

## Covid

### Fake FCA emails, websites, letters and phone calls

Find out how fraudsters claim to be from the FCA and other organisations, and what you can do to spot and avoid these scams.

Some fraudsters contact people and firms through emails, letters and on the phone, claiming to be from the Financial Conduct Authority (FCA) or using the name of FCA employees to make them seem genuine.

We have received reports that there are fake FCA emails circulating from the domain '@gabriel-FCA.org.uk'. These emails are: connect1@gabriel-FCA.org.uk

- connect2@gabriel-FCA.org.uk
  - connect3@gabriel-FCA.org.uk
  - connect4@gabriel-FCA.org.uk
  - connect5@gabriel-FCA.org.uk
  - connect6@gabriel-FCA.org.uk
- See how fake FCA correspondence works below. We would never ask a consumer for personal information like bank account details or internet banking passwords.

### Fake versions of our websites

Fraudsters may create copies of our websites and modify some of the information on them. They may change our warnings pages for example so it appears that scam firms are authorised by us when they are not. These cloned websites can be very convincing with links that work and contact us information.

You can check whether our website is genuine by checking the web address (domain name or URL), which appears in the address bar at the top of the webpage. It should always begin with: **www.fca.org.uk** or **register.fca.org.uk** for the [FS Register website](#).

Our online systems for firms have web addresses that start with:

<https://connect.fca.org.uk/>

<https://gabriel.fca.org.uk/>

<https://mutuals.fca.org.uk/>

<https://marketsecurities.fca.org.uk/>

## How fake FCA correspondence works

The scammers may contact you by email, post or a phone call and claim to be from the FCA or use the name of an employee, to give the impression that the communication is genuine.

We send emails from addresses ending in [@fca.org.uk](mailto:@fca.org.uk) and [@fcanewsletters.org.uk](mailto:@fcanewsletters.org.uk), but be aware that fraudsters can 'clone' these email addresses to make their emails seem genuine. Find out the [FCA email addresses we have been told fraudsters are using](#).

The fake emails and letters may contain our logo or other images taken from our website or publications. The fraudsters may say you owe us money or ask for personal information such as copies of your payslips or passport.

You may also be told you are entitled to a sum of money, perhaps because we have collected it from a bank, and that we need your bank account details to make the payment. However, the fraudsters intend to access your account, using the details you have given them, to remove money from it.

The fraudsters may also claim to be from the organisation that used to regulate financial services in the UK, the Financial Services Authority (FSA).

Fraudsters may claim to be from the FCA saying we are investigating your bank (or other financial institution), they may ask you to move your money to another account for security reasons. The FCA would never do this, [contact us](#) directly if you have any concerns — do not use the contact details on any correspondence received.

## Protect yourself

Remember: if it sounds too good to be true, it probably is!  
Keep in mind that we would **never** contact members of the public asking for money or your bank account details.

The correspondence is likely to be linked to organised fraud and we strongly advise you not to respond to the criminals in any way.

Look for signs that the email, letter or phone call may not be from us, such as it listing a mobile or overseas contact phone number, an email address from a hotmail or gmail account, or a foreign PO Box number. Scam emails or letters often contain spelling mistakes and poor grammar.

If you are in any doubt about the authenticity of contact from the FCA, call our [Consumer Helpline](#) on 0800 111 6768. or [consumer.queries@fca.org.uk](mailto:consumer.queries@fca.org.uk)

### **More fake communication scams**

Fraudsters also claim to be from the [Financial Ombudsman Service](#)(link is external), [Financial Services Compensation Scheme](#)(link is external) and [Money Advice Service](#)(link is external), and ask people for their personal details or money.

You should also beware of emails or calls claiming to be from [HMRC](#)(link is external) and offering a tax rebate. HMRC never sends emails or calls about tax rebates, or asks for personal or payment information in this way. For more information see [HMRC's examples of phishing emails](#)(link is external).

### **Caller ID spoofing**

We have been told **scammers are making our switchboard numbers – 020 7066 1000, 0300 500 8082 and 0800 111 6768 – appear in the caller ID** of people they contact. Ofcom explains [how to avoid 'caller ID spoofing'](#)(link is external) and why not to give any information to these people or call them back.