

ANTI MONEY LAUNDERING POLICIES & PROCEDURES

FIRM NAME: STREFFORD TULIPS

DATE: OCTOBER 2018

VERSION CONTROL:

Date	Change	Name
22.10.2018	Written AML Procedures already being utilised agreed	Chris Tulips

POLICY STATEMENT/OVERVIEW SECTION

STREFFORD TULIPS take a zero tolerance approach to being involved in illegal/illicit activity, and will fully comply with all relevant sections of the Money Laundering Regulations (ML Regs), the Proceeds of Crime Act 2002 (POCA), and the Terrorism Act 2000 (TACT).

All partners and employees of the firm are under an obligation and duty to comply with the above. This policy & any related procedures aims to help partners and staff fulfil these responsibilities, by providing a clear framework, along with setting out the firm's key principles and obligations.

- Failure to fulfil these responsibilities may result in disciplinary action and may also result in criminal sanctions for the staff involved.
- Breaches may also be reportable to our AML Supervisor (The Law Society of Scotland) which may result in professional disciplinary action.
- Furthermore, a report may also have to be made to the NCA or other law enforcement agencies, which may result in a criminal investigation.

AML LEGISLATIVE FRAMEWORK SECTION

Responsibilities under relevant legislation include:

ML REGS:

- Risk Based Assessment
- Customer Due Diligence, including ID&V requirements, assessing SoW, and application of KYC information
 - Enhanced Due Diligence & Ongoing Monitoring (incl. definition and treatment of PEPs)
- MLRO Responsibilities, SAR Reporting, Tipping Off, Police Orders
- Quality Assurance
- AML Record Keeping
- AML Training

- *Compliance with International Sanctions Requirements*

POCA 2002/TACT 2000: MLRO responsibilities, Suspicious Activity Reporting, Tipping Off & Police Orders

Key responsibilities of staff therefore include (*but are not limited to*):

- Conducting an adequate risk assessment and appropriate due diligence (CDD) on clients and transactions, including PEP and sanctions checking.
- Monitoring all clients/transactions on an ongoing basis for potential money laundering or terrorist financing activity;
- Reporting any suspicious activity in respect of client or transactions to the MLRO in accordance with the firms SAR (suspicious activity reporting)procedure;
- Avoiding discussing any potential or actual SARs with clients or any third parties (“Tipping off”)
- Referring any Police/Law Enforcement queries or requests to the MLRO ;
- Undertaking any AML-related training provided by the Firm.
- Keeping appropriate records of all AML related activity

FIRM RISK PROFILE SECTION:

*The partners believe **STREFFORD TULIPS** are at a medium risk of being used to launder the proceeds of crime. This is based on the following factors:*

- *Types of Work undertaken – regulated/non-regulated. Mostly Property? Litigation? Wills/Executry? Etc.*
- *High turnover of clients or a stable existing client base?*
- *High proportion of one-off clients/deals?*
- *Mostly F2F or non-F2F contact with clients?*
- *Geographical location of practice – high levels of crime?*
- *Act for clients across both criminal and civil matters*
- *International element to your business?*

RISK BASED ASSESSMENT SECTION:

Here, detail the Firm’s approach/procedures to risk assessment, including

- Who is responsible for risk assessment/how it is undertaken
The fee earner who is responsible for the specific file on a day to day basis is initially responsible for carrying out a risk assessment of the transaction and ongoing monitoring of the file to ensure compliance at all times. Risk assessments are subject to approval by the supervising partner
- *Client*
- *Transactional*
- *When/How Often reviewed **Files are typically reviewed to ensure compliance with AML on three occasions – two of which are at the commencement and completion of the matter in question***

- *High level overview of risk factors/ “red flag indicators”*
- *Firm position/policy re International clients/transactions – especially from non-EU countries **These would normally be assessed as being High Risk transactions, subject to final approval by the supervising partner and AML officer if required***
- *Should control what happens when red flags/risks are identified and what standard of due diligence should then be applied, and what this entails*
- *Should state examples/type of evidence which should be held*

CUSTOMER DUE DILIGENCE PROCEDURES SECTION

Here, detail firm’s procedures in relation to taking ID&V, KYC, Source of Wealth (SoW) checks, ongoing monitoring etc.

- *Who is responsible for taking ID&V/how this is undertaken : **The fee earner dealing with the specific file is responsible for initial checks and ongoing monitoring, subject to approval by the supervising partner and MLRO if appropriate***
- *Timing of ID&V : **This information will be requested within 7 days of a specific file being opened***
- *ID&V requirements for private individuals, Companies, Trusts, other legal entities – who/what should be ID’d etc.*
- *Acceptable ID Documents*
- *Simplified – in what situations – listed/regulated companies etc. **We will require in date (ie no more than 3 months old) photographic and address ID***
- *Standard – what is the standard ID&V undertaken **We reserve the right to request further ID or verification from any client in the event that our AMO checks determine that the client in question requires to be assessed as High Risk***
- *Enhanced – in what circumstances and what is undertaken over and above standard (primarily evidence of SoW, ongoing monitoring etc. **This will depend on the individual circumstances but examples would be larger than normal cash deposits, overseas residents, or PEP’s as defined below***
- *R.17 reliance*
- *Electronic Verification **We may carry our electronic ID verification as part of our regular or enhanced Due Dilligence procedures***
- *3rd Party Funding ID&V requirements(immediate family/unrelated) **If funds are being supplies for any transaction by a third party eg family member, business etc then we will require to carry out full KYC , SoW and AML checks on those third parties, including enhanced checks if we deem this necessary***
- *Any value limits to cash transactions handled/accepted by the firm **Unless by prior approval, we will accept a maximum of £500 in cash in relation to any one specific transaction***

Politically exposed persons (PEPs)

The firm will apply enhanced and ongoing due diligence to all PEP clients and will consider and assess the heightened risk of undertaking business with or on behalf of PEPs, particularly the risk of laundering the proceeds of corruption.

What is a PEP?

- A "politically exposed person" (PEP) is a term describing someone who has been entrusted with a prominent public function.
- A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold. Positions may include:
 - Head of state, heads of government, ministers and deputy or assistant ministers
 - Members of parliament
 - Members of supreme courts, of constitutional courts, or of other high-level judicial bodies – members of courts of auditors or of the boards of central banks
 - Ambassadors, charges d'affairs and high-ranking officers in the armed forces
 - Members of the administrative, management or supervisory bodies of state-owned enterprises

The definition of a PEP also extends to:

- family members of a PEP – spouse, partner, children and their spouses or partners, and parents
- known close associates of a PEP – persons with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relationships, or who is a sole beneficial owner of a legal entity or arrangement set up by the primary PEP

If the firm deploys an electronic verification tool – this tool should be used to check potential PEP status on all clients

(If electronic verification is not deployed): Should circumstances or information arise to suggest that a client is a PEP (or a corporate client is owned/controlled by a PEP) the firm should ask the client additional questions to determine PEP status, and use open source information to verify.

International Sanctions Checking:

- The fee earner will conduct a sanctions list check on each new client via the HM Treasury website (or an electronic verification system if used) to check if the client or source of funds is related to a sanctioned jurisdiction/regime, and conduct ongoing checks periodically (*at least annually for all clients*)
- <https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets>

MLRO RESPONSIBILITIES/ SUSPICIOUS ACTIVITY REPORTING SECTION

- *The MLRO of the Firm is **David Strefford***
- *He is responsible for....*
 - *Scrutiny of unusual transactions highlighted to him*
 - *Ultimately deciding when a Client/Matter if client to be taken on where there is a high risk of money laundering*
 - *Reviewing SARs made from employees - decide when to submit to NCA*
 - *Deal with any contact to or from LSS or Police*
 - *Ensure all staff trained to level appropriate to their role*

Further detail in this section should include:

- Encourage & detail how staff should make reports to the MLRO
- Make it clear obligations under POCA are mandatory – criminal offences
- Detail tipping off definition and potential issues
- What should be included in reports
- Timing of reports **These are all determined and dealt with as part of ongoing staff monitoring and training**
- What process should be followed in the event of a Police Order being served **Any such Orders received are dealt with by the supervising partner and/ or the MLRO only**

QUALITY ASSURANCE SECTION

- This section should detail how, and to what frequency the firm undertakes quality checking of compliance/AML files **All file are subject to random quality checks to ensure compliance with our AML officer. These checks are carried out on a monthly basis**

AML RECORD KEEPING SECTION

Procedures should detail:

- How the firm manages, records and stores AML related material, incl. retention period **All such information is stored by the firm electronically on our secure server for a minimum period of 10 years.**

Relevant records could be:

- AML Policies, Procedures, Manuals
- Risk Assessments
- CDD/KYC/SoW Evidence
- Evidence of staff training
- Suspicious Activity Reports
- E-Verification records
- PEP/Sanction Screening Searches

Firms do need to keep adequate records of AML/CDD material – a list of relevant records is on the slide, and should be kept for a minimum of 5 years after the relationship has ended or the transaction has been concluded.

AML TRAINING OF PARTNERS & STAFF SECTION

Procedures should detail:

- Which staff require what training (specific to role) **All fee earners (solicitors and paralegals) receive regular updates, training and random file checks to ensure compliance with AML**
- What form the training will take
- How often training should take place
- How staff will be kept up-to-date with emerging risk factors/new developments for the firm **This is dealt with as part of our regular staff training**

RELATED DOCUMENTS SECTION

Detail any internal firm documents, checklists, procedures which underpin/support this policy

- All files contain a specific Risk Assessment form which is checked at several points during any transaction and updated or amended as required.
- Internal SAR reporting form
- Acceptable ID as per our Terms of Business Letter issued in relation to each file opened

FURTHER INFORMATION SECTION

<http://www.lawscot.org.uk/members/regulation-and-standards/financial-compliance/money-laundering-counter-terrorist-financing/>

ML Regs 2007:

<http://www.legislation.gov.uk/uksi/2007/2157/contents/made>

(this link will change to 4th MLD post 26th June 2017)

POCA 2002:

<http://www.legislation.gov.uk/ukpga/2002/29/contents>