How to protect yourself from fraud

Have you ever received a call where someone tells you there's thousands of pounds in compensation waiting for you, for an injury you may have suffered in a car accident?

This is known as claims farming and could land you in serious financial, and in some cases even legal, trouble.

What is claims farming?

Claims farming, also known as 'insurance vishing', is when a person or company encourages someone else to make a claim – usually a personal injury claim after a car accident or a claim against mis-sold PPI (payment protection insurance). Some claims farming companies make cold calls to people, asking if they can talk to them about an accident they've had, with a view to manipulating them into making a fraudulent claim. The claims farmer will pass the information over to a lawyer, who may pay the claims farmer a fee if they take on the case. These calls are vishing calls and scammers will sway you into believing it's ok to make the claim and the money is rightfully yours, but if you don't have a genuine accident related injury, it's not.

How to recognise a vishing call, and how to respond

If you haven't been in an accident, hang up.

Otherwise, ask questions to make sure that the caller is from a genuine insurer that could be involved in your case. Scammers use various techniques to find people who may have been involved in an accident but not suffered any personal injury, including using social media. In other cases, information can be obtained illegally from sources such as insurance companies, or even car rental companies. Insurers will often contact innocent third parties if one of their customers has been in an accident, and will know far more about the incident than claims farmers.

Insurance vishers often go to great lengths. They use a number of techniques to convince you to make a claim. Here's some of the methods to look out for:

Information: the caller already has your name, address, phone number, vehicle details - essentially the kind of information you would expect a genuine caller to have. Most genuine firms will ask you data security questions to confirm they are speaking to the correct person.

Urgency: You are made to believe time is running out to make a claim and you have to act quickly - fear often leads people into acting without thinking.

Phone spoofing: The phone number can appear as if it's coming from somewhere local, so encouraging you to answer without question as the caller's number looks friendly.

Atmosphere: You hear a lot of background noise so it sounds like a call centre rather than a guy in a basement - they either do have a call centre, or are playing a sound effects CD.

Don't answer any questions before they satisfactorily answer yours – many companies will quote the Data Protection Act and say they don't have all the details, using it as an excuse for you to tell them. And if you think you've been vished, please report it straightaway using the info below:

1. **Ofcom:**

   Independent Regulator and Competition Authority for the UK communications industry.

   Report a claim or issue relating to cold calls.

2. **The Information Commissioner's Office (ICO):**

   An independent authority set up to uphold information rights in the public interest.

   Report a claim or issue relating to vishing calls.

3. **Telephone Preference Service (TPS):**

   UK's only official 'Do Not Call' register.

   Provides a free opt out service enabling people to record their preference on the official register and not receive unsolicited sales or marketing calls.

4. **Action Fraud:**

   National fraud and cybercrime reporting centre in England, Wales and Northern Ireland.

   Reports of fraud and any other financial crime in Scotland should be reported to the police via 101.

If you feel you have a good reason to make a claim, always contact your insurance company first for advice on how to pursue it.

LV= BROKER

0037466-2024