13
Retention of Records

13.1 General Principles and Objectives

FATF Recommendation 10 states that:[12]

> *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 the identification data obtained through the customer due diligence process, (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.*
>
> *The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.*

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 if they are the beneficial owner of assets deposited or invested, or if they have effected cash transactions requiring identification. In addition, the financial institution should be able to identify all 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:

- The 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; and
- The institution can satisfy within a reasonable time any enquiries or orders from the appropriate authorities as to disclosure of information.

13.2 Identity Records

Records retained must:

- Indicate the nature of the evidence of identity obtained; and
- Comprise either a copy of the evidence or provide such information as would enable a copy of it to be obtained or sufficient to enable details of identity to be re-obtained. Sometimes legislation demands that actual copies must always 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.

13.3 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;
- 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; and
- 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 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.

13.4 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 money laundering reporting officer 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.

13.5 Format and Retrieval of Records

13.5.1 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, while still complying with statutory requirements. Retention may therefore be by way of original documents, documents stored on microfiche, or computerised or electronic records, subject to their being in a format that is admissible as evidence in court proceedings.

However, the record retention requirements 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.

13.5.2 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.

13.5.3 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.

13.6 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 possible (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 should 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.

13.7 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.

13.7.1 The Introduction of International Standards to Combat Terrorism

At an extraordinary plenary on the Financing of Terrorism held in Washington DC on 29–30 October 2001, the Financial Action Task Force (expanded its mission beyond money laundering. During the plenary, the FATF agreed on and issued new international standards to combat terrorist financing, which it calls on all countries to adopt and implement. The agreement on the Special Recommendations commits members, inter alia, to strengthen customer identification measures in international and domestic wire transfers. FATF Special Recommendation VII states:

> *Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.*
>
> *Countries should take measures to ensure that financial institutions, including money remitters conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).*

The FATF issued an Interpretative Note to Special Recommendation VII on 14 February 2003.

By November 2003, all banks worldwide will have migrated to SWIFT MT 103 message format which will incorporate designated fields to enable disclosure of the name, address and account number of the originator. The originator is defined as the account holder or, where there is no account, the person (natural or legal) that places the order with the financial services business to perform the wire transfer.

Until that date, banks worldwide will be building systems designed to populate these designated fields; the FATF recognises that there will need to be a sensible lead time in which to enable systems and procedures to be adopted, many of which will be developed at group level, which provide for compliance with FATF Recommendation VII: 'Wire Transfers' and its Interpretative Note. Time will also be required by all countries to consider and address any legal and customer security issues that may arise from implementation of FATF Recommendation VII. Consequently, many countries agreed to be in full compliance with Recommendation VII by January 2005.

Scope

The term *wire transfer* refers to any transaction carried out on behalf of an originator (both natural and legal persons) through a financial services business by electronic means with a view to making an amount of money available to a beneficiary at another financial services business. The originator and beneficiary may be the same person.

The term is not intended to cover the following types of payments:

- Any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction. However, when credit or debit cards are used as a payment system to effect a money transfer, they will be subject to the requirements for cross-border or domestic wire transfers, as appropriate.
- Transfers between financial institutions and settlements where both the originator person and the beneficiary person are financial services businesses acting on their own behalf.

Role of Ordering Financial Services Businesses

From the date of implementation, the ordering financial services business must ensure that qualifying wire transfers contain complete originator information, as set out below.

Cross-border wire transfers

Originator information accompanying cross-border wire transfers must always contain:

- the name of the originator, and where an account exists, the number of that account. In the absence of an account, a unique reference number must be included; and
- either the address of the originator, his/her national identity number, a customer identification number, or date and place of birth.

FATF Special Recommendation VII defines cross border transfer as any wire transfer where the originator and beneficiary are located in different jurisdictions.

Domestic wire transfers

Information accompanying domestic wire transfers must also include originator information as required for cross-border transfers, unless full originator information can be made available to the beneficiary financial services business and the FIU by other means. In this latter case, financial institutions may include only the account number of a unique identifier provided that this number will permit the transaction to be traced back to the originator.

Where financial institutions choose to benefit from the concession permitted for domestic transfers, the ordering business should be required to make complete originator information available within three days of receiving the request either from the beneficiary financial services business or the FIU.

FATF Special Recommendation VII defines a domestic transfer as any wire transfer where the originator and beneficiary institutions are located in the same jurisdiction. The term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the system used to affect the wire transfer may be located in another jurisdiction.

Role of Intermediary and Beneficiary Financial Services Businesses

From the date of implementation, financial institutions processing an intermediary element of a chain of wire transfers will be required to ensure that all originator information remains with the transfer or related message through the payment chain.

Where technical limitations prevent the full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer (during the necessary time to adapt payment systems), a record must be kept for five years by the receiving intermediary financial institution of all the information received from the ordering financial institution and made available on request to the beneficiary financial institution and to the FIU.

From the date of implementation, beneficiary financial institutions should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and, as appropriate, whether they are thus required to be reported to the FIU. In some cases, the beneficiary financial institution should consider restricting or even terminating its business relationship with financial institutions that fail to meet standards set in FATF Recommendation VII: Wire Transfers and its Interpretative Note.

13.7.2 Record Keeping

Records of electronic payments and messages must be treated in the same way as any other records in support of entries over an account and kept for a minimum of five years.