HOW TO IDENTIFY EMAIL PAYMENT FRAUD.



The request claims to be urgent and/or confidential.



The request includes grammatical and spelling errors.



The request is made on behalf of the CEO or CFO.



The type of request, language or format are unusual.



You are requested to ignore standard payment authorisation processes.



The 'reply to' email address is different to the sender's address.

Be vigilant.

- **1.** Never deviate from standard procedures for payments.
- 2. If a request for payment doesn't look right, don't be afraid to escalate.
- **3.** Validate suspicious requests on an alternative communication channel, using contact details listed in your internal records.
- **4.** Notify your bank immediately if you have made a payment by mistake.



Things you should know: The information and advice contained in this document is of general application and is not tailored to your individual circumstances. The Bank cannot guarantee that by implementing the advice in this guide you will never be a victim of fraud. All material presented in this guide, unless specifically indicated otherwise, is under copyright to the Commonwealth Bank of Australia. None of the material, nor its content, nor any copy of it, may be altered in any way, transmitted to, copied or distributed to any other party, without the prior written permission of the appropriate entity within the Commonwealth Bank of Australia ABN 48 123 124 AFSL 234945.