6: Financial advisers

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Overview of the sector

6.1. Financial advisers give customers advice on their investment needs (typically for long-term savings and pension provision) and selecting the appropriate products.

Typical customers

6.2. The typical customers of financial advisers are personal clients (including high net worth individuals), trusts, companies. Some firms also advise charities.

6.3. Financial advisers, whether they only give advice or whether they act on behalf of their customers in dealing with a product provider, are subject to the full provisions of UK law and regulation relating to the prevention of money laundering and terrorist financing. The guidance in Part I therefore applies to financial advisers.

6.4. Other sectoral guidance in Part II that is relevant to financial advisers includes:

- Sector 7: *Life assurance, and life-related pensions and investment products*
- Sector 8: *Non-life providers of investment fund products*
- Sector 9: *Discretionary and advisory investment management*

6.5. Generally, financial advisers do not hold permission from the FSA to handle client money, so in practice there is unlikely to be any involvement in the placement stage of money laundering. There is, however, considerable scope for financial advisers being drawn in to the layering and integration stages.

6.6. Whether or not financial advisers hold permission to handle client money, they should consider whether their relationship with their customers means that the guidance in sector 5: *Wealth management* or in sector 9: *Discretionary and advisory investment management* applies more directly to them.

What are the money laundering or terrorist financing risks for financial advisers?

6.7. The vast majority of financial advice business is conducted on a face-to-face basis, and investors generally have easy access to the funds involved.

6.8. Some criminals may seek to use financial advisers as the first step in integrating their criminal property into the financial system.

6.9. The offences of money laundering or terrorist financing include aiding and abetting those trying to carry out these primary offences, which include tax evasion. This is the main risk generally faced by financial advisers. In carrying out its assessment of the risk the firm faces of becoming involved in money laundering or terrorist financing, or entering into an arrangement to launder criminal property, the firm must consider the risk related to the product, as well as the risk related to the client.

6.10. Clearly, the risk of being involved in money laundering or terrorist financing will increase when dealing with certain types of customer, such as offshore trusts/companies, politically exposed persons and customers from higher risk or non-FATF countries or jurisdictions, and may also be affected by other service features that a firm offers to its customers. Customer activity, too, such as purchases in secondary markets – for example, traded endowments – can carry a higher money laundering risk.

Customer due diligence

6.11. Having sufficient information about customers and beneficial owners, and using that information, underpins all other anti-money laundering procedures. A firm must not enter into a business relationship until the identity of all the relevant parties to the relationship has been verified in accordance with the guidance in Part I, Chapter 5. Depending on the nature of their business, firms should also have regard to the requirements of product providers (see Part II sectors, 7, 8 and 9).

6.12. When a full advice service is offered, the process will involve information gathering, an understanding of the customer's needs and priorities and anticipated funds available for investment. The amount of information held about a client will build over time, as there will often be ongoing contact with the customer in order to review their circumstances. However, the level of information held about a customer will be limited if business is transacted on an execution-only or direct offer basis and financial advisers should have an increased regard to the monitoring of business undertaken in this way.

Whose identity should be verified?

6.13. Guidance on who the customer is, whose identity has to be verified, is given in Part I, paragraphs 5.3.2 to 5.3.7. Guidance on who the beneficial owner is, whose identity also has to be verified, is given in Part I, paragraphs 5.3.8 – 5.3.13 generally, and in Part II sector 7, paragraph 7.56(v), specifically for investment bonds.

Private individuals

6.14. Guidance on verifying the identity of private individuals is given in Part I, paragraphs 5.3.68 to 5.3.114. Guidance on circumstances where it may be possible to use the source of funds as evidence of identity is given in Part I, paragraphs 5.3.92 to 5.3.96.

6.15. The firm’s risk assessment procedures will take account of the money laundering and terrorist financing risks identified in the sectors in which the relevant product provider operates (see paragraph 6.4). Customers may be assessed as presenting a higher risk of money laundering, whether because he is identified as being a PEP, or because of some other aspect of the nature of the customer, or his business, or its location, or because of the product features available. In such cases, the firm must conduct enhanced due diligence measures (see Part I, section 5.5) and will need to decide whether it should require additional identity information to be provided, and/or whether to verify additional aspects of identity. For such customers, the financial adviser will need to consider whether to require additional customer information (see Part I, section 5.5) and/or whether to institute enhanced monitoring (see Part I, section 5.7).

6.16. Some persons cannot reasonably be expected to produce the standard evidence of identity. This would include persons such as individuals in care homes, who may not have a passport or driving licence, and whose name does not appear on utility bills. Where customers cannot produce the standard identification evidence, reference should be made to the guidance set out in sector 1: *Retail banking*, Annex 1-I.

Non-personal customers

6.17. Guidance on verifying the identity of non personal customers is given in Part I, paragraphs 5.3.115 to 5.3.277. Categories of non personal customers that are likely to be of particular relevance to financial advisers are:

- Private companies (paragraphs 5.3.149 to 5.3.160)
- Partnerships and unincorporated businesses (paragraphs 5.3.163 to 5.3.177)
- Pension schemes (paragraphs 5.3.216 to 5.3.225)
- Charities, church bodies and places of worship (paragraphs 5.3.226 to 5.3.245)
- Other trusts and foundations (paragraphs 5.3.246 to 5.3.269)
- Clubs and societies (paragraphs 5.3.270 to 5.3.278)

Non face-to-face

6.18. Non face-to-face transactions can present a greater money laundering or terrorist financing risk than those conducted in person because it is inherently more difficult to be sure that the person with whom the firm is dealing is the person that they claim to be. Enhanced due diligence is required in these circumstances, and verification of identity undertaken on a non face-to-face basis should be carried out in accordance with the guidance given in Part I, paragraphs 5.5.10 to 5.5.17.

Using verification work carried out by another firm

6.19. The responsibility to be satisfied that a customer's identity has been verified rests with the firm entering into the transaction with the customer. However, where two or more financial services firms have an obligation to verify the identity of the same customer in respect of the same transaction, in certain circumstances one firm may use the verification carried out by another firm. Guidance on the circumstances in which such an approach is possible, and on the use of pro-forma confirmation documentation, is given in Part I, section 5.6.

6.20. Financial advisers should bear in mind that they are often the party which is carrying out the initial customer identification and verification process. As such, it is they who will be asked to confirm to a product or service provider that such verification has been carried out. Although not directly related to the sort of work that financial advisers typically carry out, the significance of issuing such confirmations is highlighted by the actions of the FSA in 2005 in fining a bond broker who gave such conformation when he was aware that he had not, in fact, carried out appropriate customer due diligence.

6.21. Product providers often rely on customer verification procedures carried out by financial advisers, which underlines the importance of their systems and procedures for risk assessment being effective.

6.22. Where the financial adviser has carried out verification of identity on behalf of a product provider, the adviser must be able to make available to the product provider, on request, copies of the identification and verification data and other relevant documents on the identity of the customer or beneficial owner obtained by the adviser (see paragraph 6.29). This obligation extends throughout the period for which the financial adviser has an obligation under the ML Regulations to retain these data, documents or other information.

Suspicious transactions

6.23. Financial advisers are ideally placed to identify activity which is abnormal, or which does not make economic sense, in relation to a person's circumstances. Obtaining details on the source of a customer's wealth, and identifying the purpose of an activity are all mandatory parts of the normal advice process. Financial advisers do not have to handle the transaction personally to have an obligation to report it.

6.24. Guidance on monitoring customer transactions and activity is set out in Part I, section 5.7. Guidance on internal reporting, reviewing internal reports and making appropriate external reports to SOCA, is given in Part I, Chapter 6. This includes guidance on when a firm needs to seek consent to proceed with a suspicious transaction, with which financial advisers need to be familiar.

Staff awareness and training

6.25. One of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risks of money laundering/terrorist financing and well trained in the identification of unusual activities or transactions, which may prove to be suspicious.

6.26. Guidance on staff awareness, training and alertness is given in Part I, Chapter 7. This guidance includes suggested questions that staff should be asking themselves, and circumstances that should cause them to ask further questions about particular transactions or customer activity.

Record-keeping

6.27. General guidance on record-keeping is given in Part I, Chapter 8. The position of financial advisers means that some of the guidance in Part I, Chapter 8 cannot easily be applied. Generally, financial advisers will verify customers' identities by means of documentation, as they will often not have access to electronic sources of data. Where documents are used, it is preferable to make and retain copies.

6.28. In circumstances where a financial adviser is unable to take a record of documents used to verify identity, (e.g., when at a customer's home) he/she should keep a record of the type of document, its number, date and place of issue, as proof of identity, so that, if necessary, the document may be re-obtained from its source of issue.

6.29. Financial advisers may, from time to time, be asked by product providers for copies of the identification evidence that they took in relation to a particular customer. Financial advisers' record-keeping arrangements must therefore be capable of enabling such material to be provided in a timely manner (see Part I, paragraph 5.6.18).

6.30. Documents relating to customer identity must be retained for five years from the date the business relationship with the customer has ended (see Part I, paragraph 8.12).