In a networked globalised world dominated largely by technology, cyber security risks have become more complex, volatile and pervasive. The contributing factors are:

- Accessibility and complexity have overwhelmed systems security.
- Systems are developed with insufficient controls and security testing.
- More identity and financial information is available online.
- Cyber criminals are more sophisticated and more organized.
- Computer security is not keeping pace with the intensity, magnitude, proliferation and sophistication of internal and external attacks.
CREDIT/DEBIT CARD FRAUD

WHY IS PAYMENT CARD FRAUD SO PREVALENT, SO PERSISTENT AND SO INTRACTABLE?
SINGAPORE CREDIT CARD FRAUD

2007: $5.1 mil
2008: $4.7 mil

9% decrease

*Billings: 2007 $17 billion; 3 basis points fraud loss
*Billings: 2008 $20 billion; 2 basis points fraud loss

* excluding bank fees, interest charges and cash withdrawals.
2008 CREDIT CARD FRAUD $4.7m

Y2007 $5.1m

- Counterfeit: 63%
- Lost/Stolen: 6%
- CNP: 20%
- Others: 11%
## SINGAPORE DEBIT CARD FRAUD

<table>
<thead>
<tr>
<th></th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Billings</strong>* ($million)</td>
<td>550</td>
<td>730</td>
<td>900</td>
<td>1,210</td>
<td>1,480</td>
</tr>
<tr>
<td><strong>Fraud loss</strong> ($thousand)</td>
<td>280</td>
<td>300</td>
<td>170</td>
<td>260</td>
<td>440</td>
</tr>
<tr>
<td><strong>Fraud loss basis points</strong></td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

* Excluding fees, interest charges, withdrawals and advances
## CREDIT & DEBIT CARD FRAUD LOSS

<table>
<thead>
<tr>
<th></th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>United Kingdom</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No of cards issued (million)</td>
<td>140</td>
<td>140</td>
<td>140</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td>Billings (£ billion)</td>
<td>392</td>
<td>449</td>
<td>453</td>
<td>508</td>
<td></td>
</tr>
<tr>
<td>Fraud loss (£ million)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card-not-present</td>
<td>183</td>
<td>213</td>
<td>291</td>
<td>328</td>
<td>6.5</td>
</tr>
<tr>
<td>Counterfeit</td>
<td>97</td>
<td>99</td>
<td>144</td>
<td>170</td>
<td>3.4</td>
</tr>
<tr>
<td>Lost/ Stolen</td>
<td>89</td>
<td>69</td>
<td>56</td>
<td>54</td>
<td>1.0</td>
</tr>
<tr>
<td>Others</td>
<td>70</td>
<td>46</td>
<td>44</td>
<td>58</td>
<td>1.1</td>
</tr>
<tr>
<td><strong>Total fraud loss (£ million)</strong></td>
<td>439</td>
<td>427</td>
<td>535</td>
<td>610</td>
<td>12.0</td>
</tr>
<tr>
<td><strong>Fraud loss basis points</strong></td>
<td>11.2</td>
<td>9.5</td>
<td>11.8</td>
<td>12.0</td>
<td></td>
</tr>
</tbody>
</table>
## Total Fraud Loss Comparison

<table>
<thead>
<tr>
<th></th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UNITED KINGDOM</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No of cards issued (million)</td>
<td>140</td>
<td>150</td>
</tr>
<tr>
<td>Total fraud loss in (S$ million)</td>
<td>1,550</td>
<td>1,770</td>
</tr>
<tr>
<td><strong>SINGAPORE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No of cards issued (million)</td>
<td>6.7</td>
<td>7.3</td>
</tr>
<tr>
<td>Total fraud loss (S$ million)</td>
<td>5.4</td>
<td>5.1</td>
</tr>
</tbody>
</table>

Total fraud loss ratio (SG:UK) 1:14 1:17

Exchange rate:
2007 and 2008: 1 £ = 2.9 SGD
LARGEST CREDIT CARD HEIST IN SOUTH EAST ASIA

24 - 30 January 2008
Public tip-off leading to an arrest of 8 suspects involved in a large scale drug distribution and credit card fraud.

1 - 6 February 2008
More were arrested. Laptops and storage devices containing the data of over two million credit cards were uncovered.

11 February 2008
The Indonesian police made a press statement.

How did the perpetrators manage to harvest so much card data?
<table>
<thead>
<tr>
<th>Merchants / Payment SP compromised</th>
<th>Millions of accounts / cards hacked or stolen</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009 Heartland</td>
<td>100</td>
</tr>
<tr>
<td>2008 RBS WorldPay</td>
<td>2</td>
</tr>
<tr>
<td>2008 Hannaford</td>
<td>4</td>
</tr>
<tr>
<td>2007 TJX</td>
<td>46</td>
</tr>
<tr>
<td>2005 CardSystems</td>
<td>40</td>
</tr>
<tr>
<td>2005 BJ Wholesale</td>
<td>8</td>
</tr>
</tbody>
</table>

Heartland announced on 27 Jan that it would be creating a new department that will be “dedicated exclusively to the development of end-to-end encryption.”
US$9m, 130 ATMS, 49 CITIES IN 30 MINS

RBS WorldPay Press Release

• 1.5 million card holders affected
• 1.1 million social security numbers accessed
• Actual fraud committed on 100 cards – Nov 2008

Cities included: Atlanta, Chicago, New York, Montreal, Moscow and Hong Kong

WANTED BY FBI
POSSIBLE ATM CARD FRAUD
UNSUBS

 THE ABOVE IMAGES WERE TAKEN AT THE FOLLOWING LOCATIONS IN CHICAGO, IL.

AMERICAN CHARTERED BANK
1020 WEST RANDOLPH STREET

AMCORE BANK
1033 WEST VAN BUREN

NATIONAL CITY BANK
3340 WEST ROOSEVELT ROAD

UNKNOWN SUSPECTS ARE WANTED IN A POSSIBLE ATM CARD SCAM.
IF YOU HAVE ANY INFORMATION CONCERNING THE IDENTITY OF THE ABOVE INDIVIDUALS, PLEASE CONTACT:
SPECIAL AGENT KIMBERLY CHRISTY
(404) 679-6235
The hearing will examine the effectiveness of the Payment Card Industry’s Data Security Standards (PCI DSS). These standards were established to reduce the number and size of data breaches, the proceeds of which may be used to fund terrorist activities.
Were Heartland and RBS WorldPay in compliance with PCI DSS at the time of their security breach?

How effective is PCI DSS?

How can PCI DSS be improved?
SECURITY COUNTERMEASURES

1. CHIP & PIN (DYNAMIC AUTHENTICATION)  
   ELIMINATE MAGNETIC STRIPE

2. ONE-TIME-PASSWORDS (OTP) FOR CNP TXN

3. DATA ENCRYPTION – NETWORK END-TO-END  
   AND STORAGE

4. SOURCE CODE REVIEW / SECURITY TESTING

5. VULNERABILITY / PENETRATION TESTING

6. SYSTEM ACCESS CONTROLS / LOGGING
PROGNOSIS - MORE ATTACKS

PAYMENT CARD SCHEMES

ATM NETWORKS / iBANKING

WHOLESALE PAYMENT SYSTEMS

STOCK EXCHANGES

INTERNAL SABOTAGE
Q & A

THANK YOU