

Crooks dine out on card swiping

'Syndicates even consider patron volumes according to the day of the week and time of day to maximise the volumes of cards skimmed' — Superintendent Solly Magobosha

15 March 2009 Swindled: Credit card skimming and related fraud costs the South African economy hundreds of millions each year

Small businesses, mainly independent restaurants and businesses that have recently come under new management, are often more prone to being targeted by this rapidly increasing criminal activity. Hendri Pelsler investigates a scourge that is difficult to detect if several staff act in cahoots

Kevin Coetzee, owner of The Royal Boma restaurant and theatre in Alberton, is R112000 out of pocket. A syndicate recently targeted employees at his establishment, harassing them into committing credit card fraud, leaving Kevin with the bill and nursing a sizeable headache.

The Royal Boma is just one restaurant in a long list of small businesses that have to carry the annual R118-million price tag of credit card skimming and fraud.

Out Of Pocket

Kevin explains that a syndicate persuaded and later intimidated employees to swipe fraudulent credit cards while taking cash out of the tills. As a result, the daily transaction total tallied for three weeks.

"It is very sad," Kevin says. "I sat with a barman in jail — he's been with me for seven years." A manager and accountant were also allegedly involved, allowing the fraud to carry on unnoticed.

"I wouldn't have placed them in positions dealing with money if I didn't trust them."

Kevin's frustration is plainly evident as he explains that the business has systems and processes in place to combat this type of fraud, as another of his restaurants was a victim several years ago.

"The systems are watertight and this should have been picked up in one day. But, if a couple of people work together you will never catch them.

"Luckily I have other businesses (that can help carry the loss). But, if this was a one-man show the business would have gone under."

Kevin adds that the ripple effect of the fraud is still playing itself out among the 47 other staff members left as the trust relationship between employer and employee has been broken.

Rampant Practice

The Royal Boma's story is more common than most entrepreneurs realise. The Kauai franchise was also recently targeted in the Western Cape. Kauai financial director, Hendrik Coetsee, explains that waiters at two group-owned gym stores also used copied cards to skim cash from the till.

“Credit card fraud is a risk for everyone (in business). Fraud will always place your systems under pressure. You need to install enough ‘dashboard warning lights’ to ensure that you keep your finger on the business’s financial pulse so you can pick up anything out of the ordinary,” Hendrik says, but adds that unfortunately there is not a system available that can overcome several employees working together.

Similarly, two franchisee-owned Dros restaurants became victims of card skimmers in the Western Cape two years ago.

Dros national operations manager, René Jordaan, says that waiters would pass the credit card details to a ringleader. As with the Royal Boma, the Dros waiters involved were being blackmailed.

Despite the fact that the criminals were caught in these cases, it created a bad reputation for the restaurants involved.

Be Alert

Wendy Alberts, the Restaurant Association of South Africa CEO, says that the widespread rollout of mobile credit card machines has led to a significant decrease in credit card skimming in restaurants.

Unfortunately, these machines come with higher monthly rentals and higher transaction commissions — something a risk analysis needs to take into consideration.

She adds that smaller, independent restaurants and businesses that have recently come under new management are often more prone to becoming targets.

Restaurants serving foreign clients are also targets because it takes time for tourists to realise their accounts have been compromised.

The association provides members with an employee database, which has helped to catch criminal elements moving from restaurant to restaurant. “If information is shared among the industry we can do something about it. Together we can put preventive measures in place,” Wendy says.

Syndicates

Superintendent Solly Magobosha, acting section commander of the SAPS banking-related crime group, says there are usually two parts to this type of fraud.

Firstly, criminals need to skim or copy the information stored on a credit card’s magnetic strip. This information is used to create a fraudulent card resulting in fraudulent transactions.

Solly says the syndicates usually consist of a kingpin who issues card- skimming devices to runners and collects the stolen data.

Restaurants are often targeted for the first part of this operation because the volume of clientele creates easy access to credit cards.

“These syndicates are highly organised and research their targets. They even consider patron volumes according to the day of the week and time of day to maximise the volumes of cards skimmed.”

The duplicate cards in turn are used for a variety of unauthorised and fraudulent transactions. These include the rental and subsequent theft of vehicles and the buying of phone air time, liquor, furniture or electronic and consumer goods that can easily be sold. Solly says that skimming and spending hotspots tend to migrate.

Catching the Crooks

Statistics on the number of card-skimming criminals charged and convicted are not available, but credit card fraud losses on South African-issued cards have increased at an annual average rate of nearly 60% since mid-2005.

At the same time, the South African Banking Risk Information Centre (Sabric) says that counterfeit card fraud has doubled since mid-2006.

According to Susan Coetsee, head of Sabric's commercial crimes office, bank investigators and the SAPS retrieved a total of 115 hand-held skimming devices in 2008.

"This is a notable success considering that a single hand-held skimming device, on average, can store data stolen from approximately 2000 cards."

Susan says business owners should vet all their employees, especially those who are directly involved in the payment process, such as cashiers, waiters and waitresses.

"It is also important for business owners to educate their staff members about the risk of co-operating with criminal syndicates. Not many people understand that helping someone to commit a crime is also a crime."

Don't be a victim

Many banks will not cover the loss of a fraudulent credit card transaction if the correct safety procedures were not followed.

As a merchant, it is imperative that business owners:

- Ensure that the card security features are present;
- Hold onto the card until the transaction is completed;
- Compare the signature on the card to that on the sales voucher;
- Phone for authorisation if requested by the point of sale device;
- Phone for authorisation if you become suspicious;
- Make an imprint of the card in the case of a manual transaction; and
- Make sure you can identify a card-skimming device or identify odd behaviour of staff mem