Update On Braintree Fraud Protection

Last Modified on 22/02/2017 2:56 pm AEDT

Recently we advised our clients that we have moved to a new merchant provider (**Braintree**) and also introduced Paypal as a new payment method.

One of the key features of moving to our new merchant provider was the **enhanced fraud protection** which Braintree provides through its provider Kount.

This has been of particular **benefit to our Ecommerce clients in significantly reducing fraudulent orders**, however we understand that some legitimate customers have unintentionally been caught up in this enhanced fraud protection, and as a result have not been able to process transactions.

The fraud detection works around a number of parameters that Kount use to detect potential fraudulent activity. **This happens automatically for every transaction, and is not something we control**. Some of the examples of where legitimate transactions may be detected as fraudulent include:

- **MULTIPLE TRANSACTIONS PROCESSED ON THE SAME CARD**

A common fraudulent practice is for someone to try and process **multiple transactions using stolen credit card details in a short period of time**. If a legitimate customer is **attempting to process multiple payments on the one card**, possibly for themselves or on behalf of others, **this will likely get flagged as fraud**.

In this case, we would recommend that **customers process only their own transactions on their cards**, and **not process multiple payments on the one card**. If a customer needs to purchase multiple memberships for example, then this should be **completed in one transaction**, rather than trying to process each one individually.

- **PROCESSING TRANSACTIONS ON BEHALF OF A CARDHOLDER**

Kount assesses the **location of someone attempting to process a transaction** as one of its fraud tools, which matches the location of the person attempting to use the card to the location of the cardholder, or being used from computers in different physical locations within a short period of time. If the **locations do not match**, or are too far apart to be possible, it may be flagged as fraud, as this is commonly the case for people using stolen credit card details.

As a result, if a legitimate customer is **attempting to process transactions using someone else's card**, this may be detected as fraud

- **PROCESSING MULTIPLE TRANSACTIONS FROM THE SAME COMPUTER / IP ADDRESS**

Similar to above, this is a common sign of fraud, where fraudsters will try and **process multiple transactions on stolen cards from one location**. If someone is legitimately trying to process multiple payments, either on the one card or multiple cards, then they are likely to be flagged as fraud.

- **HOW TO AVOID UNINTENTIONALLY BEING DETECTED FOR FRAUD**

The best way for customers to avoid unintentionally being detected as processing a fraudulent transaction, is for only the cardholder to process their own transactions. Customers, clubs etc should **avoid practices whereby payments are processed on behalf of others**, whether this involves using other people's card details or not.

We also stress again, that the fraud detection is automatic, and is not something that we are able to direct or control.

- **WHAT DO YOU NEED TO DO?**

Please **distribute this message to any staff members** that the heightened fraud protection service has been included into the console.
This includes any casual staff members that may put through any payments on behalf of customers.

Related Articles

[template("related")]