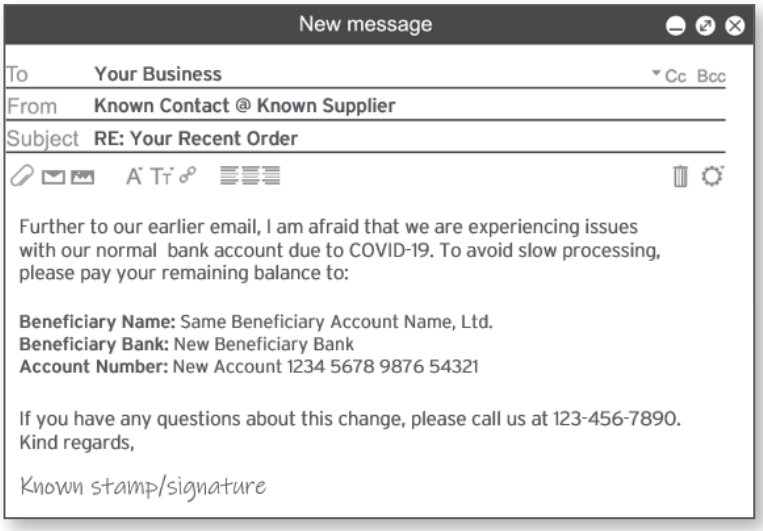
This is what fraud looks like

Fraudsters are increasingly taking advantage of the disruption caused by COVID-19 to target businesses. The most common type of scam involves the attacker impersonating one of your suppliers, which will normally look something like this:



If you ever receive an email asking for a payment to be sent to a new bank account, contact the sender via telephone to verify the request. It's important to be aware that fraudsters:

- Will make the email look like it has been sent from a known contact or supplier
- Can make it look like the request is replying to an earlier email
- Try to make the attempt look as normal as possible – e.g. expected value, normal timing, genuine invoice numbers, etc.

PLEASE REMEMBER:

KNOWN SENDER + KNOWN CONTEXT ≠ GENUINE EMAIL

Best practice advice:

- Always call a known telephone number; do not use any numbers given in the email
- Ensure that two employees check any payment being sent to a new beneficiary
- Be particularly wary of requests to send a payment to an account held in a different name, or located in a different country

The pandemic is already causing significant challenges for businesses; by following the guidelines above, you can help ensure that fraud does not add to the burden. For further resources on Fraud Prevention, please visit the Citi Commercial Bank website, citi.com/commercialbank.

1985609 08/20