Card skimming fraud: who is liable?

With a 23% year-on-year increase in card skimming fraud from R366 million to R453 million recorded last year, according to the Hawks, it is becoming increasingly important for both consumers and establishments to be vigilant about this type of fraud, especially during the busy festive season. Due to each case being different, determining who is responsible for the loss can be challenging.

© amorn prajakjit – 123RF.com

This is according to Anton Meyer, Executive Head of SHA Specialist Underwriters, who said that while most people may automatically think that the bank handling the transaction is responsible for the loss, the bank is not necessarily liable if the consumer or merchant has not taken proper care. "There are various factors that need to be taken into consideration when determining liability for card-skimming fraud."

He explained that most of the fraudulent card-skimming machines are actually imported and, on the face of it, look and feel exactly the same as any other mobile card machine. "In order to clone a card, all the fraudster needs to do is clone the strip and take note of the three-digit Card Verification Value (CVV) number on the back of the card. The fraudster uses these details to create a cloned card, which is then used elsewhere for fraudulent purchases. These machines also record the PIN number and the customer is simply advised that the machine does not work and the fraudster then processes the transaction on the correct machine, but by this time all the information sorted on the card has been copied and the cardholder's security compromised."

Migrate to EMV-compliant cards

To combat this type of fraud, and reduce the associated costs for the crime, various African countries, including South Africa, have begun to migrate to EMV (Europay, MasterCard and Visa)-compliant cards, said Meyer. "These cards have a chip-and-pin system. Every time an EMV-compliant chip card is used, a unique transaction code is created that cannot be used again, making it impossible to use the same code for a future fraudulent transaction. While it does not prevent data breaches from occurring, the EMV-compliant cards do make it harder for fraudsters to use the cloned card, although this is still possible if these cards are 'exported' to territories that are not EMV compliant."

He said that it is important for merchants, such as restaurant owners, to ensure their employees are not involved in card-skimming scams, as the merchant can be held liable if he has not taken due care. "If a consumer goes to a restaurant he expects proper service and his data to be secure."

In the same vein, it is important for consumers to be proactive and look for signs of card-skimming scams. "If the machine does not work and does not produce a paper slip to prove the transaction failed for some reason (such as failed communication or lack of authorisation), it could be a sign that the machine is a fake. In this case, consumers should make sure they speak to the manager. The customer has the right to ask the manager if the machine belongs to the establishment. It is also a good idea never to let the machine or the card out of sight during transactions."

Instant notification service

Unfortunately, it is usually only after a customer has left an establishment and fraudulent transactions are performed that the victim realises that he has become a victim of card skimming, said Meyer. "The bank will only flag the transactions if they seem suspicious after a few transactions have occurred. That is why it is beneficial to have the instant notification service activated, where the consumer receives communication in the form of an instant message once a transaction has occurred. This way he can flag possible fraudulent activities with the bank as soon as they occur."

Locating the venue where the card skimming occurred can be challenging, he said. "However, the advent of social media can make it easier to find the location if multiple people start complaining that their cards were skimmed - and they find out other victims were at the same venue. Even after the location is determined, the injured party would still have to prove negligence on the part of the owner. As per all social media posts, people need to be very careful not to post statements that could be deemed defamatory."

Due to the various factors that come into play when determining liability for card-skimming fraud, it is vital that both consumers and merchants take the necessary precautionary measures to avoid becoming a victim, concluded Meyer.