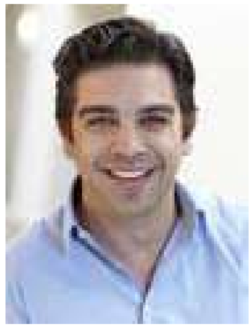
# Cyber crime risks destroying the gains made over the last year



Brendon Williamson
CSO at DPO South Africa

Online merchants are revelling in the excellent growth of new online customers, driven largely by the Covid pandemic. But while they are making hay, fraudsters are also migrating online and, if left unchecked, these bad actors could destroy the windfall of this new customer acquisition.

Brendon Williamson, CSO at DPO South Africa, looks at the state of digital fraud and advises merchants on how to protect themselves and their customers.

Everyone likes to quantify the cyber fraud problem, and this is certainly useful for tracking purposes. The problem, however, is that the data is inevitably 12 months behind our lived reality and so shifts in trends often go under reported and mostly ignored by the general public. It is very much up to consumers to inform themselves. Merchants, meanwhile, must ensure they are on top of trends, understand their liabilities, and, if they're smart, use the opportunity to better understand their customers' behaviour.

## From skimming to stuffing

Before fraudsters upped their game, card skimming was the main payment fraud we would see. You would hand over your card and the criminals would use skimming devices to make a clone of it, copying the details stored in the mag strip on the back of the bank card.

Fortunately we are seeing a decline in this particular type of fraud with fewer counterfeit cards circulating at present. Unfortunately, while the physical card fraud has decreased, card not present fraud is on the rise.

It's worth noting that many South Africans will have their card details stolen and used internationally – especially in places like the United States which doesn't have the added security of 3D Secure, which has proved especially effective in cutting down on online fraud.

In fact, the introduction of 3D Secure and just how effective it has proved has given rise to sophisticated social engineering where the criminals will contact the card holder, posing as their bank, and fast-talk the customer into disclosing their One Time Pin (OTP). The challenge with this type of fraud is that customers are seldom able to seek recourse in these instances

as they have handed over their OTPs, despite the many warnings we may have had from our banks.

Another cyber crime that is on the rise is credential stuffing. This year has seen a number of high-profile data breaches, where names and passwords have been acquired from various sites. Since so many of us recycle just a handful of passwords, the fraudsters will use the details they have to attempt to breach other sites. More than this, since they have so much of our information it is easy to impersonate banks or other service providers and dupe you into handing over information they can use to access accounts.

### Quantum can help

### But for now, it's up to you

One of the big problems when it comes to card fraud is managing false positives. This is when a bank or payment provider monitors behaviour out of the ordinary and incorrectly predicts a possible case of fraud.

Because quantum computers can process huge data sets in a fraction of the time of our regular computers, banks are able to throw much more information into their fraud engines, delivering increased accuracy. This will benefit the entire online ecosystem including merchant and customer. Unfortunately, we are not quite there yet and so for now, the risk lies more often than not, with the banks. What this means, is that managing risk is still a costly affair and of course, these costs get passed on via transaction fees.

From a merchant's point of view, it's important to know as much as you can about your customers. This should be managed carefully, because you don't want to spook first time buyers with overly extensive registration questionnaires, but at the very least get their name and email address.

More than just allowing future communication, profiles allow you to track how customers engage with your site and can prove exceptionally valuable in managing your risk. If a customer is behaving or buying in a way that is very out of the ordinary, merchants can call them to ensure the transaction's bonafides. This better understanding of the customer can also help brands forge a stronger relationship with their patrons, help design targeted digital marketing campaigns as well as assist in better product design and marketing. Knowing your customer is just great business practice all round.

### Virtual cards can help

A new addition to the South African digital landscape is the virtual bank card. The ability to create virtual credit cards can help reduce risk for consumers who are wary of sharing their details online.

These digital cards have randomly generated, once off numbers that are associated with your credit card account, but your actual card details are never exposed, keeping you safe even if the merchant's site is compromised. These cards are also a way for customers to manage spending on a shopping spree since they can limit the amount loaded on them.

It's clear that as fast we produce ways to combat fraud, cyber criminals will find new ways of breaching our systems. In this endless game of cat and mouse, it's imperative that the merchant do whatever they can to make their customers feel safe.

All it will take is one bad experience to spook a new online shopper and all the hard work and money spent in gaining them – not to mention the lost future revenue – is lost. It's also a great reason for merchants to partner with a payment service provider who can minimise their daily transactional risk. **SR**