HONG KONG MONETARY AUTHORITY

Credit card operation and the recent CardSystems incident

4 July 2005

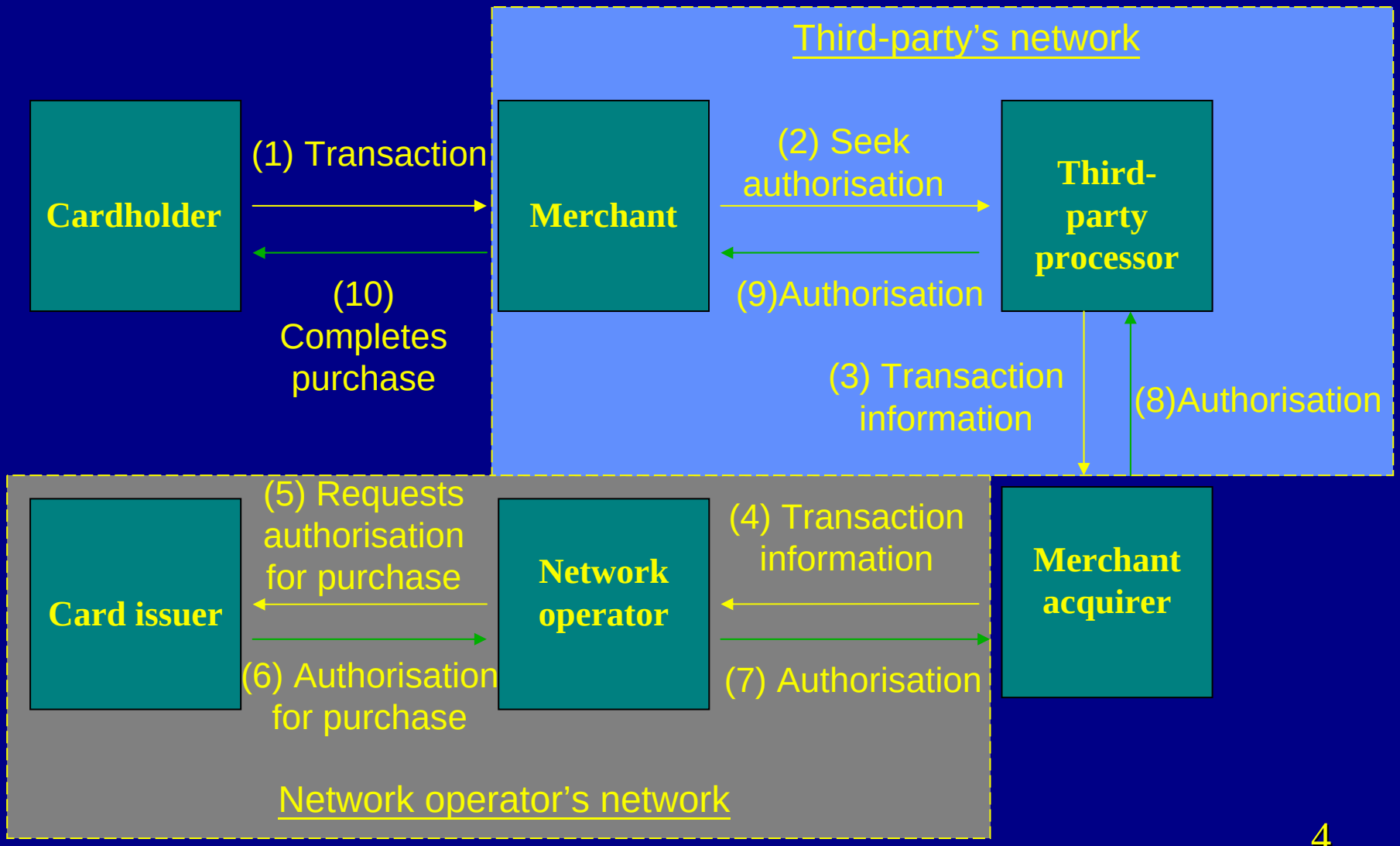
CONTENT

- Credit card system overview
- The CardSystems incident
- Impact on credit cardholders in Hong Kong
- Liability for financial loss
- Follow-up actions by the HKMA
  - Impact assessment
  - Risk evaluation

CREDIT CARD SYSTEM OVERVIEW

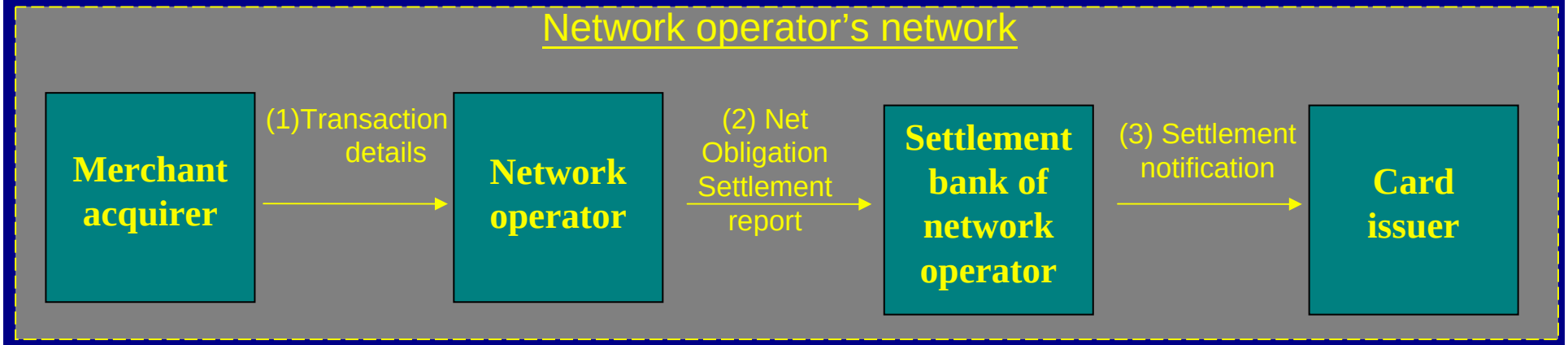
- Network operators (Visa, MasterCard, American Express, Diners, JCB, China UnionPay)
- Card issuers (mainly banks)
- Merchant acquirers (mainly banks)
- Merchants
- Cardholders
- Third party service providers
  - Third-party processors
  - IT processors

AUTHORISATION FLOW

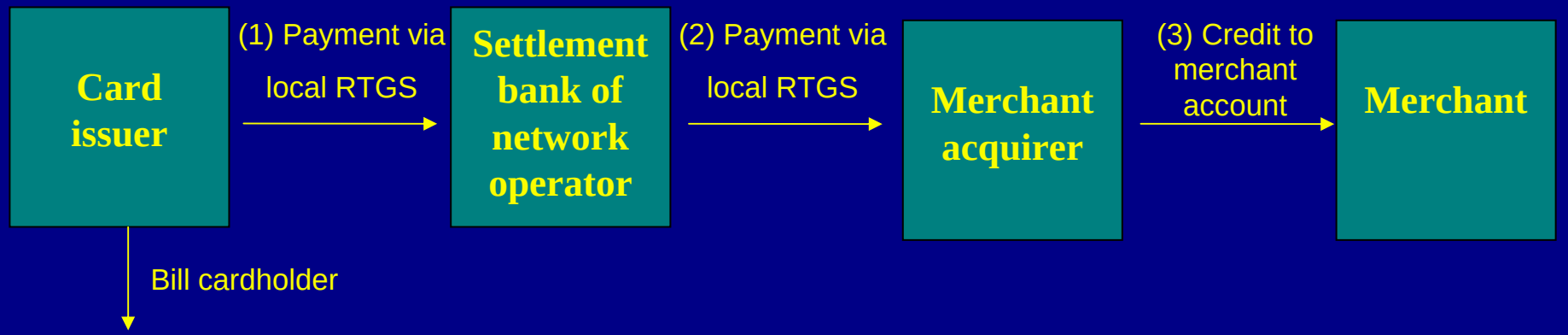


CLEARING AND SETTLEMENT FLOW

Clearing (usually within 1 day)



Settlement (usually within 3 days)



THE CARDSYSTEMS INCIDENT

- CardSystems is a third-party processor providing authorisation and validation processes on behalf of the merchant/merchant acquirer
- Cardholder information stored after completion of authorisation and system hacked
- Compromised data could be used for fraudulent transactions

THE CARDSYSTEMS INCIDENT

- CardSystems reportedly breached the security standards set by the network operators:
  - NOT to retain sensitive cardholder information after completion of authorisation process
  - to encrypt the information should such information be retained for special business, legal or regulatory purposes

IMPACT ON CARDHOLERS IN HK

- Cardholders in HK may be affected if
  - purchase retail outlets in the US (at the point-of-sale or through Internet); and
  - retail outlets in the US submit transaction information to merchant acquirer through CardSystems
- About 12,000 credit cards issued by AIs in Hong Kong potentially affected
- No financial loss to cardholders in this case

LIABILITY FOR FINANCIAL LOSS

Card issuers will bear the full loss incurred:

- **when faults have occurred in the terminals, or other systems used, which cause cardholders to suffer direct loss (section 30.1(c) of the Code of Banking Practice); and**
- **when transactions are made through the use of counterfeit cards (section 30.1(d)).**

FOLLOW-UP ACTIONS OF THE HKMA - IMPACT ASSESSMENT

- AIs contacted most of the potentially affected cardholders for card replacement
- For cardholders who cannot be contacted, transactions conducted through their cards are monitored closely

FOLLOW-UP ACTIONS OF THE HKMA - EVALUATION OF RISK

- Risk of occurrence of similar incident in Hong Kong is relatively low
  - **Comprehensive guidance issued to AIs, including:**
    - **Outsourcing**
    - **Technology risk management**
    - **Supervision of Internet banking**
  - **Prior approval from the HKMA before entering into an outsourcing contract**
  - **Submission of annual IT controls self-assessment reports to the HKMA by all major AIs**
- HKMA's specialist IT on-site examinations cover the review of IT controls of AIs and their service providers

FOLLOW-UP ACTIONS OF THE HKMA - EVALUATION OF RISK AND STRENGTHENING OF SECURITY SYSTEM

- Letters issued to AIs and credit card companies, and other companies handling credit card/debit card data:
  - **Requesting AIs to re-assess the adequacy and effectiveness of controls over customer data security, retention and confidentiality (including AIs and their service providers)**
  - **Requesting credit card companies, consumer credit bureau and debit card operators to assess the security controls over internal and outsourced processing of consumer and transaction data and to strengthen their companies' security system where necessary**
  - **Liaising with Privacy Commissioner's Office**

End of Presentation