MasterCard International

LC Paper No. CB(1)1953/04-05(01)

29 June 2005

MasterCard Response:
Panel on Financial Affairs
Hong Kong SAR Legislative Council

On Friday, June 17 (US time), MasterCard announced that it had identified a significant security breach at a third-party processor, CardSystems Solutions, Inc. based in Tucson, Arizona. A third party processor is an entity that processes payment card data on behalf of merchant bank acquirers and merchants. Using our fraud detection tools, our team of experts identified the breach in cooperation with reports from issuers and others. We subsequently alerted issuers and the public.

We recognize that our announcement has generated significant media attention and some contention. For this reason and because of the importance of the issues involved, we believe you should be fully aware of the facts and circumstances leading up to our decision to act as we did. It is important to note that MasterCard first received the list of affected account numbers from CardSystems Thursday, June 16, 2005 (US time). Our communication to all affected banks began the following day, Friday, June 17, and was completed late on Saturday, June 18.

Background

Account numbers used in transactions at merchants that processed through CardSystems between August 1, 2004, and May 27, 2005, were exposed to possible compromise as a result of a security breach. We initially believed that 13.9 million MasterCard branded accounts globally may have been at risk. However, based on ongoing examinations of the account numbers sent to us by CardSystems, we now believe approximately 10.1 million of the possibly compromised accounts worldwide are MasterCard-branded cards. The data retrieved from CardSystems revealed that a potential maximum number of 10,113 accounts could have been impacted in Hong Kong. However the data maintained by CardSystems contained numerous duplicate and invalid account numbers. And these numbers are expected to be significantly reduced.

The impact on Hong Kong cardholders is minimal and we have already ascertained that based on the HKMA's guidelines and local banks' liability policy, cardholders will not be held responsible for unauthorized card transactions. We should highlight that while members may decide to block and reissue cards, this does not however imply that cards have been used for fraudulent purposes.

CardSystems had captured and stored magnetic stripe data and card validation codes (CVC 2). Retention of this account information is in violation of MasterCard's security rules and CardSystems is no longer storing this information. The company is now in the process of securing full compliance with our rules. Had the processor been in compliance, this breach would not have occurred.

Actions Taken

By Thursday, June 16 (US time), the MasterCard Fraud Management team learned that the forensic investigation had confirmed that a breach occurred and that the risk was significant. Based on this information, we determined it was imperative that MasterCard obtain the account numbers and disseminate them to issuers immediately. In the United States and elsewhere, there is significant regulatory and legislative scrutiny on how businesses protect consumer data and whether or not they alert the public of a data compromise. While it is our practice to notify issuers of compromised accounts, in such an environment it became imperative to also notify the public of this significant breach as quickly as possible.

The Federal Bureau of Investigation is investigating this crime, and regulators in the United States are reviewing CardSystems' security protocols.

Across Asia/Pacific, MasterCard has been working closely with our member financial institutions to assess the situation in terms of compromised cards. Member financial institutions will, based on their own investigations, determine the number of cards they wish to monitor or block and reissue.

In Hong Kong, MasterCard has undertaken a program to inform cardholders. This includes both media relations and working with our member financial institutions via their card call centers.

Although security breaches and credit card fraud are a continual challenge to the payment industry, MasterCard continues to stay vigilant and work with our member financial institutions to monitor any unusual transactions or card activity, and take the necessary action. MasterCard also has a number of fraud detection and prevention initiatives in place to help members and merchants fight fraud such as the Site Data Protection (SDP) program and mandatory onsite reviews and inspections.

MasterCard is working on a program which will alert the regulatory authorities of a security breach or potential fraud situation in the markets across Asia/Pacific. This advisory will be disseminated at the same time as our advisory to the members to inform them of potential fraud or compromised accounts. We hope to have this regulatory advisory system in place by end July 2005.