Legislative Council Panel on Financial Affairs

Credit Card Data Security Breach Incident in the United States and its Impact on Hong Kong Consumers

Submitted by Visa Hong Kong

29 June 2005

Purpose

1. This paper provides information on the background of Visa's payment system, the data security breach incident in the United States reported in June 2005 and security measures taken by Visa to protect cardholders in Hong Kong.

About Visa International

2. Visa is the world's leading payment brand and Visa branded cards are widely accepted at more than 24 million merchant locations in over 150 countries and territories around the world. Visa International is a membership association owned by more than 21,000 financial institutions ("members") globally.

3. Visa facilitates the processing of payment transactions for its members, providing a "highway" through which informational and financial transactions can travel quickly and smoothly. Visa does not issue cards nor does it directly offer services to merchants. Since it is Visa's members who enter into contracts with cardholders and merchants, Visa does not receive fees from either cardholders or merchants. Visa's operational costs are funded by its members in the form of processing fees, service fees and other types of funding. Visa's revenue is intended to cover its expenses and investment in its networks and services, and it does not seek to generate a profit.

4. In Hong Kong, there are approximately 7.3 million Visa cards in circulation issued by 22 Visa member banks.

About the Payment System

5. A typical Visa transaction involves four parties**: a cardholder, a merchant, an issuing bank and an acquiring bank.**

    a. A **cardholder** is the person who has been issued a Visa card or other Visa-branded payment product.
    b. A **merchant** is a store, restaurant, online retailer, hotel, airline, or one of the countless other locations that accepts Visa as payment.
    c. An **issuer**, or **issuing bank**, is a financial institution that provides Visa cards or other Visa-branded products to cardholders.
    d. An **acquirer,** or **acquiring bank,** is a financial institution that signs up merchants to accept Visa payments, and sees that those merchants get paid for the Visa transactions they accept.

6. Consider the example of a cardholder who buys a pair of shoes with a Visa card. When the cardholder goes to buy the shoes, the **merchant** (the shoe store) submits the transaction details, including the cardholder's credit card information, to the **acquirer** for approval.

7. The **acquirer** then sends the transaction details to the **issuer** via VisaNet, Visa's worldwide network to switch and settle payment transactions, for authorization of the purchase. After receiving an authorization from the **issuer** via VisaNet, the **acquirer** sends a confirmation of the transaction to the **merchant**, who then gives the shoes to the cardholder. All these messages happen in a few seconds through worldwide electronic systems.

8. Visa later settles the transaction amount between **issuer** and **acquirer**. The **acquirer** then pays the shoe store and the cardholder will later be billed the retail price by the **issuer**. The Visa system assures cardholders that their cards will be accepted wherever **merchants** display the VISA acceptance mark, and assures **merchants** that payment to them will be guaranteed, in terms of their contract with their **acquiring bank**, as long as they follow the rules for accepting cards (such as obtaining authorizations).

The US Security Breach

9. A US-based third-party payment card processor, Card Systems Solutions Inc, operating primarily on behalf of a number of US-based acquirers, experienced a data security breach resulting in the compromise of payment card account information. The processor processes for all major payment brands.

10. Visa USA is working with the payment card processor, law enforcement and the affected member financial institutions to monitor and help prevent Visa-related fraud. Visa continues to work with financial institutions and law enforcement to protect cardholders and investigate this breach.

11. Approximately 40 million cards across all payment brands were involved. The vast majority of these accounts are US-issued, including more than 20 million out of the 22 million Visa accounts impacted. Around 205,000 accounts at risk were Visa cards issued by banks in Asia Pacific, about 92 percent of which did not suffer a loss of sensitive cardholder data needed for the production of counterfeit cards i.e. the full magnetic stripe data was not compromised.

12. Full details of the compromised accounts were made available to Visa Asia Pacific on Sunday, 19 June 2005 and to Hong Kong on Monday, 20 June 2005. Visa provided issuing banks in Asia Pacific with full details of the accounts involved within two days of receiving the data so they could monitor the accounts independently and if warranted, cancel and reissue cards. Banks are taking appropriate action with their individual cardholders.

13. Visa respected law enforcement's request not to compromise the confidential nature of the investigation by going public with this information as open communication of the situation may have compromised the integrity of the investigation.

14. Beyond this, we cannot provide details of the data breach at this time because of the sensitive nature of the ongoing forensic and criminal investigations. Further details will be provided to interested parties as soon as the investigations have been completed.

Implications for Hong Kong Cardholders and Actions Taken by Visa to Protect the Public

15. At the time of the security breach, information pertaining to Hong Kong cardholders who had purchased goods or services from merchants whose transaction data was processed by this particular processor, could have been compromised. These included data of cardholders who had shopped in the United States, who used their cards to purchases goods from U.S.-based websites, or made transactions by mail order or the telephone.

16. Visa identified 9,122 accounts in Hong Kong that were potentially compromised by this breach and therefore considered "at risk". Visa provided the issuing banks with account details so that they can monitor the accounts independently and, if warranted, cancel and reissue cards. The term "account at risk" is used in the risk management community to describe accounts that require heightened monitoring from a fraud risk perspective. It should be noted that 92 percent of the compromised

information of Hong Kong cardholders did not contain the full magnetic stripe information needed to create counterfeit cards. Even for the remaining 8 percent of the accounts, there is not necessarily a link between accounts at risk and subsequent fraud, because of the fraud detection systems and processes installed by Visa and the issuers to monitor fraud and to help stop it from happening.

17. It is the practice of Visa's member banks in Hong Kong to absorb the cost for any fraudulent transactions made on accounts identified as "at risk" reported by Visa to issuers.

18. Visa has also reached out to the media and addressed public concerns in Hong Kong through a number of channels – speaking directly to media, issuing statements and providing general information by posting "The Facts of the Case and Cardholder Tips" on its website www.visa.com.hk. Visa has worked with the media to inform cardholders of the situation, reassure them that they are not liable for fraudulent charges, advise them on measures they can take to help prevent fraud, and explain what is being done by Visa and the issuing banks in their fight against fraud. Visa is also sending out cardholder advice through its member banks on how consumers can help keep their cards secure. As always, Visa encourages cardholders to monitor their accounts continually through regular statements, Internet account access and to notify their issuing banks of any unusual activity. Visa Asia Pacific's own communication activities support those undertaken by its issuers.

19. Visa's members continue to monitor the compromised accounts to establish the potential amount of fraud that actually occurred. As a matter of standard operating procedure, Visa's members also report fraudulent transactions to Visa.
    - Visa is fully engaged with law enforcement, banks and other payment card associations; and
    - Once the full facts of the case are available, Visa and its members will incorporate learnings from this case to strengthen further their fraud monitoring and prevention activities.

Visa's Security Programs

20. Visa and its members undertake extensive measures to monitor and protect the Visa system and engage in cooperative efforts to deal quickly with any breach.

21. Fraud within the global Visa system is at an all-time low of just 7 cents per $100 transacted. In Asia Pacific, the rate is less than half the global rate at 3 cents per $100 transaction. Having said that, Visa continues to review its data security and protection practices to derive further improvement to its system and thereby increased security for its members and cardholders.

22. **Account Information Security (AIS)**: Within the payment card industry, entities that handle cardholder information have a responsibility to protect it. Visa is committed to working with members and their agents to ensure that customer information is secure. This is why Visa was the first to introduce its AIS data security requirements for merchants, processors, Internet payment service providers and other payment service providers (collectively here called processors).

23. Visa requires that its members ensure all merchants and processors participating in the Visa payment system that store, process or transmit Visa cardholder account and/or transaction information meet the minimum security requirements as defined by the AIS standard.

24. Those security requirements include standards for data encryption, the timely adoption of security updates and the destruction of data that is not needed. The two most important principles of the program are, 'Don't store the data unless you absolutely need it,' and 'If you need to store the data, encrypt it.'

25. As part of the AIS program, Visa asked its members to certify that about 100 of Asia Pacific's biggest processors have completed their AIS validation tasks in the past 12 months. Currently five processors based in Hong Kong have undergone the necessary compliance validation tasks (self-assessment of security setup and Internet vulnerability scanning). The compliance validation tasks have to be completed annually. Visa will work with members in Hong Kong and the region to identify additional existing or new processors for which Visa will request certificates of compliance.

26. However, compliance with AIS is an ongoing process. A company which has validated its compliance must maintain this standard by ensuring all policies and procedural controls are in place and Visa Asia Pacific will continue to request its members to certify that processors meet this requirement annually. Visa Asia Pacific continues to educate and communicate to the processing and merchant community the requirements, including the benefits of AIS compliance. The AIS program is regularly subject to review and updates by the Visa Asia Pacific Board, the Audit & Risk Committee of the Visa Asia Pacific Board and various advisory groups representing Visa members.

27. **EMV Chip**: Visa has established a global standard, EMV (Europay, Mastercard, Visa), for chip-based debit and credit transactions with Europay and MasterCard. The EMV standard ensures security and global interoperability so that Visa cards can continue to be accepted everywhere. EMV chip cards offer the best long-term solution to the problem of counterfeit fraud.

28. More importantly, Visa is leading the industry in implementing specific security features that further protect consumers. These include PIN protection and chip cards that carry small integrated circuit chips that store account information and secret data. The secret data is used to authenticate the chip if the card is used in a specially-equipped chip terminal. It is very difficult to create a counterfeit chip from transaction data created during a chip transaction. In a mature chip acceptance environment, this would greatly reduce the impact of data compromise.

29. Visa also continues to work towards the establishment of a comprehensive EMV chip card infrastructure in the Asia Pacific region. This represents a major undertaking for the cards industry, but Visa is seeking to ensure that the majority of payment infrastructure is ready in most countries by 2008.

30. Visa's commitment to EMV chip migration has seen national programs underway in four Asia Pacific markets. In addition to these national programs, many members are themselves upgrading point-of-sale and transaction acquiring systems to provide a greater level of protection.

31. As of March 2005, Visa has close to 33 million EMV-compliant chip cards and more than 743,000 EMV terminals deployed in the region. In Hong Kong, Visa members have issued around 220,000 EMV chip cards and major banks are either upgrading their systems for EMV chip migration or are in the project-planning stage.

32. **Verified by Visa***:* Verified by Visa provides Visa cardholders with an additional level of online protection when shopping at participating Internet merchants. It utilizes authentication procedures to help reduce merchant and financial institution losses from unauthorized card usage. To date, more than 56,000 merchants and 15 million cardholders have been activated in the service.

33. In the recent security breach situation, criminals possessing compromised account information would not be able to use the account to make Internet purchases when dealing with a participating Verified by Visa merchant because the buyer would be asked for a private password.

Conclusion

34. The battle against fraudulent activity remains a major long-term challenge. Visa is working with law enforcement and the affected member financial institutions to monitor and prevent fraud. Visa will continue to work with financial institutions and law enforcement to protect cardholders and investigate this breach. As always, Visa encourages cardholders to monitor continually their accounts through regular statements, Internet account access and to notify their issuing bank of any unusual activity.

35. Fraud within the global Visa system is at an all time low of just 7 cents out of every $100 transacted. In Asia Pacific, this figure is even lower, at 3 cents in every $100. To remain one step ahead of criminals, Visa and its members are continuously enhancing their security programs through improving technologies, collaboration across the industry and with law enforcement, and through consumer education and awareness. The industry's shared goal is to limit fraud, and when it does occur, to minimize the impact.