
FRAUD PROTECTION IMPROVEMENTS NEEDED IN UAE BANKS

LONDON, UK, September 19, 2008 -The spate of ATM withdrawals on customer accounts with fraudulent cards has sparked widespread concern across the Middle East. The incidents that happened in UAE have rattled many banks and have instilled fear in the minds of cardholders.

Dubai is now maturing into a major leisure and business destination and this means that many foreign-issued cards will be used at local ATM machines and to make various purchases around the city. Middle East-issued cards also have a very high level of out of country spending, since a large portion of cardholders are expatriates, the cards are more prone to overseas usage.

With the implementation of chip and pin in both cards and ATM machines, local card fraud usually goes down; however cross-border ATM fraud and card-not-present fraud dramatically increases. The usual defenses dished out by the card schemes - EMV, 3D secure - are not effective against card skimming especially when the fraudulent card is used with terminals and ATM machines that still read the magnetic strips. These incidents are likely to grow in numbers leading to higher losses as organized gangs realize that the Middle East is easy picking for card fraud.

The banks in the Middle East must secure their cardholders with appropriate and effective systems. And there are solutions out there that do just that. This is why a product like CardSwitch Technology should be implemented into all banks and card issuing organizations.

The CardSwitch system would prevent any card skimming from occurring as it would be useless for a fraudster to skim a card that's protected by this technology. CardSwitch Technology offers a system that is the only really effective method to deflect the increase in card fraud while guaranteeing an excellent quality of service to cardholders.



PRESS

This new technology enables cardholders to put an electronic lock and key to their card accounts, making it futile for hackers and fraudsters to skim cards. When a cardholder decides that his card will not be used for any ATM transaction abroad, he can lock his card account, making it impossible for fraudulent out of country ATM transactions. The same control can be applied to card-not-present transactions, out of country card payments and local ATM transactions.

Cardholders can then unlock their card accounts for these types of transactions before they want to use their card and can specify particular limits, such as which countries the card will be used in, period of time (start date/time: stop date/time) and/or amount of money. These parameters, called 'cardholder user limits' can be set by simply sending an SMS command with a mobile phone, making a quick call to an automated system by using a landline phone, or via internet by simply setting these user limits online.

Cardholders can lock or unlock their card accounts 24 hours a day, seven days a week. These cardholder user limits will take effect immediately, allowing cardholders to unlock or lock their cards without delay.

The rise in instances of card related fraud across the world is a concern and cardholders need to take precautions. But it's most important that banks need to act fast about fraud and allow cardholders to actively participate in the security and authorization of their own cards and enable them to control the disbursement of funds that banks are doing on their behalf.