LLOYD'S

Market Bulletin

Ref: Y5424

Title	**Anti Money Laundering, Countering Financing of Terrorism, and Proliferation Finance – Implications for Insurers**
Purpose	To provide guidance to Market Participants on the UK's anti-money laundering, countering financing of terrorism, and proliferation finance regimes.
Type	Event
From	Chris Po-Ba Head of Sanctions Financial Crime Advisory (Market) t: +44 (0)20 7327 5473
Date	19 February 2024

PURPOSE

This market bulletin outlines the UK's money laundering (ML), countering financing of terrorism (CFT) and proliferation financing (PF) requirements as they relate to the insurance industry. These requirements are governed by the Proceeds of Crime Act 2002 (PoCA), the Terrorism Act 2000 (TACT) and, for life insurance, the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs).

This bulletin also provides guidance and best practice recommendations on ML, CFT and PF risks set out by the Financial Action Task Force (FATF), National Crime Agency (NCA), Financial Conduct Authority (FCA), Joint Money Laundering Steering Group (JMLSG), Lloyd's and the Lloyd's Market Association (LMA).

Contained in this Bulletin:

- A summary consolidating best practice recommendations; red flags for ML, CFT and PF risks; and reporting requirements.
- Appendices 1-4 provide expanded guidance on ML, CFT and PF for general insurance and life syndicates; reporting requirements; and possible offences.

BACKGROUND

FATF sets international standards for national authorities to implement and prevent ML, terrorist financing and PF. In the UK, these standards form the basis of the MLRs (as well as retained EU legislation from EU directives on ML).

Money Laundering

UK general insurance falls outside the regulated sector for ML, and general insurers are neither governed by the MLRs, nor the FCA's Senior Management Arrangements, Systems and Controls (SYSC) requirements specific to ML as specified within the FCA Handbook. Managing agents are however at risk of ML offences under Part 7 of PoCA and the TACT where applicable and should still adopt a risk-based approach in implementing anti money-laundering (AML) controls. Expanded guidance on the relationship between the UK MLRs and insurance business is provided in Appendices 1 and 2.

ML is defined under PoCA as "*the process by which the proceeds of crime are converted into assets which appear to have a legitimate origin, so that they can be retained permanently or recycled into further criminal enterprises*". The process of ML can be broken down into three stages:

- Placement – where illicit funds are introduced to the financial system in such a way as to make them appear legitimate, and to mix them with legitimate funds.

- Layering – the creation of a complex sequence of transactions intended to obscure the origin of illicit funds and to distance the launderer from the illicit activities. This is the most likely stage at which insurers can become involved.

- Integration – criminal proceeds appear legitimate and are successfully integrated into the economy.

All serious acquisitive crimes are likely to involve ML where property or benefits have been gained illegally through activity such as bribery and corruption, fraud, theft, tax evasion, and the handling and facilitation of criminal or terrorist property.

While the UK's 2020 national risk assessment considers the risk of ML within the insurance sector to be comparatively lower than in other sectors, some risk still remains. The assessment notes that this risk increases within the London insurance market where cover is provided in "high risk jurisdictions, trades and industries". All insurers should therefore maintain appropriate measures to mitigate potential ML activity while conducting business.

Counter Terrorist Financing

The TACT defines "terrorist property" as money or other property likely to be used for the purposes of terrorism, or which are themselves the proceeds of terrorism. CFT is concerned with the identification and denial of such terrorist property where it can be found within the financial system. Insurers may be inadvertently exposed to terrorist financing where, for instance, illicit actors attempt to launder terrorist property using insurance products; use the benefits of insurance products for the purpose of terrorism; or attempt to purchase services

using the proceeds of terrorism. By maintaining effective CFT due diligence processes, insurers can mitigate their risk.

Proliferation Financing

Regulation 16A of the MLRs define PF in part as the provision of "funds or financial services" for activities "in connection with the possession or use of chemical, biological, radiological or nuclear (CBRN) weapons". Research conducted by the Royal United Services Institute (RUSI) highlights the role that the insurance industry can play in supporting global efforts to counter the proliferation of these weapons, especially where parties may attempt to exploit the London insurance market to facilitate the movement of CBRN materiel.

IMPLICATIONS FOR THE MARKET

Managing agents should familiarise themselves with their obligations under PoCA and TACT, ensuring that robust procedures are in place to comply with those obligations. While UK general insurance is not governed by the MLRs or the FCA's SYSC requirements specific to ML, managing agents should still be proactive in mitigating ML, CFT and PF risks. It is expected that they should apply appropriate customer due diligence (CDD), including Know Your Customer (KYC) checks in conjunction with existing sanctions screening to ensure the legitimacy of all clients and business.

Managing agents writing life business, including under a group life policy or any other form of long-term insurance as defined under the Financial Services and Markets Act 2000, should ensure that they are compliant with the MLRs in addition to the regulated sector offences under PoCA and TACT, referring to JMLSG guidance parts I, II and III where relevant.

Insurers may wish to review both FATF's publication on methods and trends, as well as the Council of Europe's Typology Research on red-flag indicators for ML within the insurance sector for further information on KYC and CDD requirements.

SUMMARY OF RECOMMENDATIONS

As detailed within the appendices to this market bulletin, the following consolidates best practice recommendations to manage ML, CFT and PF risk.

Insurers should:

- Develop a well-documented Governance Framework for escalation of identified risks.
- Implement an Enterprise-Wide Risk Assessment (EWRA) of ML, CFT and PF.
- Conduct regular review of relevant financial crime publications, regulatory alerts and guidance including HM Treasury Advisory notices on the status of ML and CFT controls in high risk third countries, as well as FATF's public statements on jurisdictions with deficiencies in their AML/CFT regimes.
- Maintain robust and well-documented processes on how to report internally (known as an ISAR – Internal Suspicious Activity Report) and for relevant staff on how to complete an

external Suspicious Activity Report (SAR). For external reporting this may include guidance for relevant staff on how to report to the NCA via their SAR portal, the consequences of failing to report, and the "tipping-off" offence.

- Appoint a Money Laundering Reporting Officer (MLRO) or other Nominated Officer for assessing SARs and engaging with the NCA or other relevant authorities and law enforcement, ensuring that staff are aware of how to contact their MLRO or Nominated Officer. Lloyd's requires each managing agent to appoint an MLRO or Nominated Officer to act as the focal point for all activity relating to ML, regardless of whether the managing agent is conducting general insurance or regulated business.

- Implement automated responses to advise on the risk of a "tipping-off" offence if the MLRO inbox is used for submission of reports.

- Implement policies, procedures, and training for all staff on recognising suspicious activity and expectations for appropriate due diligence.

- Develop monitoring and assurance processes, including post-bind review, analysis of payments including overpayment and return premium, and sample testing by the second line of defence to ensure that underwriters are correctly identifying ML, CFT and PF red flags and actioning appropriately.

- Recognise responsibility for AML compliance, even where reliant on third parties.

RED FLAG INDICATORS

The Council of Europe's Typology Research offers some of the following red flag indicators for ML activity within the insurance industry:

New Business

- Difficulties and delays in obtaining copies of accounts or other documents of incorporation about a new corporate / trust insured.

- Reluctance to provide information about the ownership of a risk (or source of funds) which is difficult to verify.

- Numerous uses of offshore accounts, companies / structures in circumstances where the insured's needs do not support such economic requirements.

- No discernible reason for seeking the insurance in question, including insureds whose requirements are not in the normal pattern of business.

- Transactions involving third parties whose involvement becomes apparent at a later stage.
- Insureds showing no interest in the performance / general terms of the policy but interested in the early cancellation of the contract.

- Transactions which have no apparent purpose, make no obvious economic sense, and appear unrealistic, illegal or unethical.

- Requests to insure goods or assets in transit to or situated in countries where terrorism, the production of drugs, drug trafficking or an organised criminal activity may be prevalent, or which are the subject of FATF warning notices, on their high risk or increased monitoring list, or listed as high risk on the Transparency International Corruption Perceptions Index.

Payment

Large and unusual payments (including insurance premiums and injections of capital) may indicate that further due diligence is required, such as:

- The insured purchases policies for an amount which is beyond their apparent means.
- Overpayment of premium / capital, with a request to pay the excess to a third-party or in a foreign currency.
- Attempts to use a third-party cheque when purchasing a policy or payment in cash when the type of business transaction in question would normally be handled by credit or debit cards or other methods of payment.

Intermediaries / Brokers

The use of intermediaries may obscure the insured's identity and activities from the insurer. It is therefore important that managing agents understand how business is being procured, including the identity of all intermediaries in the placing chain. The following situations may give rise to suspicions and may warrant further enquiry:

- Unnecessarily complex placing chains.
- Excessive commission paid to an intermediary or the involvement of an intermediary whose role appears superfluous.
- The overseas intermediary is based in a jurisdiction which has ineffective, poorly enforced or no ML legislation.
- Results of an audit which reveals premium financing arrangements between insureds and intermediaries, which may obscure source of funds or large, unusual cash payments.

Abnormal / suspicious transactions

- Money passing through several different persons and / or entities may introduce numerous layers to a transaction to create opacity and disguise the source of funds.
- Assignment of a policy to an apparently unrelated third-party.
- Early cancellation of policies in circumstances which appear unusual or occur for no apparent reason.
- Cancellation of the policy and a request for the refund to be paid to a third-party (or to an alternative account than used to remit premium, or to a different jurisdiction than where the insured is domiciled).

- Transactions not in keeping with the normal practice in the class of business to which they relate, e.g. due to nature, size, frequency etc.

- For personal lines business, several policies taken out by the same insured for relatively small premiums (normally paid with cash), which are then quickly cancelled, possibly with the return premium requested to be paid to a third-party.

Claims

The claims process could be used in the layering and / or integration stage of the ML process. The following situations may give rise to suspicions in this context.

- Claims requested to be paid to persons other than the insured.

- For personal lines sector, apparently legitimate claims occurring with abnormal regularity e.g. regular small claims within the premium limit from the same insured or intermediary.

- A change of ownership / assignment of the policy just prior to a loss occurring.

- Abnormal loss ratios for the class of risk bound under a binding authority, especially where the intermediary has claims settling authority (possible evidence of claims being fabricated and reported to underwriters, or under-reporting of claims where the intermediary is acting as an unauthorised insurer, or even not paying claims).

- Claims investigations, which uncover evidence of other suspicious activity independent of the claim. For example, the claims investigator might discover that the claimant enjoys a lifestyle which is beyond their apparent financial means or that the insured has not been paying tax or even national insurance income.

SANCTIONS

Managing agents may also wish to consider whether an entity's sanctioned status, even as part of a sanctions list that is not directly relevant to the transaction in question, may also increase the ML risk of that entity.

CLAIMS FRAUD

The claims process could be used in the layering and / or integration stages of ML. Managing agents may choose to refuse payment of a claim due to suspicions of fraud. In this case there are no further reporting requirements. Suspicions of ML may arise if it is known or suspected that a specific type of criminal conduct is occurring or has occurred (such as fraud) and which has generated criminal property.

Managing agents should therefore be aware that claim payments, which are later confirmed as fraud cases, would then be considered criminal property and may be in breach of ML or CFT offences unless a report to the NCA is made.

REPORTING

Where there is knowledge or suspicion that ML, CFT and / or PF has or is taking place, all firms are required to submit a SAR to the NCA. A SAR can be submitted digitally via the NCA's SAR Portal and where applicable should also be shared with Lloyd's via

FinancialCrime@lloyds.com. Further guidance on the submission of SARs can be found on the NCA's website.

It should be noted that a "tipping off" offence (per section 333 of PoCA) occurs if, once a report has been made to the NCA, any information is disclosed about the report where that disclosure is likely to prejudice an investigation being conducted. A tipping-off offence is not committed through disclosures to a supervisory body, nor to another person within the same firm/group or between financial institutions, nor if enquiries are made which form part of the usual CDD process. Given that Lloyd's possesses certain statutory regulatory powers, disclosures may be shared with Lloyd's where appropriate without constituting a tipping-off offence.

A Defence Against Money Laundering (DAML) request can be submitted to the NCA where there is a suspicion that intended activity relates to criminal property, and that by carrying out the activity there is a risk of committing one of the principal money laundering offences under PoCA.

Lloyd's recommends that all firms operate an ISAR process. These enable staff to report suspicions to the MLRO or Nominated Officer for them to assess, investigate, and escalate as necessary.

FOR FURTHER INFORMATION:

Chris Po-Ba
Head of Sanctions
Financial Crime Advisory (Market)
t: +44 (0)20 7327 5473

Rachael Penny
Manager
Financial Crime Advisory (Market)
t: +44 (0)20 7327 6380

Tom Orpen-Smellie
Graduate Trainee
Financial Crime Advisory (Market)
t: +44 (0)20 7327 5825

APPENDIX 1

EXPANDED GUIDANCE FOR GENERAL INSURANCE AND MANAGING AGENTS

PoCA 2002 and TACT 2000

UK general insurance falls outside the regulated sector for ML, and general insurers are not governed by the MLRs or the FCA's SYSC requirements specific to ML.

Managing agents conducting general insurance are still at risk of ML offences under Part 7 of PoCA and the TACT where applicable. These offences include knowingly concealing, entering into or arranging the acquisition, use, and / or possession of "criminal property" and the related failure to disclose knowledge or suspicion of ML, as well as prejudicing an investigation and tipping-off offences.

Article 326 of PoCA defines "criminal property" as property that "constitutes a person's benefit from 'criminal conduct' or represents such a benefit (in whole or part whether directly or indirectly)", irrespective of who carried out the conduct and who benefited from it. "Criminal conduct" is in turn defined as conduct which "constitutes an offence in any part of the United Kingdom" or would "constitute an offence in any part of the United Kingdom if it occurred there".

Appendix 4 details offences and penalties under PoCA and TACT. Penalties for failing to comply with legislation and regulation can result in criminal punishment including imprisonment and unlimited fines.

Firms may also be subject to the provisions of Schedule 7 to the Counter-Terrorism Act 2008, imposing obligations on UK general insurers and life insurers to combat ML, CFT, and PF. Under this Act, HM Treasury can issue directions regarding CDD, ongoing monitoring, systematic reporting and limiting or ceasing business.

Financial Conduct Authority (FCA)

The FCA suggests that the guidance on ML and CFT in their Financial Crime Guide may assist general insurers in complying with the requirements of PoCA.

General insurers are not subject to the money laundering rules outlined under the FCA's SYSC 3.2.6 A-J but remain subject to the general provisions under SYSC 3.2.6 requiring firms to have appropriate risk management systems to mitigate risk of financial crime.

General insurers are under no regulatory obligation to appoint an MLRO or to allocate a director or senior manager responsibility for AML under SYSC rules. Lloyd's however requires each managing agent to appoint an MLRO or Nominated Officer to act as the focal point for all activity relating to ML, regardless of whether the managing agent is conducting general insurance or regulated business.

Joint Money Laundering Steering Group (JMLSG)

The JMLSG issues comprehensive guidance (Parts I , II and III) on the steps that firms should take to comply with applicable ML, CFT and PF legislation and regulation.

Part II Section 7A recognises that general insurers are not subject to the CDD requirements under the MLRs but nevertheless recommends that they adopt a risk-based approach to comply with their ML obligations. Part I, whilst aimed at the wider financial sector, may be useful to consider when completing risk assessments alongside Part III Section 4 on the UK's financial sanctions regime.

While general insurers may not be required to undertake CDD to the same degree as life assurers, the JMLSG recommend that risk assessments are conducted at the earliest possible stage of the life cycle of the insurance policy. This could be when introduced to a new client as well as at the renewal and claims stage.

Part II Annex 15-V recommends the inclusion of PF within the current risk assessments of customers, where dual-use goods can be exploited for illegal purposes including the development of weapons of mass destruction and / or terrorism. Market participants should assess the risk associated with such goods to avoid inadvertently facilitating or supporting illicit activities.

Equally, procedures should be appropriately risk-based to ensure compliance with ML legislation. The JMLSG guidance states that general insurers should consider the following systems and controls:

- Internal policies and procedures, communicated to all staff, which should include direction of due diligence standards and red flags.
- Guidance to all staff on failure to report suspicions and tipping off offences.
- Short reporting lines between front line staff and a nominated officer.
- Record keeping of reports made to competent authorities including evidence to support submissions. Where reports are not made, the rationale for not doing so should be recorded.
- Ongoing training for staff to recognise suspicious activity and how to report internally.
- A system for testing compliance that should be independent and adequately resourced.
- The appointment of a nominated officer for assessing suspicious activity reports and engaging with the NCA and law enforcement.

Lloyd's

In 2020, Lloyd's Monitoring and Assurance (M&A) team issued an e-alert highlighting areas where ML risk is potentially elevated. These include products such as kidnap and ransom (K&R), ransomware, bloodstock and specie insurance policies. Managing agents are encouraged to consider the M&A e-alert when conducting their own risk assessments of ML, CFT and PF risk. Assessments should include consideration of customer documentation, products, product distribution channels, geographical risk, complexity of transactions, existing systems and the operating environment, as necessary, to determine inherent and residual risk levels. For areas which are identified as being high-risk, enhanced due diligence (EDD) is recommended.

Other recommendations include:

- Enhancing second line of defence controls through post-bind review and sample testing to ensure that underwriters are correctly identifying red flags and actioning appropriately.

- Conducting return premium analysis particularly in cases where return premiums exceed a pre-defined limit and / or cumulative total, or where additional red flags are present (such as payments to third-parties or payments to different bank accounts).

- Ensuring that ML training details staff obligations in respect of suspicious transaction reporting, including information relating to the tipping-off offence, as well as the name and contact details of a firm's MLRO or nominated contact. Where managing agents utilise specific MLRO inboxes the use of automated responses to advise on the risk of a tipping off offence is recommended.

- Where crisis management firms are recommended to K&R policyholders, managing agents should seek assurances regarding the ML standards within these firms.

- Managing agents should ensure a consistent and complete approach to screening a reimbursement in relation to a K&R claim by establishing a checklist of items to be analysed and assessed.

Under Lloyd's Principles of Doing Business (Principle 11), managing agents should have robust frameworks in place to address regulatory and financial crime risks arising from their UK and international businesses. Frameworks should support compliance and enable transparent relationships with Lloyd's and other applicable regulators.

To support this, managing agents should:

- Embed a culture of transparency, regulatory and financial crime compliance, and an understanding of the benefits of this across their managed businesses.

- Have a robust understanding of their regulatory and financial crime risk exposure and appetite, which is subject to appropriate challenge.

- Have appropriate systems and controls, including training, in place to manage regulatory responsibilities and financial crime risk.

These systems and controls should include appropriate due diligence and KYC checks.

Further to this, it should be noted that while not legally required by the MLRs, it remains best practice for general insurers to conduct screening for Politically Exposed Persons (PEPs). As well as an increased risk of involvement in bribery and corruption, the FCA's AML guidance on PEP screening explains that PEP status introduces a possibility of heightened risk for ML, but caveats that screening should not "be interpreted as stigmatising PEPs as being involved in criminal activity".

Lloyd's Market Association (LMA)

The LMA has produced guidance for handling a ransomware incident. Market participants are urged to proceed with caution when approaching products related to ransomware or K&R coverage. Managing agents should not engage directly in the making of payments to an entity demanding a ransom and all claims should be thoroughly screened and scrutinised for ML, CFT and sanctions exposure to understand whether a payment is permitted to be made and whether any notifications to relevant authorities are required. For further guidance on handling a ransomware claim incident please consult Market Bulletin Y5359.

Financial Action Task Force (FATF)

FATF is the global ML and CFT watchdog. It sets international standards aiming to prevent these illegal activities. FATF's Recommendations ensure a co-ordinated global response to prevent organised crime, corruption and terrorism.

FATF regularly issues updates on high-risk jurisdictions which have significant strategic deficiencies in their regimes to counter ML, CFT, and PF. Managing agents are encouraged to keep up to date with FATF's list of high-risk jurisdictions.

APPENDIX 2

EXPANDED GUIDANCE FOR LIFE SYNDICATES

Money Laundering Regulations

While the MLRs do not apply to general insurance, they do apply to "contracts of long-term insurance" as defined under Schedule 1, Part II of the Financial Services and Markets Act 2000 and capture other related activities. Certain activities of a life syndicate may therefore be caught by the MLRs. Relevant managing agents operating a life syndicate should ensure that they understand the applicability of the MLRs to any activities undertaken, applying controls in line with the MLRs' expectations. PoCA and TACT also apply regardless.

Where their business is in scope, life syndicates are bound under Part 3 of the MLRs legislation to implement CDD, EDD and record keeping processes.

Article 33 of the MLRs state that EDD should also be conducted where the following exists:

- A high risk of ML or CFT.
- Business relationships or transactions with persons in a high-risk third country, except where the customer is a branch or majority owned subsidiary of an entity established in an EEA state, subject to further conditions detailed in the Article.
- Correspondent relationships with a credit or financial institution.
- If a relevant person is a PEP, or a family member or close known associate thereof.
- Where stolen or false identification documents have been used.
- Where transactions are complex, unusually large, occur in unusual patterns or have no apparent economic or legal purpose.

Life syndicates are expected to be familiar with the requirements of the MLRs and must obtain sufficient information for applicants for life assurance to comply with its due diligence obligations.

Failure to establish adequate and appropriate policies and procedures to prevent ML constitutes a criminal offence under the MLRs, regardless of whether ML occurs. A relevant person as defined under the Regulations can be liable for a fine and/or prison sentence of up to two years.

The MLRs also require in-scope firms to maintain appropriate systems and controls to mitigate PF risk. These controls include:

- A regulatory requirement to take appropriate steps to identify and assess the risk of PF, which must be added to the risk assessments covering ML and CFT.

- The implementation of clear and well-articulated policy and procedures to ensure that employees are aware of their obligations in respect to PF.

- Sufficient training should be given to employees enabling them to recognise when a transaction is unusual, suspicious, or when they have reasonable grounds to suspect that PF is taking place and how to report.

FCA

The FCA's SYSC rules relating to ML are relevant to Lloyd's syndicates underwriting life business. Chapter 3 of the FCA's handbook on ML and CFT should be considered, noting SYSC 3.2.6I and the requirement that a relevant firm must appoint a MLRO with appropriate authority and independence to oversee compliance with the FCA's rules on ML.

Life assurers and Lloyd's syndicates underwriting life business are likely to require an appointed MLRO under the FCA's Senior Management Functions (SMF) 17. Further guidance on SMF 17 is available in the FCA's Guide for Insurers.

The FCA has provided specific guidance on the treatment of PEPs for AML purposes, which can be referred to when conducting EDD screening per Article 33 of the MLRs.

JMLSG Guidance

Part II Section 7 of the JMLSG guidance is dedicated to the life assurance sector but should be read in conjunction with Parts I, III, and associated FAQs for further detail about the requirements.

Section 7 divides life business into reduced, intermediate, and increased risk levels for ML activity offering guidance on appropriate due diligence for each.

The guidance notes that life business classified at a reduced risk level is considered at low risk of money laundering activity. Term life assurance and Group Life Protection are included within this classification. For such business, the guidance states that in most instances counter-fraud checks conducted at point of claim would be sufficient to satisfy the due diligence obligations for such business.

At an intermediate risk level KYC and other due diligence checks become increasingly necessary, alongside a monitoring programme. These checks then become more sophisticated where business is considered to be at increased risk.

It is recommended that life syndicates review the JMLSG guidance to familiarise themselves with the risk levels and necessary due diligence requirements associated with their products.

APPENDIX 3

REPORTING

Internal Suspicious Activity Reporting (ISAR)

To comply with PoCA, all staff are obliged to monitor, recognise, and report potential or actual unusual / suspicious activity and transactions which may give rise to knowledge or suspicion of ML or terrorist financing. Staff must report any suspicions immediately to the MLRO or a Nominated Officer.

Lloyd's recommends that all firms operate an ISAR process. A member of staff can complete an ISAR to detail any reportable suspicious behaviour. The completed report is sent to the MLRO or Nominated Officer, who will then review and decide whether to report to the NCA or other relevant authority. Where necessary reports to the NCA should be done as soon as reasonably practicable.

General insurers should be aware of the 'Attempted Offences' within JMLSG guidance Part I Sections 6.7 to 6.9, confirming that there is no obligation for firms to disclose an unsuccessful attempt to commit fraud. The requirement under PoCA and TACT is to disclose attempted ML and terrorist financing offences. It is therefore only in relation to knowledge or suspicion that a benefit / criminal property has been acquired (meaning that there is knowledge or suspicion of ML, and terrorist financing) that a report should be made to the NCA.

Staff should be made fully aware of the reporting process, and training should be given in this regard.

External Suspicious Activity Reporting

Both regulated and non-regulated firms for ML and CFT purposes are required to submit a SAR to the NCA to avoid committing offences under PoCA and TACT. It should be noted that these are not considered to be crime reports and therefore reports should still be made to local law enforcement or Action Fraud where appropriate.

Under Part 7 of PoCA, as well as the TACT, regulated firms (e.g. life assurers) are required to submit a SAR if they have knowledge, suspicion, or reasonable grounds to know or suspect that a person is engaged in, or attempting, ML or CFT.

Firms outside of the regulated sector may also have an obligation to submit a SAR. This is because a failure to disclose constitutes an offence under sections 330, 331 and 332 of the PoCA should there be knowledge or suspicion of ML activity.

The NCA suggest that the easiest way to submit a SAR is via the secure NCA SAR Portal. Further guidance on SARs can be on the NCA website.

In addition, the Law Society has issued guidance about SARs, reportable suspicions and existing criminal property i.e. where there is knowledge or suspicion that a "*specific type of criminal conduct is occurring (such as fraud or tax evasion) and you suspect this generated property*", which, in turn, will trigger ML or CFT offences.

SARs that managing agents have submitted to the NCA should be shared with Lloyd's so that it can continue to support oversight activities as a regulator of the market. Where applicable, SARs should be shared with Lloyd's via FinancialCrime@lloyds.com.

Defence Against Money Laundering (DAML) requests

The NCA has issued guidance detailing how reporters can seek a defence (or 'consent') against committing a primary ML or CFT offence by submitting a DAML prior to the activity taking place, if market participants know of or suspect that the intended activity relates to dealing with criminal property. Consent in this regard is not a form of permission or clearance. A DAML solely provides a defence to a principal ML offence should the planned activity be carried out.

It should be noted that the NCA has a statutory seven working day period to consider all DAML requests. The day that the SAR is submitted should be considered Day 0.

A DAML does not protect against committing an ML offence under any other part of PoCA or other ML legislation or regulations. It will not provide a defence for:

- Committing a "tipping-off" offence.
- Civil liability claims – including negligence, breach of trust or breach of contract.
- Committing or facilitating any other criminal offence – for example, under the MLRs or Bribery Act 2010.

Requesting a DAML does not replace taking a risk-based approach or fulfilling obligations under the MLRs.

APPENDIX 4

OFFENCES

PoCA

PoCA created a single set of ML offences applicable to the proceeds of all crimes inside and outside of UK. Under section 328 a person can be held accountable for an offence if they have knowledge or reasonable belief that a crime occurred in a specific foreign country or territory, provided that crime was illegal under the laws of that country or territory at the time it took place, and falls under a prescribed offence determined by the Secretary of State.

For the principal offences of ML, the prosecution must prove that the property involved is "criminal property". This means that the property was obtained through criminal conduct. ML offences assume that a criminal offence has occurred to generate the criminal property which is now being laundered. This is often known as a predicate offence. No conviction for the predicate offence is necessary for a person to be prosecuted for an ML offence.

The prosecution must also prove that, at the time of the alleged offence, the defendant knew or suspected that the property was criminal property.

There are three primary offences under PoCA which can apply to all Lloyd's market participants (regulated and non-regulated). They are:

Concealing etc (s.327) – Where someone knows or suspects that the property is the benefit of criminal conduct, or it represents such a benefit then they commit an offence if they conceal, disguise, convert, transfer or remove that criminal property from England and Wales, Scotland or Northern Ireland.

Arrangements (s.328) – An offence is committed by a person if they enter into or become concerned in an arrangement which they know or suspect facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.

Acquisition, use and possession (s.329) – An offence is committed if someone knows or suspects that property is the benefit of criminal conduct and acquires, uses or has possession of the property.

There are also the following offences:

Failure to disclose – Regulated sector (s.330); Nominated Officers in the regulated sector (s.331); Other Nominated Officers (s.332). To avoid committing a failure to disclose offence, nominated officers must disclose any reports to the NCA.

Tipping off (s.333) – Tipping off constitutes disclosing that a report to the NCA has been made. Once a report has been made, a criminal offence is committed if any information is disclosed about the report where this disclosure is likely to prejudice an investigation being conducted.

It would not be deemed as tipping off to disclose to Lloyd's that a SAR against another party has been submitted to the NCA, as certain disclosures will not result in an offence under s.333.

As referenced in Part I of the JMLSG guidance, normal enquiries about customer transactions or activity which form part of the usual CDD process will not give rise to the tipping off offence.

Terrorism Act 2000 (TACT)

Sections 15 to 18 of TACT outline that a person commits an offence under the following criteria:

Fund-raising (s.15) – either provides/receives/or invites another to provide money or other property and either intend/know/or have reasonable cause to suspect that it may be used for the purpose of terrorism.

Use and possession (s.16) – the use, intent to use, or reasonable cause to suspect the use of money or other property for the purpose of terrorism.

Funding arrangements (s.17) – entering into an arrangement where money or other property is made/or is to be made available, knowing or having reasonable cause to suspect that it may be used for the purpose of terrorism.

s.17A – The insurer under an insurance contract commits an offence if:

- The insurer makes a payment under the contract, or purportedly under it.
- Payment is made in respect of any money or other property that has been, or is to be, handed over in response to a demand made wholly or partly for the purposes of terrorism, and
- The insurer or the person authorising the payment on the insurer's behalf knows or has reasonable cause to suspect that the money or other property has been, or is to be, handed over in response to such a demand.

Money laundering (s.18) – entering into or becoming concerned in an arrangement which facilitates the retention or control by, or on behalf of, another person of terrorist property by concealment, removal from the jurisdiction, transfer to nominees, or in any other way.

Terrorism Act 2000 (TACT), and the Counter Terrorism and Security Act 2015

The Terrorism Act establishes a series of offences related to involvement in arrangements for facilitating, raising, or using funds for terrorism purposes. This applies to regulated and non-regulated firms. S.17A was amended by the Counter Terrorism and Security Act 2015, to criminalise the making of insurance payments in response to terrorist demands.

Counter-Terrorism Act 2008 (CTA) Schedule 7

Schedule 7 of the CTA authorises HM Treasury to issue directions to firms in the financial sector. The requirements that may be imposed by a direction under these powers relate to: CDD; ongoing monitoring; systematic reporting; limiting or ceasing business.

Criminal Finances Act 2017 (CFA 2017)

CFA 2017 made changes to PoCA and TACT to better enable authorities to pursue and obtain the proceeds of crime and terrorist financing. It also introduced the criminal offence of failure to prevent tax evasion. The CFA states that a firm commits an offence if they fail to report knowledge or suspicions of tax evasion.

Financial Services and Markets Act 2023 (FSMA 2023)

FSMA 2023 makes the prevention of financial crime integral to the discharge of the FCA's functions and fulfilment of its objectives. The FCA must ensure that the firms it regulates and their senior management are aware of the risk that their businesses may be used in connection with financial crime, and take appropriate measures to prevent this risk. General insurers (including managing agents and the Society of Lloyd's) and general insurance intermediaries are subject to the high-level regulatory requirement to counter financial crime set out in SYSC 3.2.6R. They are not however subject to the MLRs or the provisions of the Handbook that specifically relate to ML (SYSC 3.26AR – SYSC 3.2.6JG).

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs)

The MLRs state that it is an offence not to establish adequate and appropriate policies and procedures to prevent ML (regardless of whether ML has taken place or not). The MLRs emphasise a requirement on firms to take appropriate steps to identify and assess the risks of ML, CFT and PF to their business.

Penalties

Despite the lower risk of ML within the Lloyd's market, failure to comply with legislation and regulation can result in criminal punishment.

The maximum penalties are:

- For the offence of ML: 14 years' imprisonment and/or an unlimited fine. (Note: An offence is not committed if a person reports the property involved to the NCA or under approved internal arrangements, either before the prohibited act is carried out, or as soon afterwards as is reasonably practicable).

- For failing to make a report of suspected ML: five years' imprisonment and/or an unlimited fine.

- For “tipping-off”: two years’ imprisonment and/or an unlimited fine.
- For destroying or disposing of relevant documents: five years’ imprisonment and/or an unlimited fine.

TACT

The maximum penalties for an offence under sections 15 to 18 are:

- On conviction on indictment, imprisonment for a term not exceeding 14 years and/or a fine, or
- On summary conviction, imprisonment for a term not exceeding six months and/or a fine not exceeding the statutory maximum.

MLRs

Whether a breach of the MLRs has occurred is not dependent on whether ML has taken place. Firms may be sanctioned for not having AML systems.

Where failure to comply with any of the requirements of the MLRs constitutes an offence, the punishment is a maximum of two years’ imprisonment, a fine, or both.