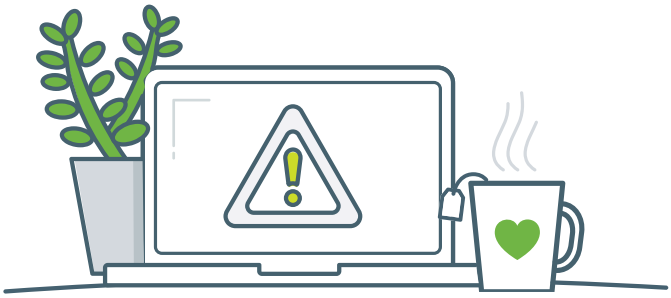
# 3 COVID-19 fraud threats you need to know about

Here are 3 emerging COVID-19 fraud trends and threats that you need to be aware of over the coming months.

## Ghost broker/ application fraud

With many people affected financially by the effects of COVID-19, we expect that more people may end up in the hands of Ghost Brokers as the lure of cheaper premiums takes hold. We continue to see large numbers of ghost brokers using stolen identities to circumnavigate 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 exposure to 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 non-genuine 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 1 vehicle. When reviewing the quote history it was clear the individual had used 3 different addresses spread across 200 miles with several different name and DOB combinations, clearly a falsely presented risk. Whilst some genuine reasons will exist for trying different quotes, it's important to ensure this is tracked and any fraudulent manipulation is identified.



## Claims fraud threats

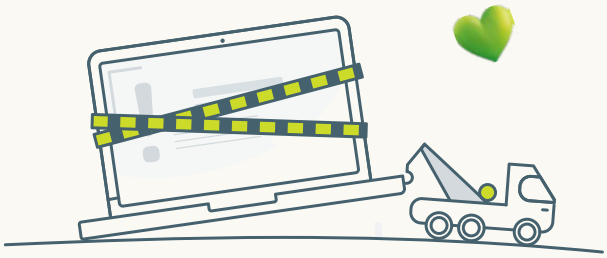
There are a number of risks that we have in this category such as the potential increase in false fire or theft claims, as people can no longer afford to keep their vehicles or are in need of cash. We may also see the layering of claims by professional enablers like credit hire firms who may look to extend hire periods or blame delays caused by COVID-19. However from a broker perspective we recommend that you stay alert to the increased risk of 'claims farmers' and 'data vishers'.

With the industry reporting huge drops in new claims due to people being at home self-isolating, it's expected that Claims Management companies may need to revisit their historic data to generate new leads. Front line staff should remain vigilant to any vishing attempts that may be made to brokers.

# Cyber or insider risk

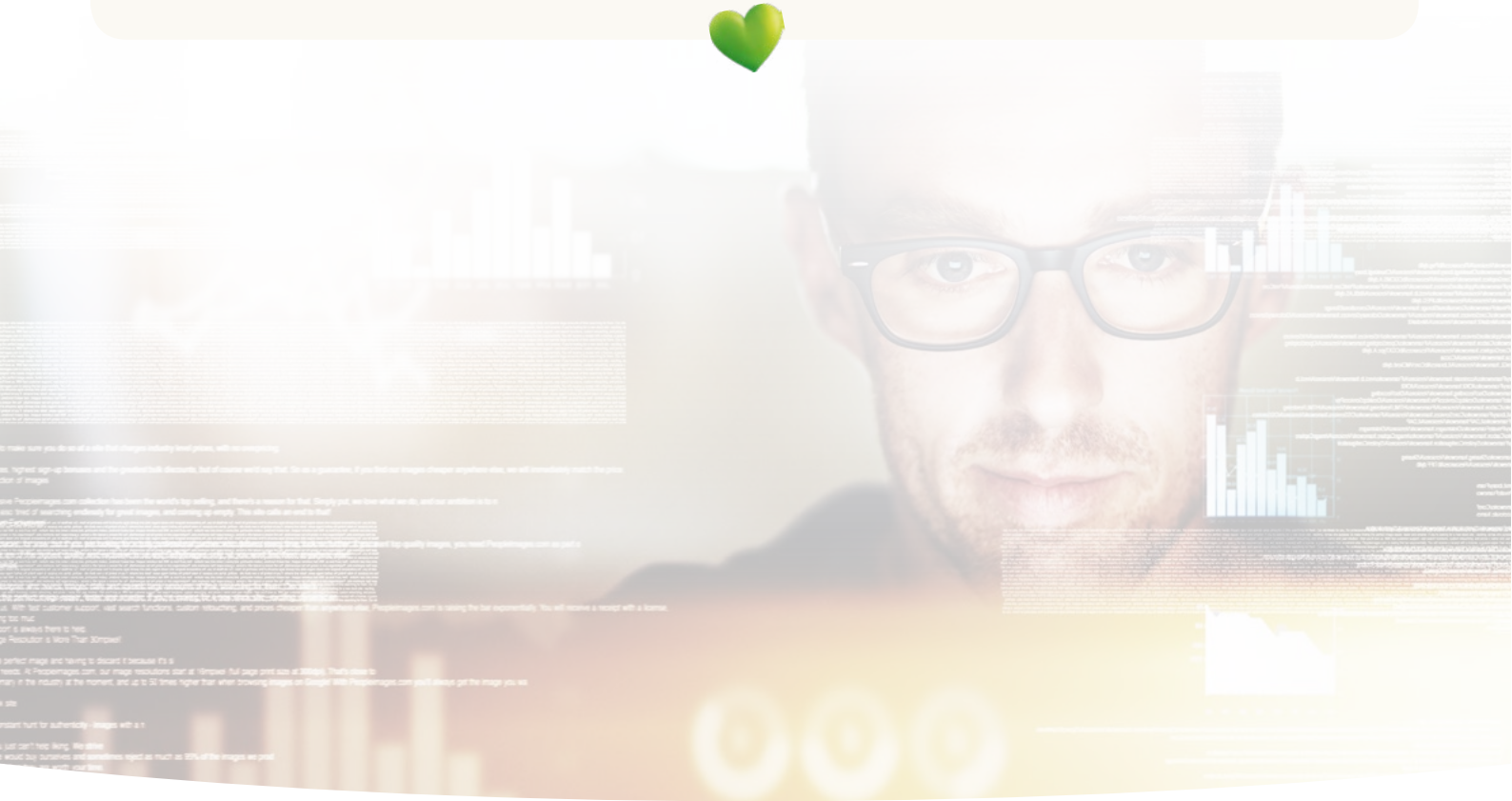
With more companies moving to home working solutions, there's an increased risk of data theft as staff, or members of the household, may have easier access to data. Whilst robust processes will be in place to combat this risk, it's recommended that the monitoring of any data access is heightened during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

In line with recent bulletins from Action Fraud, we're also seeing an increase in false vishing emails being received as fraudsters look to obtain data, carry out account take overs or change payment methods to 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 to check before making amendments to payment bank accounts within finance teams as well as HR areas.

If you require any more information on any of the above or need any more support on financial crime risks then please contact Matthew.Crabtree@lv.co.uk



LV= BROKER



0031720-2020