

5.3.89

Where identity is verified electronically, copy documents are used, or the customer is not physically present¹, a firm should apply an additional verification check to manage the risk of impersonation fraud by directly linking the customer to the claimed identity. In this regard, firms should consider:

- verifying with the customer additional aspects of their identity which are held electronically; or
- utilising biometric data (including facial recognition² and liveness checks where appropriate); or
- requesting the applicant to confirm a secret code, or biometric factor – such codes, digital verification or other secret data may be set up within the identity, or may be supplied to a verified mobile phone, or through a verified bank account, on a one-time basis; or
- following the guidance in paragraph 5.3.90.

¹ With appropriate controls in place non face-to-face may not pose a higher risk

² For example, via a UK government certified digital identity service provider (IDSP)