bizcommunity

6 tips to prevent online fraud from sinking your business

The success of the recent Black Friday and Cyber Monday weekend is testament to the opportunity offered by digital commerce. But local entrepreneurs should not underestimate the threat of online fraud, which has the potential to ruin an unsuspecting business.

By Brendon Williamson 12 Dec 2018

©Igor Stevanovic via 123RF

The introduction of the 3D Secure authentication security developed by the Card Schemes has lowered th risk for merchants and boosted buyer confidence. However, fraudsters are nothing if not innovative and th growth in online fraud continues unabated.

Financial crime information centre SABRIC shows that in 2017, lost and stolen credit card fraud saw a 44.5% increase. The centre's statistics also indicate that credit card related Card Not Present (CNP) fraud still the leading contributor to gross fraud losses in South Africa. The 2017 numbers show that CNP fraud accounted for 72.9% of the losses on SA issued credit cards.

In an effort to protect the consumer, South African shoppers who report fraudulent transactions can have their money refunded. The bank will draw the money from the merchant's account to refund the consumer and the merchant will then have to lodge a dispute with the bank if they believe they were not at fault.

This chargeback process can be long and complicated. In addition, in many instances, fraud will only be reported once the goods have already been shipped - leaving the merchant without their product and their money.

MOBILE COMMERCE

#MobileCommerce: Understanding payment trends to ensure customers get what they want

Brendon Williamson 12 Jul 2018

Keeping a close eye on your transactions makes all the difference. There are some obvious tells that will

alert you to something being untoward.

1. What's in a name?

Fraudulent transactions names are often robotically generated and can throw out very common names like John Smith, or it will choose the same name for both first and last names, such as John John. Another common choice is to use movie star names.

So, while you don't want to turn down business from every legitimate John Smith out there, the chances of Angelina Jolie or Idris Elba buying a bicycle for delivery to Centurion are slight.

2. Run the numbers

If you have a telephone number from the customer, do a quick Google search on it. In many instances of fraud you will see that number on another site selling similar goods to what have been purchased.

3. There's no place like home

In the same fashion, a quick Google Earth search can also throw up red flags. Buildings which have been demolished or addresses that have no building whatsoever require additional investigation.

4. Those lips don't lie

One of the best ways to do a quick check on a new customer, or one you may be suspicious about, is to p up the phone and chat to them. Firstly, welcoming a new shopper to your service is excellent customer service, but it also gives to a chance to check on details.

Asking a customer to verify information such address or telephone number should be no problem. Fraudsters, however, may get tripped up as they often use bogus addresses and multiple burner phones t conduct their nefarious transactions. Long pauses and an inability to immediately answer your questions w tip you off – always only give just a small part of the details you have and ask the buyer to complete them.

5. Twitter trip-ups and Facebook faux pas

Many subscription forms and customer signups ask for information such as age, gender and occupation. This can be quickly checked against social media profiles if they have them and can be a fast, valuable tickbox.

6. Seeing is believing

Many successful stores will stagger delivery to a new customer who has made multiple purchases. Shippi a lower-value product ahead of the big-ticket items lowers your risk, allowing you to establish the validity of your customer before overcommitting.

During peak buying periods such as Black Friday, annual sales and the festive season, you will see many online stores have slightly longer delivery times. This not only accounts for managing high-volume logistics but also gives them more time to see if there is fraudulent activity before dispatching the goods.

All of the above are fairly simple ways to know your customer and de-risk your online business. But by far t most important is to work with your payment service provider. Fraud units within the PSP should have

seasoned fraud experts who can work with you over the phone to establish the likelihood of a dodgy transaction. Using advanced, rules-based software, like the Mastercard GateKeeper offerings will also allo them to monitor your transactions in real time and will alert you to untoward activity.

While every online merchant should be chasing the orders and constantly finding ways to improve the customer journey, protecting yourself against the growing sophistication of the online criminal cannot be overlooked. During peak times, however, this becomes increasingly difficult. Partnering with a trusted payment solutions provider can save you a world of heartache, both now and in the future.

ABOUT BRENDON WILLIAMSON

Brendon Williamson is the Managing Director at PayFast and PayGate. A veteran of the payments and e-commerce industry, Williamson has over 20 years' experience in sales, marketi and online fraud management - with a background in online gaming and e-commerce transaction management. He has been part of the DPO Group for more than 10 years as Chief Sale Officer, Chief Marketing Officer, and most recently, Head of Commercial. Looking ahead, his goal is to take digitalisation to the next level.
View my profile and articles...

For more, visit: https://www.bizcommunity.com