Checking Client Identities – Our Policy

Reyker is a financial institution, regulated by the Financial Conduct Authority (FCA), which holds very large sums of client money and client assets. We are also registered with the Information Commissioner's Office as we hold client data. All of the client money, assets and data we hold must be protected for the benefit of our clients.

We pride ourselves on our integrity and excellence. So while we aim to provide you with the best possible service throughout your investment journey with us, we also have to ensure that we are performing our role in accordance with the laws and regulations in place. This means we will always follow the principles within the Data Protection Act and the FCA Handbook. We will also follow our own Terms and Conditions of Business, which is a contract between us and our clients, and which protect us as well as you.

As a custodian firm, various other protections also apply to the client money and client assets we hold. These include FCA rules, London Stock Exchange rules, EU rules, FSCS protections in some cases (with limits), and of course our own business policies and risk management procedures.

One of the main legal obligations we have is to take reasonable steps to help prevent financial crime, including fraud, cyber-crime, money laundering, terrorist financing, information security, and bribery and corruption. Some of our policies and procedures address the risk and compliance needs of fulfilling our obligations in order to prevent financial crime and to protect your assets, money and data. In addition, some of our policies are framed to take account of the needs of insurance companies, who cover our professional services and some of our liability risks.

There are numerous ways in which thieves and fraudsters may try to get access to your money, assets or personal data. These may include, but are not limited to, the following:

- Impersonating you (perhaps by intercepting your post to obtain personal details)
- Misrepresenting you, for example by claiming to have your authority when they do not
- Hacking into the online data that you keep yourself, and misusing it for their own gains
- Misusing your passwords if you have not kept them secure
- Using a mobile device stolen from you to access your accounts with us
- Attempting to change your address and bank details in order to try to divert funds from your account to theirs
- Trying to persuade you to move your investments to a place where they can be more easily stolen
- Impersonating or misrepresenting your financial adviser
- Impersonating or claiming to be a trustee
- Impersonating or claiming to be a spouse or other family member acting with authority
- Claiming that you are deceased and that they represent you as an executor or adviser
- Claiming that they have a Power of Attorney (when in reality it is fake, out of date or invalid).

In common with banks and building societies, we operate a number of procedures that are designed to help prevent such fraud and theft from occurring. We do not publish in detail what these procedures, methods and policies are, because we do not wish to compromise, weaken or negate our checks.

The application of our policies and procedures are strict and our staff do not have flexibility to ignore or vary them. So if you feel that our checks are onerous at times, please remember we are doing this in order to protect **your** money, assets and data. We may also have to complete our entire procedure and checks on more than one occasion, for example if you wish to make a transaction after a long period without any contact with us. Again, this is to protect you and to manage our risks.

We appreciate that every financial institution will have their own preferred methods and different standards of identity checking and financial crime prevention. But just because other institutions require what you may think to be less onerous things from you, is not a reason for us to change or reduce our policies and procedures. Our focus and principal role is protecting your money, assets and data as far as we reasonably can – so we will not change our policies or procedures, and put your money and assets at risk, simply to speed things up or appear less onerous. We will never ask you for your password.

However, there are ways in which you can help us be as efficient as possible in this area. You also have a duty to take all reasonable steps to help us prevent fraud and theft, and to look after your own money, assets and data. This includes:

- Being straightforward and honest with us from the outset and for as long as you are a client of ours
- Promptly reporting any errors or discrepancies that you notice in any aspects of your accounts or investments, so that any adverse consequences can be mitigated and corrections made promptly
- You may notice these matters from your contract notes (or by the absence of a contract note), or from your valuation statements or other correspondence
- Notifying us promptly when your address or contact details change, and co-operating with us when we require proof (this is a key way of helping us avoid fraudsters obtaining your money and assets)
- Recognising that photocopied of scanned information may have been tampered with, hence bearing with us when we require original or notarised documents
- Notifying us promptly when you change your name or any other personal information
- Safeguarding your personal data; do not give this over to third parties before being sure they are legitimate
- Be suspicious and vigilant of cold calls, emails or post requesting personal data or information about your accounts and investments.

If you have any doubts, please let us know. We are here to help you with all aspects of investing with us, and protecting your money, assets and data is key to this.

End.