasterCard



7.1.2 Digital Wallet Operator

A Digital Wallet Operator [illegible] is a Service Provider that performs any one or [illegible] services described in Rule 7.1 as DWO Program Service. A Merchant that stores MasterCard and/or Maestro Account data solely on its own behalf to effect Transactions [illegible] by the consumer is not deemed to be a DWO.

7.1.2.1 Staged Digital Wallet Methods

A Staged Digital Wallet may operate by means of [illegible] more of the following methods:

Herein, "consumer-assigned payment [illegible] means of MasterCard Account, Maestro Account, or other account data assigned to the consumer by the DWO or by an issuer, acting for or on behalf of the DWO; "Staged DWO payment account" means a proprietary account assigned to [illegible] the DWO; and "funding account" means an account accessed by means of MasterCard Account, Maestro Account, or other account data provided to the Staged DWO by the consumer.

- Introduction of Digital Wallet
  - New definitions
  - New standards
  - New data security requirements
  - New operational requirements
  - New entrants

Interoperability

Integrity

Massive data theft hits 40% of South Koreans

money.cnn.com/2014/01/21/technology/korea-data-hack/

Australia Post debit cards used in scam

http://www.couriermail.com.au/news/queensland/australia-post-debit-cards-used-in-scam/story-fnihsrf2-1226700140046

Bank Muscat hit by $39m ATM cash-out heist

http://www.theregister.co.uk/2013/03/01/bank_muscat_atm_mega_fraud/

Target: 40 million credit cards compromised

http://money.cnn.com/2013/12/18/news/companies/target-credit-card/

What it means for you

MasterCard’s Digital Vision

Issuer

A streamlined payment experience, both online and in-store, that brings global acceptance, security and simplicity across all channels and devices

Consumer

A richer shopping experience that is accessible across all channels, more secure, and provides access to more benefits than traditional methods

Merchant

A seamless ‘omni-channel’ commerce experience providing a better retail experience for consumers and generating increased sales

Jason Tymms, Prepaid Product Management APMEA, MasterCard

Barbara King, Group Head, Franchise Integrity, MasterCard

Building Effective Front-End Prepaid Strategies

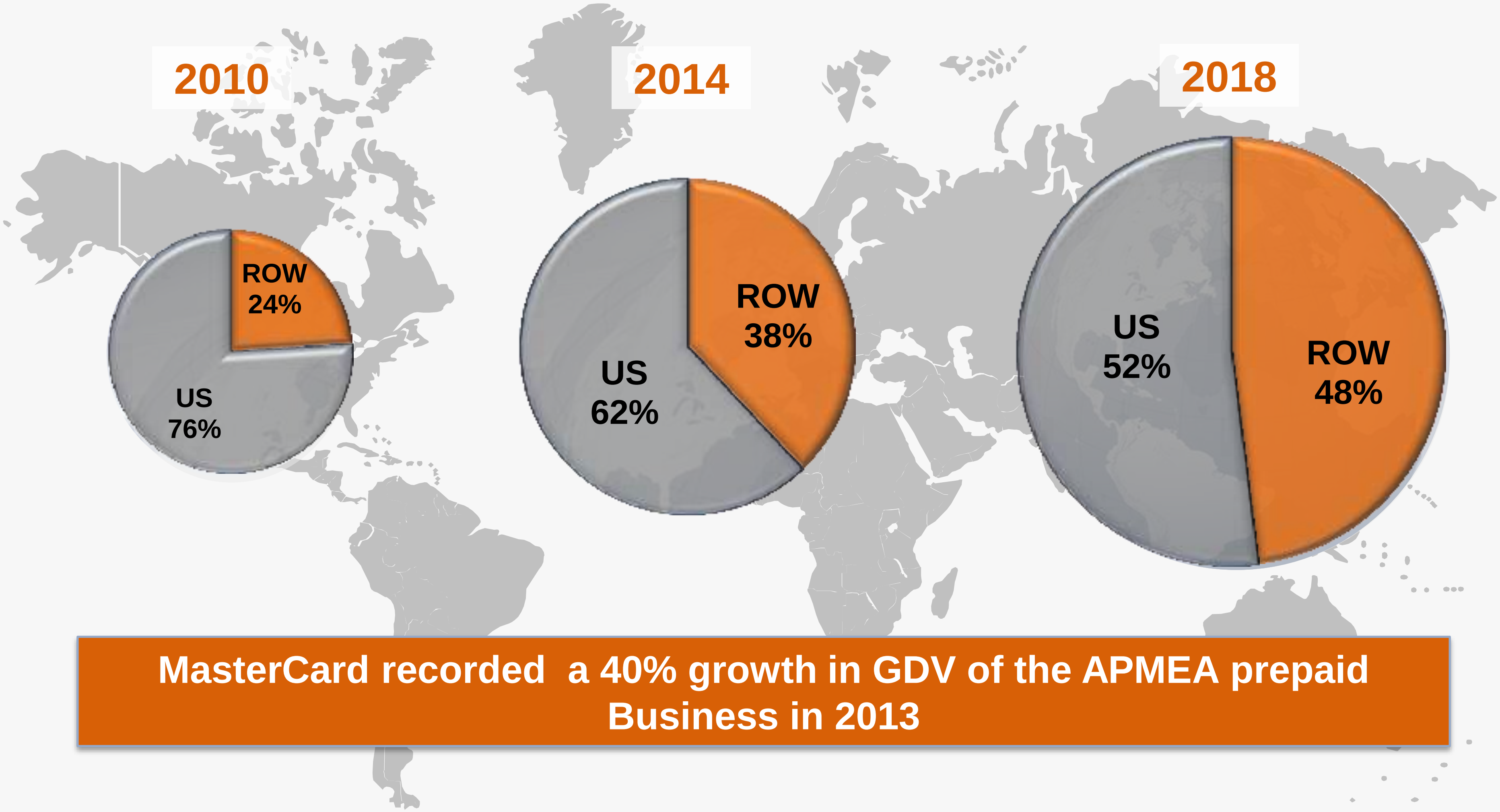
Why Prepaid Matters

Highly relevant solution that effectively **meets consumer, government and corporate needs**

Vast opportunity that is **growing fast in Asia Pacific**, increasing the complexity

With growth, comes risk - key is to manage risk without compromising growth

Evolving Risk Management Without Compromising Growth



MasterCard recorded a 40% growth in GDV of the APMEA prepaid Business in 2013

Source: Internal MasterCard data & projections

Specific Use Prepaid Cards Can Exhibit New Transactional Behaviors

- Travel and eCommerce cards
  - High international usage
  - Periods of inactivity
- Payroll/Government disbursements
  - High ATM utilization
  - Minimal transaction history

Managing Vulnerabilities in the Prepaid Value Chain

The prepaid value chain is fragmented:

- Roles and responsibilities are often unclear
- There are multiple potential points of failure

Most issuers have distant relationships with critical 3rd parties:

- Co-brand partners
- Distributors
- Program managers
- Processors

In late 2012 and early 2013, the industry experienced a series of systemic attacks impacting prepaid participants globally:

- Multiple regions
- Synchronized execution
- Limited cards/accounts compromised

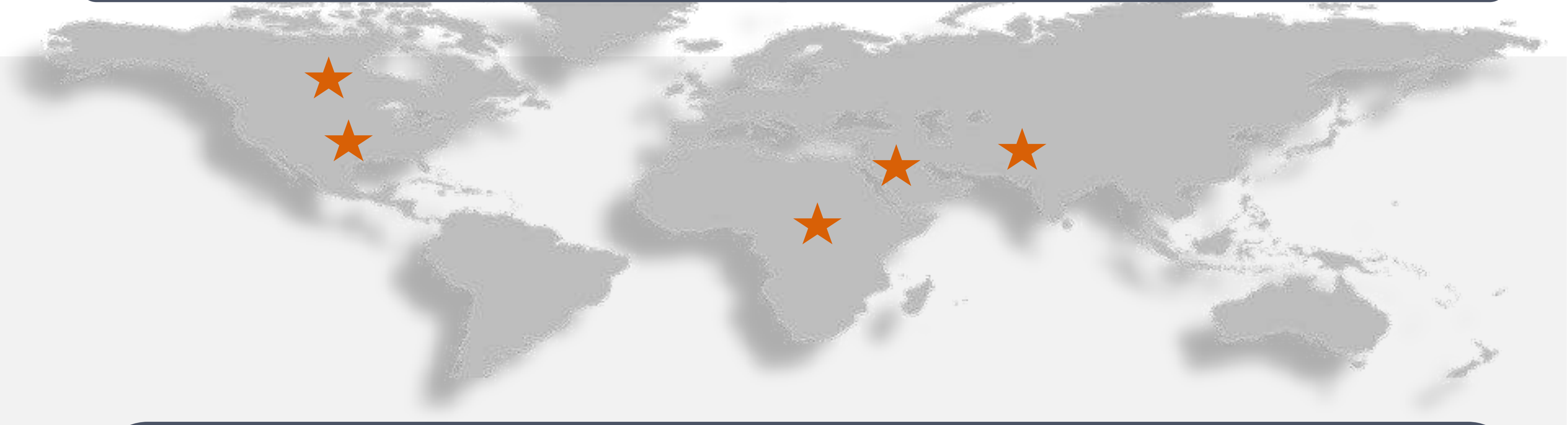
We must work together to protect all stakeholders and ensure the safety and stability of the entire industry

Barbara King
Group Head, Franchise Integrity
MasterCard

Building Effective Front-end Prepaid Strategies

Prepaid ATM Cash Out Style Attacks

- Cyber intrusion into Prepaid and Debit Processor or Program Manager Systems around the globe have undergone a resurgence over the last 2 years



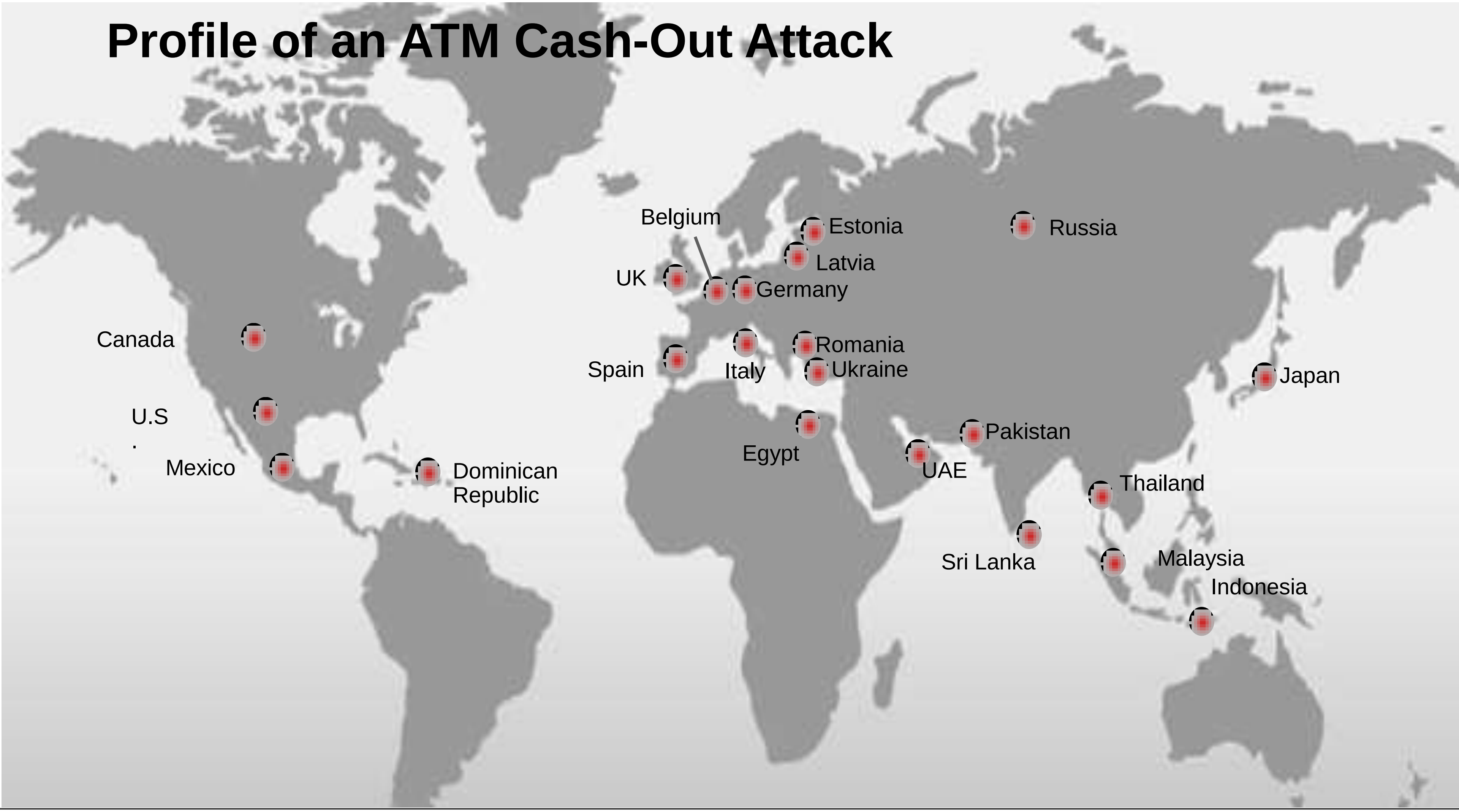
Method of attack:

- Disablement and manipulation of front -end fraud protections
  - Account balances
  - Daily withdrawal limits—daily dollar amount and number of transactions limits
- Counterfeit magnetic stripe cards for a handful of accounts transact at X00 ATMs distributed globally within 12-24 hours
- High-dollar fraud attempts

International Organized Crime Operation

MasterCard

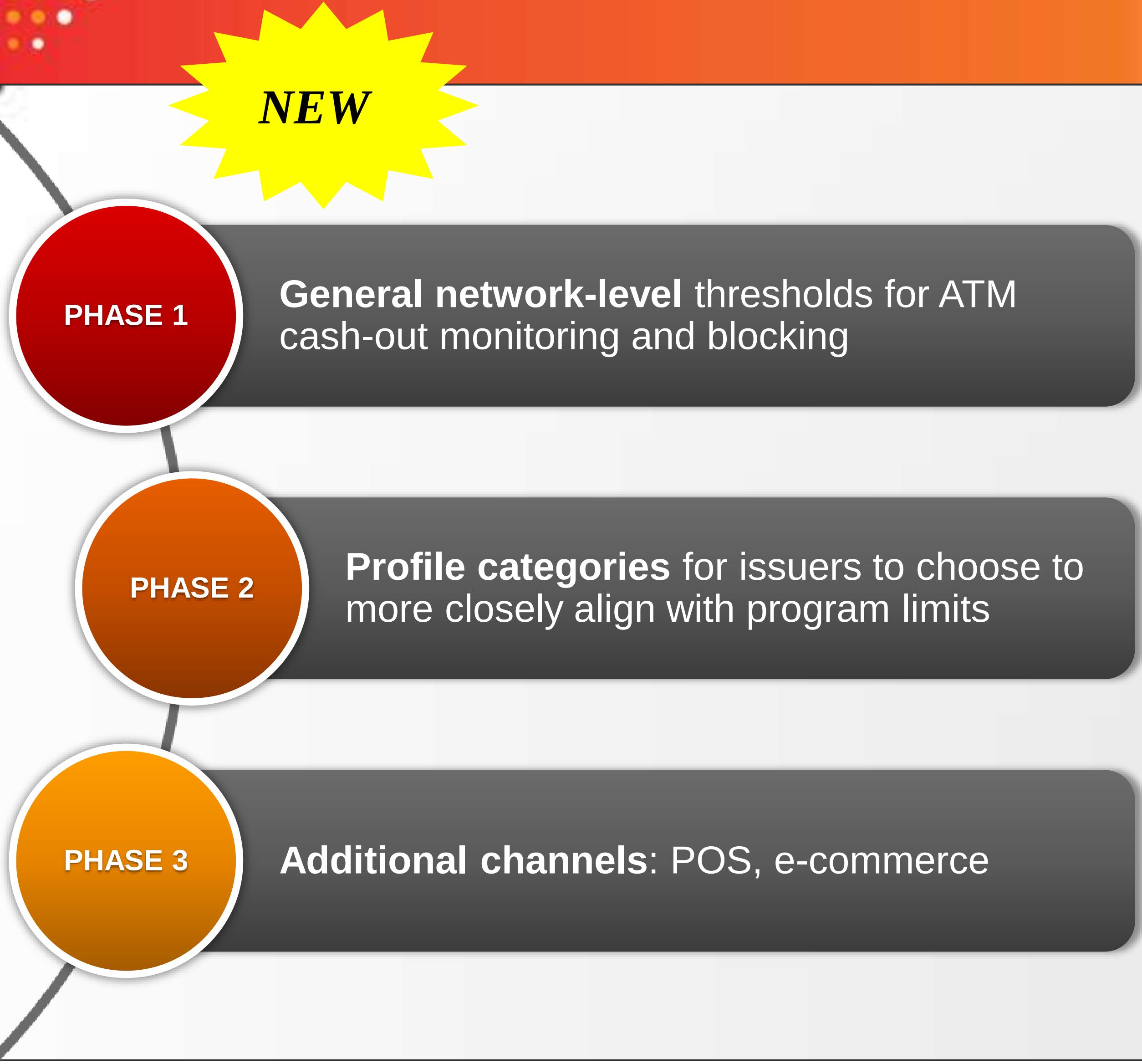
Profile of an ATM Cash-Out Attack



MasterCard Actions

- Global customer outreach
  - Series of customer briefing calls on a region basis concerning this attack vector and best practices to mitigate risk
  - Series of detailed security notices and operations bulletins concerning the threat, and data security best practices
  - Network level monitoring approach
- Advanced Training Opportunities:
  - Customized calls to global issuers and processing partners
  - Academy of Risk Management global webinars and on-demand training
  - Articles published in industry news periodicals
  - Global industry conference presentations

Prepaid Monitoring – Safety Net



NEW

PHASE 1

General network-level thresholds for ATM cash-out monitoring and blocking

PHASE 2

Profile categories for issuers to choose to more closely align with program limits

PHASE 3

Additional channels: POS, e-commerce

Effective March 6, MasterCard Prepaid Monitoring ***embedded in all Prepaid account ranges as a safety-net to help issuers avoid catastrophic fraud losses***

Network Level Monitoring, Card Level Blocking Minimizes Valid Cardholder Impact

MasterCard Network

"Our lights are always on"

If network-level thresholds are exceeded:

- Monitoring will identify specific primary account number impacted
- Issuer will be contacted
- PAN will be blocked for a period of 5 hours to allow issuer time to research and take appropriate measures

Leverage Flexibility to align with Your Prepaid Account Programs

MasterCard

ATM

1) Sum of cross border ATM transactions in 24 hours ≥ ______

2) Sum of all ATM transactions in 24 hours ≥ ______

3) Single ATM transaction ≥ ______

4) More than ______ approved ATM transactions in ______ minutes

5) ______ or more ATM transactions in 2 or more countries / states within ______ minutes.

POS

1) Sum of cross border POS transactions in 24 hours ≥ ______

2) Sum of all POS transactions in 24 hours ≥ ______

3) Single POS transaction ≥ ______

4) More than ______ approved POS transactions in ______ minutes

5) ______ or more POS transactions in 2 or more countries / states within ______ minutes.

Lessons Learned – Call to Action for Prepaid Issuers

- Enhance Payment/Fraud Control Monitoring in real-time:
  - Transaction velocity and limits
  - Geographical Location
  - Transaction Limits
  - Balance Inquiries
- Enhance Database Controls
  - Establish an internal, real-time alert system to trigger for:
    - Purse Value Updates
    - Get-PIN requests
    - Queries against database
    - Log retention expansion
  - ***Ensure senior manager(s) review alerts 24x7***

Lessons Learned – Call to Action for Prepaid Issuers

- Establish response and escalation protocols for alerts concerning purse value changes, get PIN requests, and excessive queries against database, to ensure all alarms are investigated immediately and resolved quickly
- Notify MasterCard Account Data Compromise team immediately upon detection of event
  - Immediately retain a PCI SSC approved PCI Forensic Investigator (PFI)
  - Notify appropriate law enforcement agency(ies)
  - Ensure other customers are not affected by the intrusion
  - Conduct end-to-end post event review to document process and to ensure no subsequent occurrence

Lessons Learned – Call to Action for Prepaid Issuers

- Ensure ongoing Payment Card Industry Data Security Standard (PCI DSS) compliance by revisiting scope of PCI assessment through revalidation of security controls which criminals target
- *Data security, real-time payment/fraud controls, and reviewing system change alerts in real time are the keys to preventing an ATM Cash Out*

Data Security Best Practices

- Require two-factor authentication for all administrative remote access applications
- Review firewall rules across their network
- Require proper network segmentation
- Upgrade or remove legacy systems
- Review and restrict access to sensitive applications

Visit our new website at www.mastercard.com/arm

MasterCard Academy of Risk Management

Through its global conferences, courses, online resources and customizable training sessions, MasterCard provides the latest insights, data and best practices to help risk professionals prevent and manage fraud.

INNOVATE. COLLABORATE. EDUCATE.

The MasterCard Academy of Risk Management (ARM) is the go-to resource for today's payment card fraud and risk professional. Through our global conferences, courses, workshops, online resources and customizable training sessions, MasterCard provides the latest insights, data and cutting-edge resources to help organizations and industry professionals mitigate risk and optimize performance.

View the 2014 Calendar

Join Our Community › LinkedIn

MAY 2014

CONFERENCES ›

▸ Learn More

WORKSHOPS ›

▸ Learn More

ONLINE RESOURCES ›

▸ Learn More

ARM EDUCATION SERIES ›

▸ Learn More

AMERICAS | ASIA PACIFIC | EUROPE | MIDDLE EAST & AFRICA

REGISTER

LEARN MORE

Join our online community for news, updates and the latest resources from the MasterCard Academy of Risk Management

Join Our Community › LinkedIn

MasterCard
Academy of Risk Management

2014 MasterCard Global Risk Conference: *Asia Pacific*

Academy of Risk Management | Innovate. Collaborate. Educate.