Fraud prevention and staying secure

Killik & Co are an independently owned Wealth Management firm, who help clients to plan and invest for the long term.

This document sets out how we aim to protect our clients and offers some general guidance on way to stay safe online.

Who we are and what we do

- Killik & Co are authorised and regulated by the Financial Conduct Authority and you can find us on their register *www.fca.org.uk/firms/financial-services-register*
- We help clients to plan and invest for the long term – as such we do not invest in crypto currencies (like Bitcoin) or have short term, urgent investment opportunities
- We do not cold call, so we will only contact clients or enquirers of Killik and Co or Silo services
- If you have any concerns, you can contact your Adviser, our Client Support or Silo Support

How we keep you secure

- We do not store passwords, as it is the best way to reduce the risk of targeted password attacks by hackers
- Instead, we use 'passwordless authentication', an approach adopted by a growing number of major technology and financial companies. It uses factors within a client's possession, like one-time codes, registered smartphones or biometrics (fingerprint etc), to verify a user's identity
- For those clients who struggle with technology, we have the ability to share visibility of your myKillik account with a trusted, nominated contact who can help you access secure correspondence and account information (without delegating any decision making), which is safer than sharing login details
- We provide client documents via our secure portal, myKillik and the Silo app, which complete regular security testing as per industry standards
- Custodians and administrators are major, global, regulated companies, with data protection and security that is highly scrutinised by other clients as well as Killik & Co
- We do not encourage you to send sensitive documentation via email and we do encourage any email attachments to be sent password protected
- We will never send bank details for transactions via email but instead are available via our secure port, myKillik or can be found on your statement
- Similarly, we will only make payments to clients to the bank details that have been verified and stored on our system
- Clients can change their bank details or address, through the myKillik app, by electronic forms (adobe) or by letter. Where this is not done through the app, which has additional layers of authentication, we also take steps to verify that these requests are genuine
- We expect security questions to be answered satisfactorily when the caller is unknown
- New clients complete identity verification and anti-fraud bank checks (conducted for anti-money laundering purposes) or facial recognition for all new Silo clients
- We also complete 'know your client' processes for Managed and Advised clients, which can also help to identify whether a third party is attempting to access a client account

- Any emails from our employees, including Advisers and support teams, will only ever be sent from an email ending *@killik.com* or *@silo.co.uk*
- Central emails such as service communications, marketing and things like statement alerts will always come from *@killikmail* and *@mail.silo.co.uk*
- We will never send correspondence from an address not listed on our website Killik.com

If you believe you have been a victim of fraud please contact *www.actionfraud.police.uk*.

General guidance for staying secure

- Beware of email hackers or fraudsters using email or phone, to request secure or personal information from you
- Domain spoofing is a common phishing technique used by scammers to trick individuals into believing they are receiving legitimate emails from a company or one of its employees. Scammers accomplish this by sending emails that appear to come from a genuine domain name but are actually sent from a different source
- To protect yourself from domain spoofing attacks, be cautious of emails with unusual or incorrect spelling of the domain name, or with additional words or letters. Additionally, scammers may create websites with slightly altered characters that make it seem like the website is legitimate. It is important to stay vigilant and double-check the website's URL for any discrepancies to avoid falling victim to such scams
- Never share your private information, especially passwords online.
- Do check social media privacy settings, update browser software, and install anti-virus software on devices
- For free advice and resources, you can visit the FCA's Scamsmart *www.fca.org.uk/scamsmart*

Contact details

Killik & Co:
Clientsupport@killik.com
+44 (0) 20 7337 0400

Silo support:
Support@silo.co.uk