5.3.89

Where identity is verified electronically, copy documents are used, or the customer is not physically present[1], 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 recognition[2]); 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).

Deleted: his
Deleted: (or biometric data)
Formatted: Font: (Default) Times New Roman, Ligatures: None
Formatted: List Paragraph, Indent: Left: 0.62 cm, Add space between paragraphs of the same style, Bulleted + Level: 1 + Aligned at: 0.74 cm + Indent at: 1.38 cm
Deleted: or PIN
Deleted: , that links them incontrovertibly to the claimed electronic/digital identity
Deleted: PINs,
Deleted: signing by a qualified trust service certificate
Deleted: ,
Formatted: Font: (Default) Times New Roman
Formatted: Font: (Default) Times New Roman