Melvin Chew
Customer Security & Risk Services
Franchise Integrity, Law & Franchise Integrity
MasterCard Worldwide (Asia/Pacific)
November 27, 2014

Payment Card Fraud and Security

Payment System Forum and Exhibition 2014
Sasana Kijang, Kuala Lumpur

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.

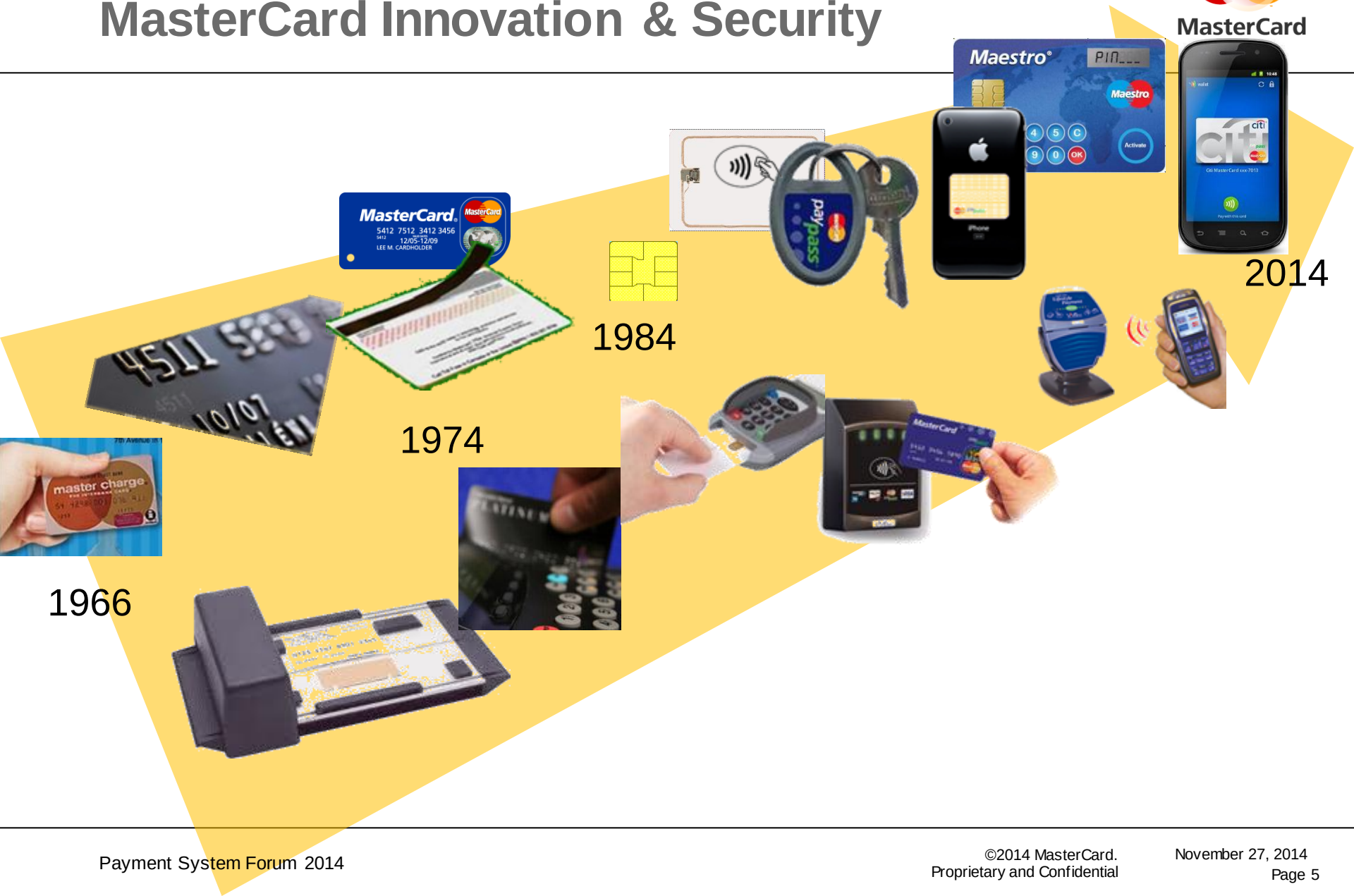
Information in this presentation or in any report or deliverable provided by MasterCard in connection herewith relating to the projected impact on your financial performance, as well as the results that you may expect generally are estimates only. No assurances are given that any of these projections, 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.

Agenda

- Payment Card Security Landscape
- Fraud Prevention Tips
- Acceptance Best Practices

Payment Card Security Landscape

The Card – MasterCard Innovation & Security



The Nature of Fraud

- Fraud typically begins after the theft of the physical credit card or the compromise of data associated with the account (i.e., name of cardholder, account number, expiration date, verification code)
- Often times, the cardholder is unaware that a compromise has occurred. A card remains usable until the issuer has been notified and takes action to block or monitor.
- Banks possess sophisticated fraud detection and monitoring systems
- Payment Card fraud is at historically low levels in the Asia/Pacific

Types of Payment Card Fraud

- Card Present
  - Lost/ Stolen
  - Never Received Issue
  - Fraudulent Application
  - Counterfeit
  - Account Takeover
  - Multiple Imprints
- Card Not Present
  - Card, Cardholder, or Merchant are not present where the transaction takes place
  - Mail Order/Telephone Order (MOTO)
  - Card Activated Terminal (CAT)
  - E-commerce
  - Recurring Payments

Comparing Genuine & Counterfeit MasterCard's Holograms

Genuine

Counterfeit

MasterCard "Micro Globes" Hologram Specifications

MasterCard Text

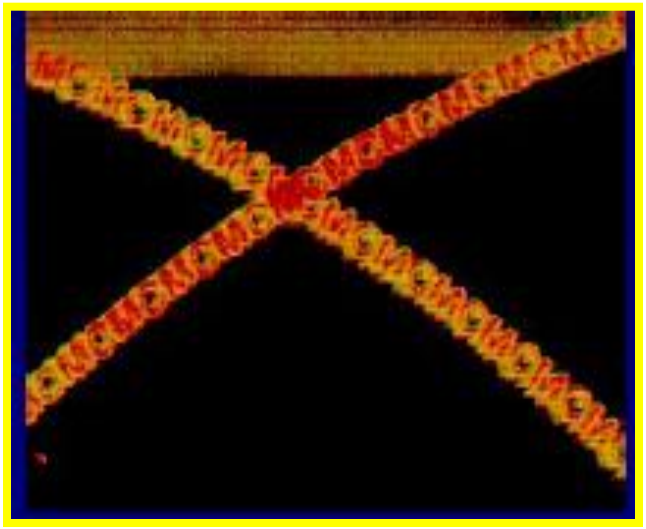
in 2 colors

Micro-Engraved

Rings of "MC"

Land Masses in

3D Spheres



MasterCard

Fraud Prevention Tips

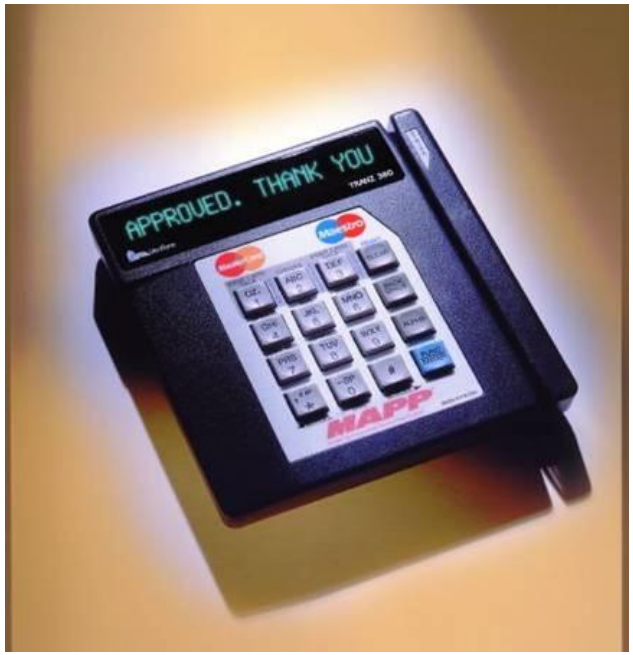
Startup – Understand the Exposure

What are the Risks.....

- Fraud Risk
- Use stolen cards
- Falsely claim non-receipt of goods
- Get into Merchant systems and create credits (refunds) to their own card numbers
- Cyber theft
  - Steal card account data in transmission or from Merchant's or Service Provider's database

Completing an Electronic Transaction

- There are five steps to take to complete an electronic transaction:
  1. Dip/ Slide the card
  2. Compare account numbers
  3. Request authorization
  4. Complete the sales draft
  5. Obtain and compare signatures



Account Number Verification

- Compare account numbers displayed on the terminal or printed on the sales draft (Last Four Digits) to the embossed number on the customer's card
  - If the numbers match, enter the amount of the transaction into the terminal and request authorization
  - If the numbers do not match, call the authorization center and say, "Code 10." Follow the instructions the operator gives over the phone.

Potential Responses

- When you ask for authorization, you will receive one of four messages:

  1. Approve
  2. Decline
  3. Call or call center
  4. Pickup

Four Steps to Avoid Payment Card Fraud

1. Hold the card
2. Review card security features
3. Obtain authorization
4. Compare signatures

10 Tips to Help CNP Merchants Spot & Stop Fraud

1. Is the sale too easy? Is the customer disinterested in the price or details of the goods?

   Are they a new customer?

2. Are the goods high-value or easily resalable?

3. Is the sale excessively high in comparison with your usual orders? Is the customer ordering many different items? Do they seem unlike your usual customer?

4. Is the customer providing details of someone else's card e.g., that of a client or family member?

5. Is the customer reluctant to give a landline contact phone number – are they only prepared to give a mobile number?

10 Tips to Help CNP Merchants Spot & Stop Fraud (cont.)

6. Does the address provided seem suspicious? Has the delivery address been used before with different customer details? Is the delivery or contact address overseas?
7. Is the customer being prompted by a third party whilst on the phone?
8. Is the customer attempting to use more than one card in order to split the value of the sale?
9. Does the customer seem to lack knowledge of their account?
10. Does the customer seem to have a problem remembering their home address or phone number? Does the customer sound as if they are referring to notes?

Acceptance Best Practices

Best Acceptance Practices

Best Practices of Accepting Payment cards Including...

- Don't
  - Assign a minimum or maximum purchase amount
  - Add a surcharge or fee
  - Splitting authorization amount for the same card account
  - Restrict payment card use (for a sale or discounted item)
  - Use a payment card to guarantee a check
  - List a cardholder's personal information on a payment card sales slip
  - Deny a purchase because a cardholder refuses to provide additional identification such as a phone number, address, social security number or driver's license

Declining a Payment Card

Never Honor a Payment card When…

- The customer does not have the actual payment card
- The card appears to have been altered or tampered
- Authorization is declined or you're told to pick up the card
- The signatures do not match

Chargeback

A Chargeback Occurs When...

- A cardholder disputes a charge or when proper payment card acceptance and authorization procedures were not followed, the acquirer notifies the merchant and debits the amount from the merchant's account.

Top 10 Reasons For Chargebacks

1. Merchant didn't provide a copy of sales slip to their acquirer within the time frame
2. Legitimate cardholder was not the person who made the mail / telephone or e-commerce order transaction
3. A single transaction was processed more than once
4. Authorization was not obtained for a transaction
5. A credit voucher wasn't processed

Top 10 Reasons For Chargebacks (contd.)

6. A card imprint (whether electronically by swiping the card through the POS terminal or manually by imprinting the card) was not obtained for a face-to-face sale
7. The account number from the swipe didn't match the account number on the front of the card
8. Merchandise or services were not provided to the cardholder
9. Merchant accepted an expired card or a card used before the effective date and didn't receive proper authorization
10. The sales slip was altered or not signed by the cardholder

Payment Card Fraud Prevention Training

The training tool includes two modules:

- Spotting Fraud in Your Store
- Spotting Card Not Present Fraud

http://www.mastercard.com/us/merchant/security/index.html

Payment Card Fraud Prevention Training

- **Other features include:**
  - An animated introduction to MasterCard's Payment System Integrity within the Heart of Commerce™ campaign against fraud
  - A resource library of useful publications
  - Merchant fact sheets on MasterCard security features and programs
  - A link to MasterCard's Payment Card Industry (PCI) Merchant Education Webinar Series

Welcome

- One counterfeit card can result in thousands of dollars lost
- You can learn to detect fraud
- You can make a difference

Forward

Welcome

- One fraudulent card-not-present transaction can result in thousands of dollars in losses
- You can better prepare yourself to detect fraud
- You can make a difference

Forward


MasterCard
Worldwide
Certificate of Achievement
Melvin Chew
MasterCard
Has successfully completed
Payment Card Fraud Prevention Training
for the Card-Not-Present Environment
MasterCard
Worldwide