

Information Guide (“Guide”) on the Prevention of Money Laundering and Countering the Financing of Terrorism for Moneylenders



Information Guide (“Guide”) on the Prevention of Money Laundering and Countering the Financing of Terrorism for Moneylenders

1 This Guide seeks to improve the awareness and understanding on issues relating to money laundering (“ML”) and financing of terrorism (“FT”) and to inform moneylenders of the appropriate preventive measures to be adopted against such activities that might be conducted through your course of business. This Guide also highlights the key provisions, offences and obligations for compliance by moneylenders.

National Risk Assessment

2 On 10 January 2014, the Monetary Authority of Singapore (MAS) issued its inaugural national risk assessment report on money laundering and terrorism financing risks in Singapore. The report serves to help regulatory authorities maintain an effective risk-based regime in regard to anti-money laundering and counter financing of terrorism (“AML/CFT”), as well as to prioritise and allocate public sector resources efficiently. The report also serves to help private sector stakeholders better understand the money laundering and terrorism financing risks in their own and related industries, assess the adequacy of their AML/CFT controls, and strengthen them where necessary.

3 The section of the report pertaining to the moneylending regime can be found on page 71 of the [report](#)¹. As moneylenders, you are urged to read the report for a better appreciation of the AML/CFT gaps relevant to the moneylending industry, as well as the larger economic landscape of Singapore. This will better equip you to tailor your AML/CFT measures as necessary to counter such risks.

4 The cash-intensive nature of the money lending industry raises potential ML concerns. However, due to the usually low lending limits coupled with an average loan value of less than \$1,500, the industry has been identified as moderately attractive as a channel for ML. Additionally, the FT risk of foreign terrorist exploiting the services of moneylenders for their activities has been identified to range from moderate to low. This is because of the low incidences of lending to foreigners and absence of overseas transactions.

Overview of Money Laundering (“ML”) and Terrorism Financing (“TF”)

5 ML is an illegal activity carried out by criminals to turn “dirty” money into what appears to be “clean” money. It involves converting cash or other property derived from illegal activities, into a form which appears to have originated from legitimate sources². Additionally, continual terrorist attacks in countries and cities in many parts of the world

¹ The full report can be accessed at https://www.mlaw.gov.sg/content/dam/minlaw/rop/assets/documents/Singapore%20NRA%20Report%202013_24032015.pdf

² To illustrate, while the loan money issued by a moneylender is “clean” money, the money used to repay the moneylender may be “dirty” money.

Information Guide (“Guide”) on the Prevention of Money Laundering and Countering the Financing of Terrorism for Moneylenders

have increased the focus of governments worldwide on countering the act of terrorism and the financing of terrorism.

6 The Financial Action Task Force (“FATF”) is an international task force established in 1989 to develop and promote national and international policies to fight money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction. The FATF published a revised set of 40 recommendations on anti-money laundering measures in June 2003. As a member of the FATF, Singapore has an obligation to implement these recommendations.

7 FATF’s recommendations are applicable to the moneylending sector. The other professional sectors that need to comply include the financial sector as well as the designated non-financial business and professions (“DNFBP”) such as the public accountants, real estate agents, casinos, company service providers, developers, lawyers as well as the non-profit organisations such as the charities. They have been identified as important gatekeepers to counter the threat of money laundering and terrorist financing.

What is Money Laundering (“ML”)?

8 ML is a process intended to turn “dirty” money (which are normally proceeds from a criminal activity) into what appears to be “clean” money. It is done so with the intention to hide their illegal origins. With such an act, criminals can get to enjoy the proceeds without the fear of detection or prosecution, as there will not be any recognisable audit trail to trace back to the criminals/criminal activities.

9 If money laundering activities are left undetected, it will lead to the following consequences:

- a. There will be difficulty in taking prosecution action against key culprits as criminals are able to remove or distance themselves from the criminal activities that generated the proceeds;
- b. Criminals will get to enjoy the proceeds of crime as such crime proceeds do not get confiscated even if the criminal is caught;
- c. Criminals can fund further criminal activities by reinvesting the proceeds of previous crimes.

What is Terrorism Financing (“TF”)?

10 TF is the provision, collection, use, possession or dealing with property for terrorist purposes. The source of such funds used can be either legitimate or illegal. These funds may not always be in large amounts.

What legislation does ML fall under?

11 The **Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (“CDSA”)** is the primary legislation in Singapore to combat and criminalise money laundering. Sections 43, 44, 46(2), 46(3), 47(2) and 47(3) of the CDSA also criminalise third-party laundering of proceeds derived from drug dealing and other serious crimes. The CDSA provides for the tracing and confiscation of such proceeds and its benefits.

12 Section 39 of the CDSA makes it mandatory for a person to lodge a suspicious transaction report (“STR”) with the Suspicious Transaction Reporting Office (“STRO”) if in the course of his trade, profession, business or employment, he has reason to suspect that any property he is dealing with is linked to crime. Failure to do so is an offence punishable with a fine of up to \$20,000.

What legislation does TF fall under?

13 The **Terrorism (Suppression of Financing) Act (“TSoFA”)** was passed to give effect to the International Convention for the Suppression of the Financing of Terrorism which Singapore signed on 18 December 2001 and the United Nations Security Council Resolution 1373 (“UNSCR 1373”). The TSoFA not only criminalises terrorism financing but also prohibits any person in Singapore from dealing with or providing services to a terrorist entity, including those designated pursuant to the TSoFA. The TSoFA also imposes a duty to all to provide information pertaining to terrorism financing to the Police. This obligation is laid out under sections 8 and 10 of the TSoFA.

14 Due to Singapore’s commitment in fighting terrorism, an Inter-Ministry Committee on Terrorist Designation (“IMC-TD”) was formed in 2012 to act as Singapore’s authority relating to the designation of terrorists. This Committee consists of members from the Ministry of Home Affairs (“MHA”), Monetary Authority of Singapore (“MAS”) and the Attorney General’s Chambers (“AGC”). The IMC-TD is the competent authority responsible for identifying persons or entities for designation as terrorists pursuant to UNSCR 1373 (2001) who meet the criteria for designation under UNSCR 1373. Please refer to MHA’s Inter-Ministerial Committee – Terrorist Designation website [here](https://www.mha.gov.sg/Pages/Inter-Ministerial-Committee---Terrorist-Designation-%28IMC-TD%29-.aspx)³. You may also wish to receive updates on new information published on this website by subscribing to the website’s Rich Site Summary (“RSS”) feed.⁴ Moneylenders are also required to adhere strictly to the Moneylenders (Prevention of Money Laundering and Financing of Terrorism) Rules 2009 (“PMFT Rules”) as anyone who is guilty of an offence under these rules will be subject to a maximum fine of \$100,000.

³ <https://www.mha.gov.sg/Pages/Inter-Ministerial-Committee---Terrorist-Designation-%28IMC-TD%29-.aspx>

⁴ Such RSS feeds will send you alerts whenever updates had been made to the contents of the website.

Which are the United Nations Security Council Resolutions (“UNSCRs”) in relation to terrorism and what are our obligations in relation to them? What happens if we do not fulfil them?

15 Singapore is committed to implementing the United Nations Security Council Resolutions (“UNSCRs”). Among other measures, the UNSCRs may impose targeted financial sanctions against specific individuals and entities identified by the UN Security Council (or relevant UN Committees) as contributing to a particular threat to, or breach of, international peace and security.

16 There are a number of UNSCRs relating to terrorism, including the recent UNSCRs 2178 and 2199 which focus on terrorist threats arising to the Islamic State in Iraq and the Levant. More specifically, UNSCRs 1267/1989 and UNSCR 1988 set out measures on designated individuals and entities associated with Al-Qaida and the Taliban respectively⁵.

17 Under the TSoFA, a terrorist is defined widely as anyone who commits, or attempts to commit, any terrorist act or participates in or facilitates the commission of any terrorist act. It also includes any person set out in the First Schedule of TSoFA. All persons and entities designated by the UNSCRs 1267/1989 Sanctions Committee to the Al-Qaida Sanctions List and the UNSCR 1988 Sanctions Committee to the 1988 Sanctions List, and as updated from time to time, are included as part of the First Schedule to TSoFA.

18 Sections 3 to 6 of the TSoFA expressly prohibit all natural and legal persons within Singapore and Singapore Citizens outside of Singapore from the following:

- a. Provision and collection of property for terrorist acts;
- b. Provision of property or services for terrorist purposes;
- c. Use or possession of property for terrorist purposes; and
- d. Dealing with property of terrorists or terrorist entity.

19 Under the TSoFA, a person who contravenes sections 3 to 6 will be liable, upon conviction, to a maximum fine of \$500,000 or to imprisonment for a term not exceeding 10 years or to both. In any other case where the offender is not an individual, to a fine not exceeding \$1 million. Every person in Singapore and every citizen of Singapore outside of Singapore who has information about these transactions or proposed transactions in respect of any property, funds or other assets belonging to any terrorist or terrorist entity, is required to inform the Police immediately. Any person who contravenes this requirement will be liable,

⁵ These two lists of such individuals and entities (which links are presented below) have been provided for in the latest version of the licence conditions for moneylenders:

- a. http://www.un.org/sc/committees/1267/qa_sanctions_list.shtml
- b. <http://www.un.org/sc/committees/1988/list.shtml>

Information Guide (“Guide”) on the Prevention of Money Laundering and Countering the Financing of Terrorism for Moneylenders

on conviction, to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 5 years or to both.

Are there any other UNSCRs that we have to take note of? What are our obligations in relation to them?

20 There are also UNSCRs issued to address proliferation risks of weapons of mass destruction including those emanating from Iran and the Democratic People’s Republic of Korea (“DPRK”). More specifically, UNSCR 1718 and UNSCR 1737 sets out measures on designated individuals and entities associated with DPRK and IRAN respectively⁶.

21 In Singapore, these obligations would include the United Nations (Sanctions – Democratic People’s Republic of Korea) Regulations 2010 and United Nations (Sanctions – Iran) Regulations 2014 (collectively referred to as the “UN Regulations”). These Regulations can be accessed at [Singapore Statutes Online](#)⁷.

22 Under these regulations, all natural and legal persons in Singapore:

- a. are required to comply with targeted financial sanctions (freezing) requirements against such UN-designated individuals and entities; and
- b. should ensure that they do not deal with designated individuals and entities (as defined in the respective UN Regulations) before engaging in any business or commercial activity. Screening the names of their customers against the names (and aliases) of designated individuals and entities would help natural and legal persons meet these obligations.

23 Amongst other provisions, the UN Regulations prohibit:

- a. The provision of funds, other financial assets or economic resources and services for the benefit of designate individuals and entities; and
- b. Dealing with property of designated in individuals and entities.

24 Under the United Nations Act, a person who commits any offence under the UN Regulations will be liable on conviction, in the case of an individual, to a fine of up to \$500,000 or to imprisonment for a term of up to 10 years or to both; or in any other case, to a fine of up to \$1 million.

⁶ The links to these two lists of such individuals and entities are presented below:

- a. http://www.un.org/sc/committees/1718/sanctions_list.shtml
- b. http://www.un.org/sc/committees/1737/sanctions_list.shtml

⁷ The Singapore Statutes Online can be accessed through this link: <http://statutes.agc.gov.sg/>

How can I be kept updated on changes made to the Lists of Designated Individuals and Entities?

25 MAS published a webpage titled “Targeted Financial Sanctions⁸”. This page highlights the targeted financial sanctions against specific individuals and entities identified by the UN Security Council (or relevant UN Committees) as contributing to a particular threat to, or breach of, international peace and security.

26 Moneylenders are required to comply with the sanctions requirements. In order to ensure that no one deals with designated individuals and entities defined under the United Nations Act, and the Terrorism (Suppression of Financing) Act, all persons should screen their clients against the lists found on this webpage titled “Lists of Designated Individuals and Entities⁹” before engaging in any business or commercial activity with them.

27 Moneylenders are strongly encouraged to subscribe to the RSS Feed function located on this webpage in order to receive alerts on updates made to the said lists.

Who can I approach for help on the UN Regulations and my obligations?

28 All persons should seek independent legal counsel if you have any doubts about the interpretation and applicability of the UN Regulations or of your obligations. Further enquiries can be sent to IPTO.

What is the role of the Suspicious Transaction Reporting Office (“STRO”)?

29 STRO is Singapore’s Financial Intelligence Unit. It is formed in 2000 under the Commercial Affairs Department (“CAD”) of the Singapore Police Force (“SPF”). It is Singapore’s central agency for receiving, analysing and disseminating reports of suspicious transactions, known as Suspicious Transaction Reports (“STRs”). STRO will turn raw data in STRs into financial intelligence that can be used to detect money laundering, terrorism financing and other criminal offences.

⁸ This webpage can be found at: <http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions/Targeted-Financial-Sanctions.aspx>

⁹ This webpage can be found at: <http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions/Targeted-Financial-Sanctions/Lists-of-Designated-Individuals-and-Entities.aspx>

What is a Suspicious Transaction Report (“STR”)?

30 An STR is made when a person suspects that any property is directly or indirectly connected to a criminal conduct, and the knowledge or suspicion arose during the course of the moneylender’s business. While the “transaction” usually refers to a financial transaction, it can also extend to other activities which can be used to facilitate illicit activities. In the context of a moneylender, an example encounter would be a borrower turning up to borrow money with very unusual terms with an intention to repay the debt later with criminal proceeds. The loan application (regardless of its success), while not a financial transaction, is a suspicious activity that requires the making of an STR.

What is the purpose of lodging a STR?

31 Information from each STR will be analysed to detect money laundering, terrorism financing or other criminal activities.

How to lodge a STR?

32 Moneylenders can lodge STRs by submitting it in writing, via email or via the web-based system (STROLLS). The following information should be contained in the report:

- a. A detailed account of the relevant facts and nature of the transaction;
- b. Copies of the relevant documents, if available; and
- c. Your name, NRIC / passport number, contact number and address.

33 To lodge a STR in writing, you may send the STR to:

Head, Suspicious Transaction Reporting Office (Analysis)
Commercial Affairs Department
391 New Bridge Road #06-701
Police Cantonment Complex Block D
Singapore 088762.

34 Alternatively, if your company has a valid STROLLS user account, your authorised officer may lodge an STR via STROLLS. You may wish to email STRO@spf.gov.sg to find out if your company has a valid STROLLS account. If your company does not have a valid STROLLS account, you may email your report to the abovementioned email address.

You can also use the STR form format provided at [Annex A](#) of this Guide.

What is considered a suspicious customer or transaction?

35 The following are examples / indicators of a suspicious customer or transaction:

Information Guide (“Guide”) on the Prevention of Money Laundering and Countering the Financing of Terrorism for Moneylenders

a. General

- Borrower admits or makes statements about involvement in criminal activities.
- Borrower does not want correspondence sent to home address.
- Borrower is accompanied and watched.
- Borrower shows uncommon curiosity about internal systems, controls and policies.
- Borrower presents confusing details about the loan or knows few details about its purpose.
- Borrower over justifies or explains the loan.
- Borrower took up loans that are not within the norm of the moneylending business, gives conflicting accounts as regards the purpose of the loan.
- Borrower's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact borrower shortly after transaction was made.
- Normal attempts to verify the background of a new or prospective borrower are difficult.
- Borrower appears to be acting on behalf of a third party, but does not tell you.
- Borrower insists that a transaction be done quickly and that the identification and verification processes be done away with.
- The transaction does not appear to make sense or is out of keeping with usual or expected activity for the borrower.
- Borrower attempts to develop close rapport with staff yet appears to hide his true intentions.
- Borrower spells his or her name differently from one loan to another.
- Borrower provides false information or information that you believe is untrue.
- You are aware that the borrower is the subject of a money laundering or terrorist financing investigation.
- You are aware or you become aware, from a reliable source (that can include media or other open sources), that a borrower is suspected of being involved in illegal activity.
- There is adverse information concerning the borrower where he is listed on the UNSCR lists (terrorist, pirates, genocide), sanctions list or the customer appeared in media articles indicating his investigation, arrest, prosecution or conviction;
- A new or prospective borrower is known to you as having a questionable reputation or criminal background.
- Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist).

b. Knowledge of reporting or record keeping requirements

- Borrower attempts to convince employee not to complete any documentation or verification required for the transaction.
- Borrower makes inquiries that would indicate a desire to avoid reporting.
- Borrower has unusual knowledge of the law in relation to suspicious transaction reporting.
- Borrower seems very conversant with money laundering or terrorist activity financing issues.

Information Guide (“Guide”) on the Prevention of Money Laundering and Countering the Financing of Terrorism for Moneylenders

- Borrower is quick to volunteer that repayment funds are “clean” or “not being laundered.”
- Borrower appears to be structuring amounts to avoid record keeping, client identification or reporting thresholds.

c. Identity documents

- Borrower provides doubtful or vague documents.
- Borrower does not resemble the photograph in his personal document
- Borrower produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Borrower refuses to produce personal identification documents.
- Borrower only submits copies of personal identification documents and is not able to produce the originals.
- Borrower expects the staff to establish identity using something other than his or her personal identification documents.
- All identification presented is foreign or cannot be checked for some reason.
- All identification documents presented appear new or have recent issue dates.
- Borrower presents different identification documents at different times.
- Borrower’s residential address does not correspond with domicile or employment status.

d. Cash transactions

- Borrower starts taking frequent loans in large amounts when this has not been a normal activity for the borrower in the past.
- Borrower takes on multiple loans and repay them before the due date, but is unable to provide a reasonable explanation on his source of funds.
- Borrower uses notes in denominations to make repayments that are unusual for the borrower (ie repayment in notes of SGD \$1000 or \$10000).
- Borrower presents notes that are packed or wrapped in a way that is uncommon for the borrower.
- Borrower consistently applies for loans that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.
- Borrower consistently applies for loans that are significantly below the reporting threshold amount in an apparent attempt to avoid triggering the relatively rigorous identification/verification reporting requirements.
- Borrower presents significant excessive funds for repayment without bothering to count them, which suggests that the source is doubtful.
- Borrower applies for a loan of an amount that is unusual compared with amounts of past transactions.
- Payer is neither the borrower nor surety of the loan and does not seem to be related to the borrower/surety except for in illegal activity.

What should I do if I encounter a suspicious borrower or transaction?

36 Moneylenders should take the following steps when you encounter a suspicious borrower or transaction:

- a. You should not alert the customer of your suspicion or your intention to lodge a STR against him.
- b. You should reject the loan and not enter into any transaction with the customer.
- c. File a STR in the format (as shown in Annex A) with the STRO.
- d. Keep records relating to the suspicious transaction together with all internal findings, analysis and investigation carried out.

Are there any measures that Moneylenders can take to detect and prevent money laundering and terrorist financing?

37 Moneylenders shall develop and implement internal policies, procedures and controls (“PPC”) to detect and prevent money laundering and terrorist financing, and to communicate these to his employees and officers. In developing these measures, moneylenders are required to comply with rules 5 to 9A of the PMFT Rules. Such internal PPCs must reflect the actual processes of the moneylender’s business operations and cover:

- a. Customer Due Diligence (“CDD”) measures;
Note: The activities would include customer screening against the UN Sanction Lists, face-to-face verification/interview, identifying and verifying the customer’s identity, understanding the purpose of the loan, and scrutinising transactions undertaken by the customer throughout the course of the business relation. It should be further noted that performance of CDD is not limited to only the borrower, but where applicable, must be performed on the agent of the borrower or the beneficiary of the loan amount. In the case where the borrower is not an individual, CDD must be performed on the individuals connected to the borrower, such as directors, partners, beneficial owners, etc.
- b. Record keeping;
Note: Record keeping should not be limited to requisite documents such as completed loan application forms. It should also include information that is obtained in the course of performing AML/CFT measures or information received through general conduct of business that relates to money-laundering or terrorism financing, for e.g. written record of the moneylender’s findings and the basis of a decision to continue a business relationship with a PEP.

Information Guide (“Guide”) on the Prevention of Money Laundering and Countering the Financing of Terrorism for Moneylenders

- c. Detection of unusual or suspicious applications or transactions, and the making of disclosures under section 39(1) of the CDSA;
Note: A moneylender should use the red-flag indicators listed under para 32 as a guide.
- d. Audit of the internal policies, procedures and controls;
Note: A moneylender can engage external auditors to review and audit the PPCs on a regular basis, if he does not have the means to maintain an independent audit function.
- e. Compliance management arrangements; and
Note: A moneylender must appoint a suitably competent manager or officer as the AML/CFT compliance officer who will see to the moneylender’s compliance with the AML/CFT obligations.
- f. Hiring and training of employees.
Note: A moneylender should commit that no person will be hired/engaged in the moneylending business without the Registrar’s approval. The moneylender should also have a training plan for its staff and ensures that the trainer is proficient in AML/CFT measures and is familiar with the business’ PPCs. Such training may include enrolling of staff (or even the compliance manager/officer) in AML/CFT-related talks and seminars.

To ensure full compliance of the above, please refer to the PMFT Rules and its Schedule.

What do Moneylenders have to do to ensure that they have measures in place to detect and prevent money laundering and terrorist financing?

38 Under rule 8(1) of the PMFT Rules, every moneylender shall implement and maintain an adequately resourced and independent audit function that is able to regularly assess the effectiveness of his internal PPCs. Any moneylender who contravenes this rule shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$100,000.

What are the consequences of not reporting a STR?

39 An STR shall be filed when there are grounds to suspect that any property could be associated with criminal activities, and such suspicion arose in the course of employment/business. Otherwise, you run the risk of being prosecuted for failing to file a STR.

Information Guide (“Guide”) on the Prevention of Money Laundering and Countering the Financing of Terrorism for Moneylenders

40 You could also be prosecuted for abetting the commission of more serious offences like money laundering or terrorism financing, for allowing yourself to be the conduit for the movement of criminal proceeds, if that you knew or ought to have known, that these were criminal proceeds.

Will the suspect in my STR be in any trouble with the authorities?

41 A STR is not an allegation of crime. It is also not an accusation that a person has committed a crime. It is essentially a suspicion that some property could be linked to criminal conduct. In many cases, there is nothing more than a suspicion, and there may well be no evidence of any criminal conduct.

42 STRO treats each STR as a piece of important information that could potentially lead to the detection of criminal conduct. Until then, it remains a piece of information. A suspect named in an STR will not automatically be “in trouble” with the authorities.

Will STRO arrest the suspect(s) featured in the STR?

43 There may be some apprehension on the part of the STR filer that his compliance with the statutory obligation to file an STR may result in an innocent person getting into some kind of trouble, including being arrested.

44 STRO is unlikely to arrest a person based solely on information from an STR. STRO would have to verify that the information provided in the STR is accurate, check various domestic and (if necessary) international databases to see if any useful information can be obtained, and conduct further queries and analyses. If need be, STRO will launch a full investigation.

45 If an arrest is ultimately made, it would have been after a certain amount of work has been done, and supported by evidence collected independently rather than the plain information contained in the STR. Therefore, there, ought not to be any fear that law enforcement action is taken solely on the basis of the STR, to the detriment of innocent parties.

Will my identity remain confidential?

46 There are safeguards in place to protect the identity of the STR filer. Under section 56 of the CDSA, STRO is required to preserve the secrecy of information obtained under the CDSA, including STR information. There are strict measures in place to protect the identity of the STR filer.

Information Guide (“Guide”) on the Prevention of Money Laundering and Countering the Financing of Terrorism for Moneylenders

47 Additionally, under section 40A of the CDSA, no STR information shall be admitted in evidence in any civil or criminal proceedings. Moreover, no witness in such proceedings shall be obliged to disclose the identity of the STR filer. If a document which is in evidence were to contain any entry that could lead to the discovery of the identity of the STR filer, the court shall cause those entries to be obliterated to protect the identity of the STR filer.

Will I be required to testify in court?

48 If the concern with testifying in courts is that you would then be revealed as the STR filer, section 40A of the CDSA would provide ample assurance that the identity of the STR filer is protected. You may however, be required to testify in court as an ordinary witness (not as the STR filer) if there were certain facts that were specifically within your knowledge that is relevant to the trial.

Can I be sued for filing a STR against a person, and STRO subsequently finds that the STR was a “false alarm”?

49 The key issue is whether you made the STR in good faith. Section 39(6) of the CDSA stipulates that disclosures made in good faith will not be treated as a breach of any restriction upon the disclosure imposed by law, contract or rules of professional conduct, and the maker shall not be liable for any loss arising out of the disclosure, or any act or omission in consequence of the disclosure.

Am I allowed to inform my customer that I filed a STR against him?

50 You should **NOT** inform your customer that you or anyone else has filed an STR against him. This may constitute to “tipping off”, an offence under section 48 of the CDSA. “Tipping off” is an act when a person knows or has reasonable grounds to suspect that an authorised officer is acting in connection with an investigation and discloses to any other person information that is likely to prejudice that investigation.

How can I obtain more information on anti-money laundering and counter-terrorism financing?

51 Detailed information can be obtained from the CAD Anti-Money Laundering and Counter-Terrorism Financing Handbook or CAD’s website.

Information Guide (“Guide”) on the Prevention of Money Laundering and Countering the Financing of Terrorism for Moneylenders

- CAD Anti-Money Laundering and Counter-Terrorism Financing Handbook (<http://www.cad.gov.sg/publications/cad-anti-money>);
- CAD’s website on AML/CFT (<http://www.cad.gov.sg/aml-cft>).

Information Guide (“Guide”) on the Prevention of Money Laundering and Countering the Financing of Terrorism for Moneylenders

Annex A – Suspicious Transaction Reporting Form

- (1) Reporting of Suspicious Money Laundering Transactions pursuant to section 39, Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act
- (2) Reporting of Suspicious Terrorist Financing Activities pursuant to Section 8, Terrorism (Suppression of Financing) Act

Reporting Moneylender	
Name:	
Branch:	
Address:	
Contact No:	
Facsimile:	
Email:	
Reporting Officer of Moneylender	
Name:	
Designation:	
Report Reference:	
Contact Officer (if different from Reporting Officer):	
Designations:	
Customer’s Particulars	
Name:	
NRIC / Passport No:	
Date of Birth:	
Nationality:	
Address:	
Foreign Address (if any)	
Contact No:	
Occupation:	
Date when particulars were last updated (where available)	

Information Guide (“Guide”) on the Prevention of Money Laundering and Countering the Financing of Terrorism for Moneylenders

Suspicious Transaction(s)		
Amount (Dr/Cr)	Date	Description of Transaction (E.g. Funds transfer, source of funds, destination, etc)

Reason(s) for Suspicion

Other Relevant Information (including information on other accounts that may be linked to the transaction(s) and any actions taken by the reporting entity in response to the transaction):

Supporting documents

A copy of each of the following documents is attached:

- Application for loan
- Customer identification documents
- Relevant documents supporting the Suspicious Transactions

X

(Signature of Reporting Officer)

Date: