

Retention of Records

12.1 General Principles and Objectives

FATF Recommendation 12 states:

Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the accounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour. Financial institutions should keep records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the account is closed.

These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.

When carrying out their investigations, enforcement agencies rely to a large extent on the integrity of documentation and information supplied by financial institutions. A financial institution should be able, within a reasonable time and if requested by the appropriate authorities, to demonstrate whether a particular person is its customer or the beneficial owner of assets deposited or invested, or has effected cash transactions requiring identification. In addition, the financial institution should be able to identify all of the accounts, products and services from which the person

identified is entitled to benefit.

The records prepared and maintained by any financial institution on its customer relationships and transactions should be such that:

- ❖ requirements of legislation are fully met;
- ❖ competent third parties will be able to judge reliably the institution's transactions and its observance of any policies and procedures;
- ❖ any transactions effected via the institution can be reconstructed;
- ❖ all suspicion reports received internally, and those made externally, can be identified;
- ❖ the institution can satisfy within a reasonable time any enquiries or orders from the appropriate authorities as to disclosure of information.

12.2 Identity Records

Records retained must indicate the nature of the evidence of identity obtained and comprise either a copy of the evidence or provide information which would enable a copy of it to be obtained or details of identity to be re-obtained. Sometimes legislation demands that actual copies must always be retained.

Records should indicate that the originals of identification documents have been seen. The records containing evidence of identity must be kept for the period specified in the national legislation after the relationship with the customer has ended. The date when the relationship with the customer has ended is not always clear. Experience indicates that it should be considered as the date of:

- ❖ the carrying out of a one-off transaction or the last in the series of transactions; or
- ❖ the ending of the business relationship, i.e. the closing of the account or accounts; or
- ❖ the commencement of proceedings to recover debts payable on insolvency.

Where formalities to end a business relationship have not been undertaken, but a period of five years has elapsed since the date when the last transaction was carried out, then the five-year retention period commences on the date of the completion of the last transaction.

12.3 Transaction Records

In the case of transactions undertaken on behalf of customers, the supporting evidence and records, consisting of the original documents or copies admissible in court proceedings, must be retained for the period specified in the legislation following the date on which the relevant transaction or series of transactions is completed. These will be records in support of entries in the accounts in whatever form they are used.

The investigating authorities need to be able to compile a satisfactory audit trail for suspected laundered money and to be able to establish a financial profile of any suspect account. For example, the following information may be sought as part of an investigation into money laundering:

- ❖ the beneficial owner of the account (for accounts where intermediaries are involved, the identification of beneficial owner may need to be by way of a chain of verification procedures undertaken through the intermediaries concerned);
- ❖ the volume of funds flowing through the account.

For selected transactions:

- ❖ the origin of the funds (if known);
- ❖ the form in which the funds were offered

or withdrawn, i.e. cash, cheques, etc.;

- ❖ the identity of the person undertaking the transaction;
- ❖ the destination of the funds;
- ❖ the form of instruction and authority.

Internal procedures need to ensure that *all transactions* undertaken on behalf of that customer are recorded on the customer's account. For example, a customer's records should include all requests for wire transfer transactions where settlement is provided in cash rather than by funds drawn from the customer's account or reinvested.

Where the records relate to ongoing investigations, they should be retained until it is confirmed by the relevant law enforcement agency that the case has been closed.

12.4 Records of Suspicion Reports

It is recommended that records of all suspicion reports received from staff and all external reports to the competent authorities should be retained for five years. Where the MLRO has considered information concerning a suspicion, but has not made a report to the authorities, a record of that information should be retained together with the reasons why the report was not considered to be valid.

12.5 Format and Retrieval of Records

12.5.1 Format of Records

It is recognised that financial institutions will find it necessary to rationalise their hard copy filing requirements. Most will have standard procedures which seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Documentation may therefore be kept in the form of original documents, microfiche copies, or computerised or electronic records, in a format that is admissible as evidence in court proceedings.

However, the record retention require-

ments are the same regardless of the format in which they are kept, or whether the transaction was undertaken by paper or by electronic means.

Documents held centrally must be capable of distinguishing between the transactions relating to different customers and of identifying where the transaction took place and in what form.

12.5.2 Retrieval of Records

The overriding objective is for firms to be able to retrieve relevant information without undue delay. Court Orders, granted to an investigating officer, will usually require that the information specified should be available within a specified number of days from the date of the service of the Order.

When setting document retention policy, financial institutions must weigh the statutory requirements and the needs of the investigating authorities against normal commercial considerations.

Nevertheless, financial institutions should ensure that when original documents, which would normally have been destroyed, are required for investigation purposes, they check that the destruction policy has actually been adhered to before informing the law enforcement agencies that the documents are not available.

12.5.3 Records Relating to Ongoing Investigations

Where the records relate to ongoing investigations, they should be retained until it is confirmed by the relevant law enforcement agency that the case has been closed.

12.6 Group Record Retention Policy

Where documents verifying the identity of a customer are held in one part of a group, they may not need to be held in duplicate form in another. However, if the documents are held in another jurisdiction, they must wherever possi-

ble (subject to local legislation) be freely available on request within the group, or otherwise be available to the investigating agencies under due legal procedures and mutual assistance treaties. Access to group records should not be impeded by confidentiality or data protection restrictions.

Financial institutions should also take account of the scope of money laundering legislation in other countries and should ensure that group records kept in other countries are retained for the required period.

Particular care needs to be taken to retain, or hand over, the appropriate records when an introducing branch or subsidiary ceases to trade or have a business relationship with a customer while the relationship with other group members continues. Such arrangements also need to be made if a company holding relevant records becomes detached from the rest of the group.

12.7 Wire Transfer Transactions

Investigations of major money laundering cases over the last few years have shown that criminals make extensive use of electronic payment and message systems. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the original ordering customer or the ultimate beneficiary is not clearly shown in an electronic payment message instruction.

In an effort to ensure that the SWIFT system is not used by criminals as a means to break the money laundering audit trail, SWIFT, at the request of the FATF on Money Laundering, has asked all users of its system to ensure that when sending SWIFT MT 100/103 messages (customer transfers), the fields for the ordering and beneficiary customers should be completed with their respective names and addresses.

Subject to technical limitations, ordering customers should be encouraged to include this information for all credit transfers made by

electronic means, both domestic and international, regardless of the payment or message system used. In cases where this is not contained in the message, full records of the ordering customer and address should be retained by the originating financial institution.

The transfer of funds where both ordering

and beneficiary customers are banks is exempt from this requirement. Records of electronic payments and messages must be treated in the same way as any other records in support of entries in the account and kept for a specified period.