



Circulars

14 Oct 2003

Suspected ATM fraud cases (superseded by TM-E-1 of Supervisory Policy Manual)

Our Ref: B1/15C
B9/29C

14 October 2003

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Suspected ATM fraud cases

In the light of the recent spate of reported fraud cases that may have involved ATMs, I am writing to set out the HKMA's expectation of how authorized institutions (AIs)¹ should handle customer complaints in this relation, and what precautionary measures AIs may put in place accordingly.

I would draw your attention to section 30.1 of the Code of Banking Practice which specifies that "card issuers will bear the full loss incurred:

- a. *in the event of misuse when the card has not been received by the cardholder;*
- b. *for all transactions not authorized by the cardholder after the card issuer has been given adequate notification that the card/PIN has been lost or stolen or when someone else knows the PIN (subject to section 30.4 of the Code);*
- c. *when faults have occurred in the terminals, or other systems used, which cause cardholders to suffer direct loss unless the fault was obvious or advised by a message or notice on display; and*
- d. *when transactions are made through the use of counterfeit cards."*

ATM frauds not only cause financial losses, but may also hamper customers' confidence in using ATMs, which would run counter to the industry's efforts in encouraging greater use of the electronic channels of delivery. It is therefore in the interest of your institution to prevent ATM frauds and to assist others in doing so.

Precautionary measures

Although there is no conclusive evidence on the precise methods used in the suspected fraudulent cases reported so far, it is suspected that at least some involve tampering with

ATMs. We therefore expect AIs to ensure that ATMs which are not located in secure areas² are adequately protected. It is an individual institution's commercial judgement to determine the appropriate level of precautionary measures needed. Having discussed the issue with AIs and ATM network operators, the following measures could be considered:

- a. enhancing the security features of ATMs. In this relation, I refer to a letter issued by JETCO to all its members on 3 October 2003;
- b. continuous monitoring of ATMs by installing closed-circuit televisions (CCTVs);
- c. implementing a mechanism that records relevant information on ATM cards or credit cards so that AIs can determine whether an unauthorized ATM transaction is carried out through a counterfeit card;
- d. more frequent patrols of ATMs during and after office hours;
- e. encouraging customers to report any suspicious devices detected on ATMs. Institutions should provide the relevant telephone number for customers to do so at the ATMs; and
- f. alerting customers if any unusual transaction patterns are noted.

In addition, AIs should also raise customers' awareness of the importance of protecting their cards and PINs.

As you know, we have sent out a survey to AIs offering ATM services to collect information about the precautionary measures they have or planned to be implemented to protect their ATMs. We will assess individual AIs' measures and, where necessary, require AIs to enhance their precautionary measures. Our supervisory staff will also monitor and follow up individual AIs' progress in implementing appropriate precautionary measures.

Handling of customer complaints

As stated in section 1.2 of the HKMA's Supervisory Policy Manual IC-4 "Complaint Handling Procedures", AIs are required to have systems in place to ensure that customer complaints are fully and promptly investigated and resolved in a satisfactory manner. Failure to have in place effective arrangements to handle customer complaints may also call into question whether an AI continues to satisfy the authorization criteria³ in the Seventh Schedule of the Banking Ordinance.

To aid in enhancing public confidence in ATM services, we expect AIs which offer credit card and / or ATM-related card services to put in place, as soon as possible, appropriate mechanisms whereby transactions conducted through a counterfeit card are quickly identified. This will help to enable most fraudulent usage to be monitored more quickly and resolved promptly. For cases which occur prior to the implementation of such a mechanism, we expect your institution to observe the following guidance in handling customer complaints:

- a. You should ensure that the customer promptly notifies the Police. Complainants should be notified of the staff member handling the complaint and liaising with the Police. This staff member should gather relevant information from the complainants about the cases and facilitate co-operation between the Police and the AI;
- b. Your institution should aim at completing your own internal investigations as early as possible. Internal investigations should be conducted in parallel with the Police's

investigation so that a resolution can be reached soon after the Police have completed their investigation;

- c. You should provide the fullest co-operation to any affected AI of the same ATM network when you are asked to assist in the investigation (e.g. in providing reports on the transaction records of the complainant and inspection reports on those ATMs believed to have been tampered with);
- d. You should keep the complainants and the HKMA informed of the progress of your investigations at least once every two weeks;
- e. You should make prompt decisions relating to the compensation to the customers once you have sufficient evidence from your internal investigations indicating that the cases in question are substantiated. **For cases of this kind, you should not wait for the Police's report;** and
- f. **For those cases considered unsubstantiated having regard to the results of the internal investigations and the Police's report, you should let the HKMA know your decisions within one week after receipt of the Police's report.** You should forward to the HKMA a copy of your investigation report and the proposed reply to the complainant, and ensure that a reply to the complainant is issued as soon as practicable after consulting the HKMA. A reply should be made to the complainant no later than one month after receipt of the Police's report in normal circumstances.

I hope you will find the above useful. If you have any questions on this letter, please feel free to contact Mr Shu-Pui Li at 28781826 or Mr James Tam at 28781607.

Yours faithfully,

William A. Ryback
Deputy Chief Executive

- 1. In this circular, AIs refer to those institutions that provide credit card and / or ATM-related card services to their customers.
- 2. Secure areas refer to those locations where the risk of ATMs being tampered with is small such as lobbies of bank branches and prominent positions inside MTR or KCR stations.
- 3. Specifically, paragraph 12 of the Seventh Schedule requires AIs to conduct their business with integrity, competence and in a manner not detrimental to the interests of depositors and potential depositors.

c.c. Mr Chan Kay-Cheung, Chairman of Joint Electronic Teller Services Ltd.
 Mr Vincent Wong, Chief Superintendent of Police, Commercial Crime Bureau

