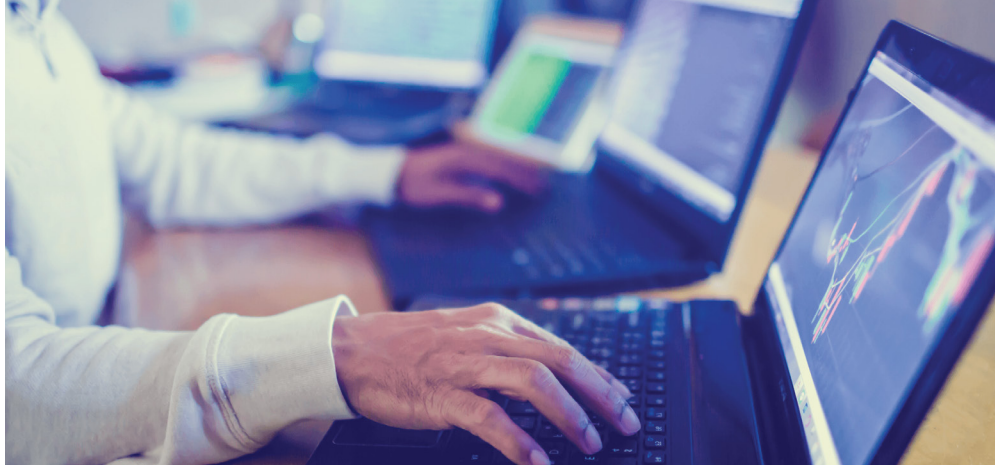
Allianz

Top three fraud threats



Make sure you and your customers stay safe from fraud

1 Ghost broker/ application fraud

We continue to see more people falling into the hands of fraudsters, lured by the promise of cheaper premiums. These so-called ghost brokers use stolen identities to get around fraud controls, so it's important to make sure front-end data (such as device characteristics and IP addresses) are regularly reviewed to look for patterns in those making the application. ID validation and strong payment controls pre-sale are key to preventing this type of fraud.

There's also a likelihood that financial hardship may see an increase in non-disclosure, or deliberate misrepresentation of risks. Brokers should be looking at quote manipulation for nongenuine reasons, and amendments to NCD, date of births (DOB) and vehicle usage that may be taking place at quote stage. In a recent case we tracked numerous quotes in a 24hr period by the same person for just one vehicle. When reviewing the quote history, it was clear the individual had used three different addresses spread across 200 miles with several different name and DOB combinations, clearly a falsely presented risk. While there are some genuine reasons for trying different quotes, make sure this is tracked to identify fraud.

2 Claims fraud threats

There are a number of risks in this category like the potential increase in false fire or theft claims. We may also see the layering of claims by professional enablers like credit hire firms who look to extend hire periods or blame delays. However, from a broker perspective we recommend you stay alert to the increased risk of 'claims farmers' and 'data vishers'. Front-line staff should keep a close eye out for any vishing attempts that may be made to brokers.

3 Cyber or insider risk

With more companies moving to hybrid working, there's an increased risk of data theft as staff, or members of the household, may have easier access to data. While there will be robust processes in place to combat this risk, it's recommended the monitoring of any data access is heightened.

In line with bulletins from Action Fraud, we're also seeing an increase in false vishing emails being received as fraudsters look to obtain data, take over accounts or divert payments into their own bank accounts rather than those of genuine customers, suppliers or even staff.

The monitoring of inbound external emails can assist in this area, as well as defined controls for finance teams and HR areas to check before making amendments to payment details.

0037656-2024