Chapter 3

Money laundering and terrorist financing

3

3.2 Themes

Governance

3.2.1 G The guidance in FCG 2.2.1G on governance in relation to financial crime also applies to money laundering. We expect senior management to take responsibility for the firm's anti-money laundering (AML) measures. This includes knowing about the money laundering risks to which the firm is exposed and ensuring that steps are taken to mitigate those risks effectively.

Regulation 21(1)(a) of the *Money Laundering Regulations* requires that where appropriate with regard to the size and nature of its business, *firms* subject to the regulations must appoint one individual who is a member of its board of directors (or if there is no board, of its equivalent *management body*) or of its *senior management* as the officer responsible for compliance with the regulations. Regulation 21(3) also requires the appointment of a nominated officer. Regulation 21(4) requires a *firm* to inform their supervisory authority of the identity of the individual appointed (including any subsequent appointments) within 14 *days* of such appointment.

As SYSC 6.3.9R and SYSC 3.2.6IR also require firms subject to those provisions to have an MLRO, the *FCA* expects that this individual can be the same individual appointed under Regulation 21(1)(a) and/or 21(3) of the *Money Laundering Regulations* and so *firms* do not need to make a separate notification to the FCA.

Self-assessment questions:

- Who has **overall responsibility** for establishing and maintaining effective AML controls? Are they sufficiently senior?
- What are the **reporting lines**?
- Do senior management receive **informative, objective information** that is sufficient to enable them to meet their AML obligations?
- How regularly do senior management commission **reports** from the **MLRO**? (This should be at least annually.) What do they do with the reports they receive? What **follow-up** is there on any recommendations the MLRO makes?
- How are senior management involved in **approving relationships** with high risk customers, including politically exposed persons (PEPs)?

Examples of good practice	Examples of poor practice
• **Reward structures** take account of any failings related to AML compliance.	• There is **little evidence** that AML is **taken seriously** by senior management. It is seen as a legal or **regulatory necessity** rather than a matter of true concern for the business.
• Decisions on accepting or maintaining high money laundering risk relationships are reviewed and challenged **independently** of the business relationship and escalated to senior management or committees.	• Senior management attach greater importance to the risk that a customer might be involved in a **public scandal**, than to the risk that the customer might be corrupt or otherwise engaged in financial crime.
• Documentation provided to senior management to inform decisions about entering or maintaining a business relationship provides an **accurate picture** of the risk to which the firm would be exposed if the business relationship were established or maintained.	• The board **never considers** MLRO reports.
• A UK parent undertaking meets the obligations under Regulation 20 of the *Money Laundering Regulations* including ensuring that AML policies, controls and procedures apply to all its branches and subsidiaries outside the UK.	• A UK branch or subsidiary uses group policies which **do not comply** fully with UK AML legislation and regulatory requirements.

The Money Laundering Reporting Officer (MLRO)

3.2.2 G This section applies to firms who are subject to the money laundering provisions in SYSC 3.2.6A – J or SYSC 6.3, except it does not apply to sole traders who have no employees.

Firms to which this section applies must appoint an individual as MLRO. The MLRO is responsible for oversight of the firm's compliance with its anti-money laundering obligations and should act as a focal point for the firm's AML activity.

Self-assessment questions:

- Does the MLRO have sufficient resources, experience, access and seniority to carry out their role effectively?
- Do the firm's staff, including its senior management, consult the MLRO on matters relating to money-laundering?
- Does the MLRO escalate relevant matters to senior management and, where appropriate, the board?
- What awareness and oversight does the MLRO have of the highest risk relationships?

3

Examples of good practice	Examples of poor practice
• The MLRO is independent, knowledgeable, robust and well-resourced, and poses effective challenge to the business where warranted. • The MLRO has a direct reporting line to executive management or the board.	• The MLRO lacks credibility and authority, whether because of inexperience or lack of seniority. • The MLRO does not understand the policies they are supposed to oversee or the rationale behind them. • The MLRO of a firm which is a member of a group has not considered whether group policy adequately addresses UK AML obligations. • The MLRO is unable to retrieve information about the firm's high-risk customers on request and without delay and plays no role in monitoring such relationships.

See SYSC 3.2.6IR and SYSC 6.3.9R.

Risk assessment

3.2.3 G The guidance in FCG 2.2.4G on risk assessment in relation to financial crime also applies to AML.

The assessment of money laundering risk is at the core of the firm's AML effort and is essential to the development of effective AML policies and procedures. A firm is required by Regulation 18 of the *Money Laundering Regulations* to undertake a risk assessment.

Firms must therefore put in place systems and controls to identify, assess, monitor and manage money laundering risk. These systems and controls must be comprehensive and proportionate to the nature, scale and complexity of a firm's activities. Firms must regularly review their risk assessment to ensure it remains current.

Self-assessment questions:

- Which parts of the business present **greater risks** of money laundering? (Has your firm identified the risks associated with different types of customer or beneficial owner, product, transactions, business line, geographical location and delivery channel (e.g. internet, telephone, branches)? Has it assessed the extent to which these risks are likely to be an issue for the firm?)

- How does the risk assessment inform your day-to-day operations? (For example, is there evidence that it informs the level of customer due diligence you apply or your decisions about accepting or maintaining relationships?)

Examples of good practice	Examples of poor practice
• There is evidence that the firm's risk assessment informs the design of anti-money laundering controls.	• An inappropriate risk classification system makes it almost impossible for a relationship to be classified as 'high risk'.
• The firm has identified good sources of information on money laundering risks, such as National Risk Assessments, ESA Guidelines, FATF mutual evaluations and typology reports, NCA alerts, press reports, court judgements, reports by non-governmental organisations and commercial due diligence providers.	• Higher risk countries are allocated low-risk scores to avoid enhanced due diligence measures.
• Consideration of money laundering risk associated with individual business relationships takes account of factors such as: company structures; political connections; country risk; the customer's or beneficial owner's reputation; source of wealth; source of funds; expected account activity; sector risk; and involvement in public contracts.	• Relationship managers are able to **override customer risk scores** without sufficient evidence to support their decision.
• The firm identifies where there is a risk that a relationship manager might become too close to customers to identify and take an objective view of the money laundering risk. It manages that risk effectively.	• Risk assessments on money laundering are unduly influenced by the **potential profitability** of new or existing relationships. • The firm **cannot evidence** why customers are rated as high, medium or low risk. • A UK branch or subsidiary relies on group risk assessments without assessing their compliance with UK AML requirements.

See regulation 18 of the *Money Laundering Regulations*, ■ SYSC 3.2.6AR, ■ SYSC 3.2.6CR, ■ SYSC 6.3.1R and ■ SYSC 6.3.3R.

Customer due diligence (CDD) checks

3.2.4 G Firms must **identify** their customers and, where applicable, their beneficial owners, and then **verify** their identities. Firms must also understand the **purpose** and **intended nature** of the customer's relationship with the firm

3

and collect information about the customer and, where relevant, beneficial owner. This should be sufficient to obtain a complete picture of the risk associated with the business relationship and provide a meaningful basis for subsequent monitoring.

Firms should note that CDD measures also apply when contacting an existing customer as part of any legal duty in the course of a calendar year for the purpose of reviewing information which is relevant to the risk assessment of the customer, and relates to beneficial ownership of the customer.

Firms should also note that CDD measures must also be applied when the relevant person has to contact an existing customer in order to fulfil any duty under the International Tax Compliance Regulations 2015.

CDD measures must also include taking reasonable steps to understand the ownership and control structure of a customer where the customer is a legal person, trust, company, foundation or similar legal arrangement.

Firms are required to keep written records in circumstances where all possible means of identifying the beneficial owner of a *body corporate* have been taken and the beneficial cannot be identified satisfactorily or at all. In circumstances where the beneficial owner of a *body corporate* cannot be identified, reasonable measures must be taken to verify the identity of the senior person in the *body corporate* responsible for managing it. In doing so, firms should keep written records made of the actions taken and any difficulties encountered.

Firms are required to collect proof of company registration (or an excerpt from the register) before establishing a business relationship with certain legal entities including a company subject to the requirements of Part 21A of the Companies Act 2006, a limited liability partnership or an eligible Scottish partnership. Firms are required to report to Companies House discrepancies between this information and information which otherwise becomes available to them in the course of complying with the *Money Laundering Regulations*. Firms may wish to refer to further guidance from the Companies House.

In situations where the money laundering risk associated with the business relationship is increased, banks must carry out additional, enhanced due diligence (EDD). FCG 3.2.8G below considers enhanced due diligence.

Where a firm cannot apply customer due diligence measures, including where a firm cannot be satisfied that it knows who the beneficial owner is, it must not enter into, or continue, the business relationship.

Firms should note that an electronic identification process may be regarded as a reliable source for the purposes of CDD verification where that process is independent of the person whose identity is being verified, secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact that person with that identity.

Self-assessment questions:

- Does your firm apply **customer due diligence** procedures in a risk-sensitive way?
- Do your CDD processes provide you with a **comprehensive understanding** of the risk associated with individual business relationships?

- How does the firm **identify** the customer's **beneficial owner(s)**? Are you satisfied that your firm takes risk-based and adequate steps to verify the beneficial owner's identity in all cases? Do you understand the rationale for beneficial owners using complex corporate structures?

- Are procedures **sufficiently flexible** to cope with customers who cannot provide more common forms of identification (ID)?

Examples of good practice	Examples of poor practice
• A firm which uses e.g. **electronic verification checks** or **PEPs databases** understands their capabilities and limitations.	• Procedures are not **risk-based**: the firm applies the same CDD measures to products and customers of varying risk.
• The firm can cater for **customers who lack common forms of ID** (such as the socially excluded, those in care, etc).	• The firm has **no method for tracking** whether checks on customers are complete.
• The firm understands and documents the **ownership and control structures** (including the reasons for any complex or opaque corporate structures) of customers and their beneficial owners.	• The firm allows **language difficulties** or **customer objections** to get in the way of proper questioning to obtain necessary CDD information.
• The firm obtains information about the purpose and nature of the business relationship sufficient to be satisfied that it **understands** the **associated money laundering risk**.	• Staff do **less CDD** because a customer is referred by senior executives or influential people.
• Staff who approve new or ongoing business relationships satisfy themselves that the firm has obtained **adequate CDD** information before doing so.	• The firm has **no procedures** for dealing with situations requiring enhanced due diligence. **This breaches the** *Money Laundering Regulations*.
	• The firm fails to consider: any individuals who ultimately control more than 25% of shares or voting rights of a corporate customer; any individuals who exercise control over the management of a corporate customer; and any individuals who control the body corporate

3

Examples of good practice	Examples of poor practice
	when identifying and verifying the customer's beneficial owners. **This breaches the** *Money Laundering Regulations*.

See regulations 5, 6, 27, 28, 30A, 31, 33, 34 and 35 of the *Money Laundering Regulations*.

Ongoing monitoring

3.2.5 G A firm must conduct ongoing monitoring of its business relationships on a risk-sensitive basis. Ongoing monitoring means **scrutinising transactions** to ensure that they are consistent with what the firm knows about the customer, and taking steps to ensure that the firm's knowledge about the business relationship remains current. As part of this, firms must keep documents, data and information obtained in the CDD context (including information about the purpose and intended nature of the business relationship) up to date. It must apply CDD measures where it doubts the truth or adequacy of previously obtained documents, data or information (see FCG 3.2.4G).

Where the risk associated with the business relationship is increased, firms must carry out enhanced ongoing monitoring of the business relationship. FCG 3.2.9G provides guidance on enhanced ongoing monitoring.

Self-assessment questions:

- How are transactions **monitored** to spot potential money laundering? Are you satisfied that your monitoring (whether automatic, manual or both) is adequate and effective considering such factors as the size, nature and complexity of your business?
- Does the firm **challenge** unusual activity and explanations provided by the customer where appropriate?
- How are **unusual transactions** reviewed? (Many alerts will be false alarms, particularly when generated by automated systems. How does your firm decide whether behaviour really is suspicious?)
- How do you feed the **findings from monitoring** back into the customer's risk profile?

Examples of good practice	Examples of poor practice
• A large retail firm complements its other efforts to spot potential money laundering by using an **automated system** to monitor transactions	• The firm fails to take adequate measures to understand the risk associated with the business relationship and is therefore **unable to conduct meaningful monitoring**.
• Where a firm uses automated transaction monitoring systems, it understands their capabilities and limitations.	• The MLRO can provide **little evidence** that **unusual transactions** are brought to their attention.

Examples of good practice	Examples of poor practice
• Small firms are able to apply credible **manual procedures** to scrutinise customers' behaviour.	• Staff **always accept a customer's explanation** for unusual transactions at face value and do not probe further.
• The '**rules**' underpinning monitoring systems are understood by the relevant staff and updated to reflect new trends.	• The firm does not take risk-sensitive measures to ensure CDD information is **up to date. This is a breach of the** *Money Laundering Regulations*.
• The firm uses **monitoring results** to review whether CDD remains adequate.	
• The firm takes advantage of **customer contact** as an opportunity to update due diligence information.	
• **Customer-facing staff** are engaged with, but do not control, the ongoing monitoring of relationships.	
• The firm updates CDD information and reassesses the risk associated with the business relationship where monitoring indicates **material changes** to a customer's profile.	

See regulations 27, 28(11), 33, 34 of the *Money Laundering Regulations*.

Source of wealth and source of funds

3.2.6 G Establishing the source of funds and the source of wealth can be useful for ongoing monitoring and due diligence purposes because it can help firms ascertain whether the level and type of transaction is consistent with the firm's knowledge of the customer. It is a requirement where the customer is a PEP.

'Source of wealth' describes how a customer or beneficial owner acquired their total wealth.

'Source of funds' refers to the origin of the funds involved in the business relationship or occasional transaction. It refers to the activity that generated the funds, for example salary payments or sale proceeds, as well as the means through which the customer's or beneficial owner's funds were transferred.

The JMLSG's guidance provides that, in situations where the risk of money laundering/terrorist financing is very low and subject to certain conditions, firms may assume that a payment drawn on an account in the customer's name with a UK, EU or equivalent regulated credit institution satisfied the standard CDD requirements. This is sometimes referred to as 'source of funds as evidence' and is distinct from 'source of funds' in the context of Regulation 28(11) and Regulations 33 and 35 of the *Money Laundering*

Regulations and of *FCG*. Nothing in *FCG* prevents the use of 'source of funds as evidence' in situations where this is appropriate.

Where the customer is either a PEP, a family member of a PEP or known close associate of a PEP, a firm may have regard to guidance issued by the *FCA* on the treatment of PEPs.

[**Editor's Note:** see https://www.fca.org.uk/publications/finalised-guidance/fg17-6-treatment-politically-exposed-persons-peps-money-laundering.]

Handling higher risk situations

3.2.7 G The law requires that firms' anti-money laundering policies and procedures are sensitive to risks. This means that in higher risk situations, firms must apply enhanced due diligence and ongoing monitoring. **Situations that present a higher money laundering risk** might include, but are not restricted to: customers linked to higher risk countries or business sectors; or who have unnecessarily complex or opaque beneficial ownership structures; and transactions which are unusual, lack an obvious economic or lawful purpose, are complex or large or might lend themselves to anonymity.

Firms must take account of risk factors set out under regulation 33(6) which relate to customer risk, product risk and geographical risk when assessing whether there is a high risk of money laundering or terrorist financing in a particular situation and the extent of measures which should be taken to manage and mitigate that risk.

The ***Money Laundering Regulations*** **also set out some scenarios in which specific enhanced due diligence measures have to be applied:**

•**Correspondent relationships**: where a correspondent credit institution or financial institution is outside the EEA, the UK credit or financial institution should apply EDD measures commensurate to the risk of the relationship. This can include in higher risk situations thoroughly understanding its correspondent's business, reputation, and the quality of its defences against money laundering and terrorist financing. Senior management must also give approval before establishing a new correspondent relationship. JMLSG guidance sets out how firms should apply EDD in differing correspondent trading relationships.

•**Politically exposed persons (PEPs), family members and known close associates of a PEP**: a PEP is a person entrusted with a prominent public function, other than as a middle-ranking or more junior official. PEPs (as well as their family members and known close associates) must be subject to enhanced scrutiny. A senior manager at an appropriate level of authority must also approve the initiation of a business relationship with a PEP (or with a family member, or known close associate, of a PEP). This includes approving a relationship continuing with an existing customer who became a PEP after the relationship begun. In meeting these obligations firms may have regard to the *FCA's* guidance on a risk-based approach to PEPs.

•**Business relationships or a 'relevant transaction' where either party is established in a high risk third country**: the *Money Laundering Regulations* defines:

(a)a high-risk third country as being one identified by the EU Commission by a delegated act. See EU Regulation 2016/1675 (as amended from time to time);

(b)a relevant transaction as being a transaction in relation to which the relevant person is required to apply customer due diligence under Regulation 27;

(c)established in a country in the case of a legal person as being the country of incorporation or principal place of business, or, in the case of a financial institution or credit institution, where its principal regulatory authority is.

In these scenarios, EDD must include specified measures which include obtaining additional information on the customer, the beneficial owner, the intended nature of the business relationship, source of funds and wealth, reasons for the transactions and senior management approval for the business relationship. Conducting enhanced monitoring is also a requirement.

•**Other transactions**: EDD must be performed:

() in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose. In this scenario, there are specified EDD measures which must include, as far as reasonably possible, examining the background and purpose of the transaction and increasing the degree and nature of monitoring of the business relationship in which the transaction is made to determine whether that transaction or that relationship appears to be suspicious;

() in any other case which by its nature can present a higher risk of money laundering or terrorist financing.

Where the customer is the beneficiary of a life insurance policy, is a legal person or a legal arrangement, and presents a high risk of money laundering or terrorist financing for any other reason, credit and financial institutions must take reasonable measures to identify and verify the identity of the beneficial owners of that beneficiary before making a payment under the life insurance policy.

The extent of enhanced due diligence measures that a firm undertakes can be determined on a risk-sensitive basis. The firm must be able to demonstrate that the extent of the enhanced due diligence measures it applies is commensurate with the money laundering and terrorist financing risks.

See regulations 19, 20, 21, 28(16), 33 and 34 of the *Money Laundering Regulations*.

Handling higher risk situations – enhanced due diligence (EDD)

3.2.8 G Firms must apply EDD measures in situations that present a higher risk of money laundering.

EDD should give firms a **greater understanding** of the customer and their associated risk than standard due diligence. It should provide more certainty that the customer and/or beneficial owner is who they say they are and that the purposes of the business relationship are legitimate; as well as increasing opportunities to identify and deal with concerns that they are not. FCG 3.2.3G considers risk assessment.

The extent of EDD must be **commensurate to the risk** associated with the business relationship or occasional transaction but firms can decide, in most cases, which aspects of CDD they should enhance. This will depend on the reason why a relationship or occasional transaction was classified as high risk.

Examples of EDD include:

- obtaining more information about the customer's or beneficial owner's business
- obtaining more robust verification of the beneficial owner's identity based on information from a reliable and independent source
- gaining a better understanding of the customer's or beneficial owner's reputation and/or role in public life and assessing how this affects the level of risk associated with the business relationship
- carrying out searches on a corporate customer's directors or other individuals exercising control to understand whether their business or integrity affects the level of risk associated with the business relationship
- establishing how the customer or beneficial owner acquired their wealth to be satisfied that it is legitimate
- establishing the source of the customer's or beneficial owner's funds to be satisfied that they do not constitute the proceeds from crime.

Self-assessment questions:

- How does EDD differ from standard CDD? How are issues that are flagged during the due diligence process **followed up** and **resolved**? Is this adequately documented?
- How is EDD information **gathered, analysed, used** and **stored**?
- What involvement do senior management or committees have in **approving high risk customers**? What information do they receive to inform any decision-making in which they are involved?

Examples of good practice	Examples of poor practice
• The MLRO (and their team) have **adequate oversight** of all high risk relationships.	• Senior management **do not give approval** for taking on high risk customers. **If the customer is a PEP or a non-EEA correspondent , this breaches the** *Money Laundering Regulations*.
• The firm establishes the legitimacy of, and documents, the **source of wealth** and **source of funds** used in high risk business relationships.	• [deleted]
• Where money laundering risk is very high, the firm obtains **independent** internal or **external intelligence** reports.	• The firm **does not distinguish** between the customer's source of funds and their source of wealth.

Examples of good practice	Examples of poor practice
• When assessing EDD, the firm **complements staff knowledge** of the customer or beneficial owner with more objective information.	• The firm relies entirely on a **single source** of information for its enhanced due diligence.
• The firm is able to provide evidence that relevant information staff have about customers or beneficial owners is **documented and challenged** during the CDD process.	• A firm relies on intra-group introductions where **overseas standards are not UK-equivalent** or where due diligence data is **inaccessible** because of legal constraints.
• A member of a group satisfies itself that it is appropriate to rely on due diligence performed by **other entities** in the same group.	• The firm considers the **credit risk** posed by the customer, but not the **money laundering risk**.
• The firm proactively **follows up gaps in, and updates,** CDD of higher risk customers.	• The firm **disregards** allegations of the customer's or beneficial owner's **criminal activity** from reputable sources repeated over a sustained period of time.
• A correspondent bank seeks to **identify PEPs** associated with their respondents	• The firm ignores adverse allegations simply because customers hold a UK **investment visa**.
• . A correspondent bank takes a view on the strength of the **AML regime** in a respondent bank's home country, drawing on discussions with the respondent, overseas regulators and other relevant bodies.	• A firm grants **waivers** from establishing source of funds, source of wealth or other due diligence without good reason.
• A correspondent bank gathers information about **respondent banks' procedures** for sanctions screening, PEP identification and management, account monitoring and suspicious activity reporting.	• A correspondent bank conducts inadequate due diligence on **parents** and **affiliates** of respondents.
	• A correspondent bank **relies exclusively** on the Wolfsberg Group AML questionnaire.

See regulations 33, 34, 34(1)(d), 35 and 35(5)(a) of the *Money Laundering Regulations*.

Handling higher risk situations – enhanced ongoing monitoring

3.2.9 G Firms must enhance their ongoing monitoring in higher risk situations.

Self-assessment questions:

- How does your firm **monitor** its high risk business relationships? How does enhanced ongoing monitoring differ from ongoing monitoring of other business relationships?

•Are reviews carried out **independently** of relationship managers?

•What **information** do you store in the files of high risk customers? Is it useful? (Does it include risk assessment, verification evidence, expected account activity, profile of customer or business relationship and, where applicable, information about the ultimate beneficial owner?)

Examples of good practice	Examples of poor practice
• Key AML staff have a **good understanding** of, and **easy access** to, information about a bank's highest risk customers.	• The firm treats annual reviews as a **tick-box exercise** and copies information from previous reviews without thought.
• New higher risk clients are more closely monitored to confirm or amend **expected account activity**.	• A firm in a group relies on others in the group to carry out monitoring **without understanding** what they did and what they found.
• **Alert thresholds** on automated monitoring systems are lower for PEPs and other higher risk customers. Exceptions are **escalated** to more senior staff.	• There is **insufficient challenge** to explanations from relationship managers and customers about unusual transactions.
• Decisions across a group on whether to keep or exit high risk relationships are **consistent** and in line with the firm's overall risk appetite or assessment.	• The firm **focuses too much** on **reputational or business issues** when deciding whether to exit relationships with a high money laundering risk.
	• The firm makes no enquiries when accounts are used for purposes **inconsistent with expected** activity (e.g. personal accounts being used for business).

See regulation 33(1) of the *Money Laundering Regulations*.

Liaison with law enforcement

3.2.10 G Firms must have a **nominated officer**. The nominated officer has a legal obligation to **report any knowledge or suspicions** of money laundering to the National Crime Agency (NCA) through a 'Suspicious Activity Report', also known as a 'SAR'. (See FCG Annex 1 list of common terms for more information about nominated officers and Suspicious Activity Reports.)

Staff must report their concerns and may do so to the firm's nominated officer, who must then consider whether a report to NCA is necessary based on all the information at their disposal. Law enforcement agencies may seek information from the firm about a customer, often through the use of Production Orders (see FCG Annex 1).

Self-assessment questions:

•Is it clear who is **responsible** for different types of liaison with the authorities?

3

•How does the **decision-making** process related to **SARs** work in the firm?

•Are procedures clear to staff?

•Do staff report suspicions to the **nominated officer**? If not, does the nominated officer take steps to identify why reports are not being made? How does the nominated officer deal with reports received?

•What evidence is there of the rationale **underpinning decisions** about whether a SAR is justified?

•Is there a documented process for responding to **Production Orders**, with clear timetables?

Examples of good practice	Examples of poor practice
• All staff **understand procedures for escalating suspicions** and follow them as required.	• The nominated officer **passes all internal reports** to NCA without considering whether they truly are suspicious. These 'defensive' reports are likely to be of little value.
• The firm's **SARs** set out a clear narrative of events and include detail that law enforcement authorities can use (e.g. names, addresses, passport numbers, phone numbers, email addresses).	• The nominated officer **dismisses concerns** escalated by staff without reasons being documented.
• SARs set out the reasons for suspicion in **plain English**. They include some context on any previous related SARs rather than just a cross-reference.	• The firm **does not train** staff to make internal reports, thereby exposing them to personal legal liability and increasing the risk that suspicious activity goes unreported.
• There is a clear process for **documenting** decisions.	• The nominated officer **turns a blind eye** where a SAR might harm the business. **This could be a criminal offence**.
• A firm's processes for dealing with suspicions reported to it by **third party administrators** are clear and effective.	• A firm provides extraneous and irrelevant detail in response to a **Production Order**.

See regulation 21 of the *Money Laundering Regulations* and s.330 POCA and s.331 POCA and s.21A of the Terrorism Act 2000.

Record keeping and reliance on others

3.2.11 G Firms must keep copies of any documents and information obtained to meet CDD requirements and sufficient supporting records for transactions for **five years** after the business relationship ends or five years after an occasional transaction. However, records relating to transactions occurring in a business relationship need not be kept beyond 10 years. Where a firm is **relied on by others** to do due diligence checks, it must keep its records of those checks for the same time period. Firms must keep records sufficient to demonstrate to us that their CDD measures are appropriate in view of the risk of money

3

laundering and terrorist financing. Regulation 40(5) requires that any data collected is deleted after these periods. Regulation 41 also sets out that personal data collected under the *Money Laundering Regulations* should only be processed for the purposes of preventing money laundering or terrorist financing.

Self-assessment questions:

- Can your firm retrieve records **promptly** in response to a Production Order?
- If the firm **relies on others** to carry out AML checks (see 'Reliance' in FCG Annex 1), is this within the limits permitted by the *Money Laundering Regulations*? How does it satisfy itself that it can rely on these firms?

Examples of good practice	Examples of poor practice
• Records of customer ID and transaction data can be **retrieved quickly and without delay**.	• The firm keeps customer records and related information in a way that **restricts** the **firm's access** to these records or their timely sharing with authorities.
• Where the firm routinely relies on checks done by a third party (for example, a fund provider relies on an IFA's checks), it **requests sample documents** to test their reliability.	• A firm cannot access CDD and related records for which it has relied on a third party. **This breaches the** *Money Laundering Regulations*.
	• Significant proportions of CDD records **cannot be retrieved** in good time.
	• The firm has not considered whether a **third party** consents to being relied upon.
	• There are **gaps** in customer records, which cannot be explained.

See regulations 28(16), 40 and 40(7) of the *Money Laundering Regulations*.

Countering the finance of terrorism

3.2.12 G Firms have an important role to play in providing information that can assist the authorities with counter-terrorism investigations. Many of the controls firms have in place in relation to terrorism will overlap with their anti-money laundering measures, covering, for example, risk assessment, customer due diligence checks, transaction monitoring, escalation of suspicions and liaison with the authorities.

Self-assessment questions:

- How have **risks** associated with terrorist finance been assessed? Did assessments consider, for example, risks associated with the customer base, geographical locations, product types, distribution channels, etc.?

- Is it clear who is responsible for **liaison with the authorities** on matters related to countering the finance of terrorism? (See FCG 3.2.10G)

Examples of good practice	Examples of poor practice
• The firm has and uses an effective **process** for liaison with the authorities.	• Financial crime **training** does not mention terrorist financing.
• A firm identifies **sources of information** on terrorist financing risks: e.g. press reports, NCA alerts, Financial Action Task Force typologies, court judgements, etc.	• A firm doing cross-border business has not assessed terrorism-related risks in **countries** in which it has a presence or does business.
• This information informs the design of **transaction monitoring systems**.	• A firm has not considered if its approach to **customer due diligence** is able to capture information relevant to the risks of terrorist finance.
• Suspicions raised within the firm inform its own **typologies**.	

Customer payments

3.2.13 G This section applies to banks subject to SYSC 6.3.

Interbank payments can be abused by criminals. International policymakers have taken steps intended to increase the transparency of interbank payments, allowing law enforcement agencies to more easily trace payments related to, for example, drug trafficking or terrorism. The Funds Transfer Regulation requires banks to collect and attach information about payers and payees of wire transfers (such as names and addresses, or, if a payment moves within the EU, a unique identifier like an account number) to payment messages. Banks are also required to check this information is present on inbound payments, and chase missing data. The *FCA* has a legal responsibility to supervise banks' compliance with these requirements. Concerns have also been raised about interbank transfers known as "cover payments" (see FCG Annex 1) that can be abused to disguise funds' origins. To address these concerns, the SWIFT payment messaging system now allows originator and beneficiary information to accompany these payments.

Self-assessment questions:

- How does your firm ensure that customer payment instructions contain **complete payer and payee information**? (For example, does it have appropriate procedures in place for checking payments it has received?)

- Does the firm review its **respondent banks'** track record on providing payer data and using appropriate SWIFT messages for cover payments?

- Does the firm use guidance issued by the ESAs? [**Editor's Note:** see http://www.eba.europa.eu/-/esas-provide-guidance-to-prevent-terrorist-financing-and-money-laundering-in-electronic-fund-transfers.].

3

3

Examples of good practice	Examples of poor practice
• Following processing, banks conduct **risk-based sampling** for inward payments to identify inadequate payer and payee information.	• A bank fails to make use of the correct **SWIFT message type** for cover payments.
• An intermediary bank chases up **missing** information.	• Compliance with regulations related to international customer payments has not been reviewed by the firm's **internal audit** or compliance departments.
	The following practices breach the Funds Transfer Regulation:
• A bank sends dummy messages to test the effectiveness of filters.	International customer payment instructions sent by the payer's *bank* **lack meaningful payer and payee information**.
• A bank is aware of guidance from the **Basel Committee** and the **Wolfsberg Group** on the use of cover payments, and has considered how this should apply to its own operations.	An intermediary bank **strips** payee or payer information from payment instructions before passing the payment on.
• The quality of payer and payee information in payment instructions from **respondent banks** is taken into account in the bank's ongoing review of correspondent banking relationships.	The payee bank does not check any **incoming payments** to see if they include complete and meaningful data.
• The firm actively engages in **peer discussions** about taking appropriate action against banks which persistently fail to provide complete payer information.	

Case study – poor AML controls

3.2.14 G The *FSA* fined Alpari (UK) Ltd, an online provider of foreign exchange services, £140,000 in May 2010 for poor anti-money laundering controls.

•Alpari failed to carry out satisfactory customer due diligence procedures at the account opening stage and failed to monitor accounts adequately.

- These failings were particularly serious given that the firm did business over the internet and had customers from higher risk jurisdictions.

- The firm failed to ensure that resources in its compliance and anti-money laundering areas kept pace with the firm's significant growth.

Alpari's former money laundering reporting officer was also fined £14,000 for failing to fulfil his duties.

See the *FSA's* press release for more information: www.fsa.gov.uk/pages/Library/Communication/PR/2010/077.shtml

Case studies – wire transfer failures

3.2.15 G A UK bank that falls short of our expectations when using payment messages does not just risk *FCA* enforcement action or prosecution; it can also face criminal sanctions abroad.

In January 2009, Lloyds TSB agreed to pay US$350m to US authorities after Lloyds offices in Britain and Dubai were discovered to be deliberately removing customer names and addresses from US wire transfers connected to countries or persons on US sanctions lists. The US Department of Justice concluded that Lloyds TSB staff removed this information to ensure payments would pass undetected through automatic filters at American financial institutions. See its press release: www.usdoj.gov/opa/pr/2009/January/09-crm-023.html.

In August 2010, Barclays Bank PLC agreed to pay US$298m to US authorities after it was found to have implemented practices designed to evade US sanctions for the benefit of sanctioned countries and persons, including by stripping information from payment messages that would have alerted US financial institutions about the true origins of the funds. The bank self-reported the breaches, which took place over a decade-long period from as early as the mid-1990s to September 2006. See the US Department of Justice's press release: www.justice.gov/opa/pr/2010/August/10-crm-933.html.

Case study – poor AML controls: PEPs and high risk customers

3.2.16 G The *FSA* fined Coutts & Company £8.75 million in March 2012 for poor AML systems and controls. Coutts failed to take reasonable care to establish and maintain effective anti-money laundering systems and controls in relation to their high risk customers, including in relation to customers who are Politically Exposed Persons.

- Coutts failed adequately to assess the level of money laundering risk posed by prospective and existing high risk customers.

- The firm failed to gather sufficient information to establish their high risk customers' source of funds and source of wealth, and to scrutinise appropriately the transactions of PEPs and other high risk accounts.

- The firm failed to ensure that resources in its compliance and anti-money laundering areas kept pace with the firm's significant growth.

These failings were serious, systemic and were allowed to persist for almost three years. They were particularly serious because Coutts is a high profile bank with a leading position in the private banking market, and because the weaknesses resulted in an unacceptable risk of handling the proceeds of crime.

This was the largest fine yet levied by the *FSA* for failures related to financial crime.

See the *FSA's* press release for more information: www.fsa.gov.uk/library/communication/pr/2012/032.shtml

Poor AML controls: risk assessment

3.2.17 G The *FSA* fined Habib Bank AG Zurich £525,000, and its MLRO £17,500, in May 2012 for poor AML systems and controls.

Habib Bank AG Zurich failed adequately to assess the level of money laundering risk associated with its business relationships. For example, the firm excluded higher risk jurisdictions from its list of high risk jurisdictions on the basis that it had group offices in them.

- Habib Bank AG Zurich failed to conduct timely and adequate enhanced due diligence on higher risk customers by failing to gather sufficient information and supporting evidence

- The firm also failed to carry out adequate reviews of its AML systems and controls.

- The MLRO failed properly to ensure the establishment and maintenance of adequate and effective anti- money laundering risk management systems and controls.

See the *FSA's* press release for more information: www.fsa.gov.uk/library/communication/pr/2012/055.shtml