《打擊洗錢及恐怖分子資金籌集(金融機構)條例草案》委員會

有關參考文獻的資料

《打擊洗錢及恐怖分子資金籌集(金融機構)條例草案》(《條例草案》)的客戶盡職審查及備存紀錄規定，大致反映香港金融管理局(金管局)、保險業監理處(保監處)和證券及期貨事務監察委員會(證監會)所發出的各份相關指引的現行規定。另外，在草擬《條例草案》時，當局也參考了英國的相關規例。隨文夾附以下文件，以供委員參考：

A (a) 金管局發出的《防止洗錢活動指引》(金管局《指引》)－**附件A**

B (b) 金管局發出的《防止洗錢活動指引補充文件》(金管局《補充文件》)－**附件B**

C (c) 保監處發出的《防止洗黑錢及恐怖分子籌資活動指引》(保監處《指引》)－**附件C(只備英文本[1])**

D (d) 證監會發出的《防止洗黑錢及恐怖分子籌資活動指引》(證監會《指引》)－**附件D**

E (e) 英國《2007年打擊洗錢規例》(英國《規例》)－**附件E(只備英文本)**

F 2. 現把草擬《條例草案》某些條款時所參考的資料表列於**附件F**，以供委員參考。

財經事務及庫務局
二零一零年十二月二十日

---

[1] 保監處《指引》的中文文本仍在整理中，待定稿後將提交委員會。

《防止清洗黑錢活動指引》

金融管理專員根據《銀行業條例》第 7(3)條發出的指引

目錄

2010 年 7 月修訂

附件

附件一	已廢除
附件二	已廢除
附件三	已廢除
附件四	已廢除
附件五	可疑交易舉例
附件六	向聯合財富情報組作出報告的標準格式
附件七	聯合財富情報組對舉報可疑交易的認收函件舉例
附件八	已廢除

第一部分
概覽

1. 引言

1.1 本指引包含並取代金融管理專員在一九九三年七月發出的「洗錢活動」指引，以防止銀行體系被非法用來使不正當獲得的金錢合法化。此外，本指引亦載有新修訂內容，以配合政府頒布的《有組織及嚴重罪行條例》；該條例以及《販毒（追討得益）條例》中有關洗錢活動條文其後的修訂；國際金融特別行動組對打擊洗錢活動措施的全面檢討；和英國就銀行及建屋互助會發出的洗錢活動指引。本指引還載有其他修訂和新增關於可疑交易的更多例子。

1.2 本指引直接適用於認可機構在香港從事的一切銀行及接受存款業務。不過，金融管理專員預期各機構會確保它們在香港的附屬公司亦訂有有效的控制措施，以打擊洗錢活動。在香港註冊的機構，如在海外設有分行或附屬公司，則須採取步驟，提醒這些海外分行或附屬公司的管理層，要留意集團對洗錢活動的政策。假如某地訂有洗錢法例，香港機構在該地所設的分行及附屬公司至少應遵守當地法例的規定。如當地法例與本指引有所抵觸，該等分行或附屬公司必須遵守當地法例，並須立刻知會總公司偏離集團政策的地方。

1.3 鑑於洗錢方法層出不窮，因此必須經常檢討本指引的實用性及成效，並可能需要不時作出修訂，以引入措施打擊新的洗錢方法（包括有利於隱藏戶口身分的嶄新或發展中科技）。

2. 甚麼是洗錢活動？

2.1 「洗錢活動」一詞的含義，是指將非法獲取的金錢的來歷改爲似乎出於合法來源的一切程序。

2.2 現金交易可以幫助進行各種犯罪活動的人隱藏身分，亦是毒販常用的交易方法。在收取大量現金後，罪犯在進行洗錢活動時通常會考慮到下列三項因素：

(a) 需要隱藏有關金錢的真正擁有權及來源；
(b) 需要控制有關金錢；及
(c) 需要改變有關金錢的形式。

2.3 機構日常最容易遇到的其中一種洗錢過程，是以現金存款形式累積存入銀行體系或用來購買貴重物品。這些交易雖然簡單，但可能是下文所述複雜而精密的交易網絡的一部分。儘管如此，要偵察洗錢活動，最重要的仍然是要在有關現金首次進入金融體系時便能察覺到。

洗錢階段

2.4 洗錢活動可分爲三個階段，其間洗錢人可能進行無數交易，而這些交易可能會引起機構警覺，該交易或會涉及犯罪活動：

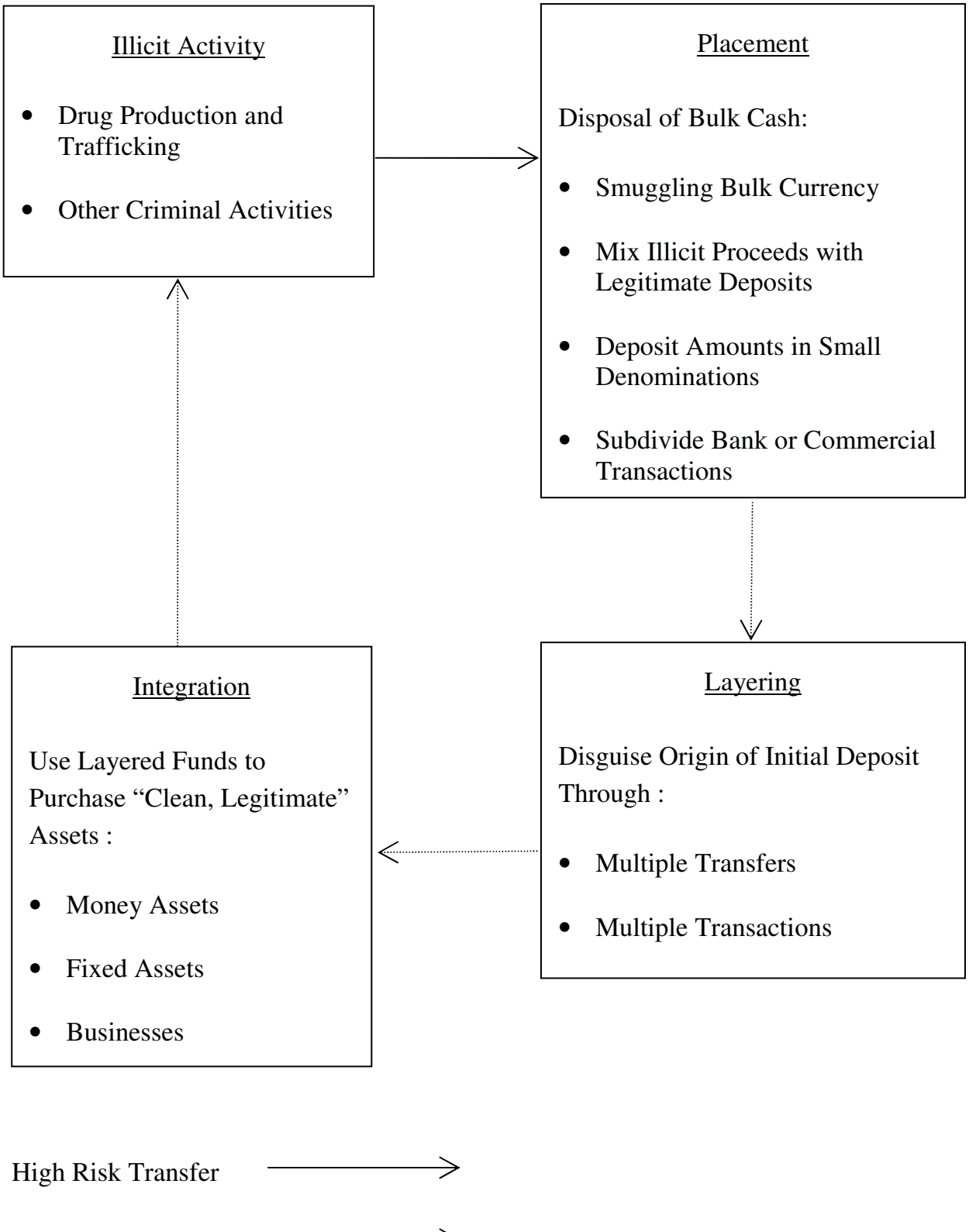
(a) 現金的處置 -- 實際處置來自非法活動的現金得益。

(b) 分層交易 -- 利用複雜多層的金融交易，將非法得益及其來源分開，從而掩飾查帳線索和隱藏罪犯身分。

(c) 融合 -- 爲犯罪得來的財富提供表面的合法性。假如分層交易的程序成功，經過洗錢過程的得益會透過融合手法回歸經濟體系，而這些得益在流回金融體系時，表面上已變成正常的商業資金。

2.5　　下圖更詳盡地說明洗錢的各個階段。

洗錢程序



3. 香港有關洗錢活動的法例

3.1 香港已制訂法例對付與販毒及嚴重罪行得益有關的洗錢活動。《販毒（追討得益）條例》於一九八九年九月生效。該條例訂有追查、凍結和沒收販毒得益的規定，並將有關販毒得益的洗錢活動訂爲刑事罪行。

3.2 《有組織及嚴重罪行條例》於一九九四年十二月生效。該條例以《販毒（追討得益）條例》爲藍本，並把洗錢活動罪行擴展至除販毒外，還包括可公訴罪行的得益。

3.3 該兩項條例其後均作出修訂，並於一九九五年九月一日同時生效。該等修訂收緊條例內有關洗錢活動的規定，並清楚指出舉報可疑交易的責任。尤其，該等修訂清楚載明，披露所知悉或懷疑的洗錢交易是一項法定責任。

3.4 下文概述兩項條例內有關洗錢活動的主要條文，但並不構成對所提及的法例條文的法律詮釋。如有需要，機構應諮詢適當的法律顧問。

3.5 根據《販毒（追討得益）條例》及《有組織及嚴重罪行條例》中的第 25(1)條，如有人知道或有理由相信任何財產全部或部分、直接或間接分別代表販毒或可公訴罪行得益而仍處理該財產，即屬犯罪。該項罪名最高刑罰爲監禁 14 年及罰款 500 萬港元。

3.6 根據該兩項條例第 25(2)條，如有關人士能證明其曾意圖在合理可行的情況下，盡快向獲授權人[1] 披露上文所述其知悉或懷疑的事項或有關事宜；或該名人士根據該兩項條例第 25A(2)條，證明其有合理的理由未能作出披露，則該名人士可以上述兩項理由作爲免責辯護。

3.7 兩項條例的第 25A(1)條均規定，任何人士如知道或懷疑任何財產是全部或部分、直接或間接代表販毒或可公訴罪行的得益，或

[1] 《販毒（追討得益）條例》及《有組織及嚴重罪行條例》第 2 條均界定獲授權人（authorized officer）指

(a) 任何警務人員；

(b) 根據《海關條例》（第 342 章）第 3 條設立的海關的任何成員；及

(c) 律政司司長爲本條例的目的而以書面授權的任何其他人士。

曾在或擬在與販毒或可公訴罪行有關的情況下使用，則該名人士有法定責任，須向獲授權人作出披露。根據第 25A(7)條，任何人士如未能作出該等披露，即屬違法，該項罪名最高刑罰爲第五級罰款（目前爲 25,001 元至 50,000 元）及監禁 3 個月。

3.8 《有組織及嚴重罪行條例》第 25(4)條規定，第 25 和 25A 條中凡提述可公訴罪行之處，包括若在香港發生即會構成可公訴罪行的行爲。即是說，任何人如果處理犯罪得益或沒有根據第 25A(1)條作出必要的披露，則即使主要罪行不是在香港發生，但如果在香港發生會構成可公訴罪行的話，便屬於違法。

3.9 第 25A(2)條規定，已作出必要披露的人士如有違反第 25(1)條的行爲，而該項披露與該行爲有關，則只要符合以下條件，該名人士並沒有犯罪：

(a) 他在有關披露後作出該行爲，而且他是在獲授權人同意的情況下作出該行爲的；或

(b) 他是在該行爲後作出有關披露的，而且他是主動在合理的範圍內盡快作出披露的。

3.10 第 25A(3)條規定，根據第 25A(1)條作的披露不得視作違反合約，或違反任何成文法則對披露資料所施加的規限，因此不得令作出披露的人士須對該項披露所引致的任何損失負上支付損害賠償的法律責任。基於以上理由，認可機構在根據該兩項條例作出披露時，毋須恐懼會違反機構對客戶所負上的保密責任。

3.11 第 25A(4)條擴充第 25A 條的條文，規定只要受僱人士是按僱主定下的披露程序向適當人士作出披露，則該等條文會如適用於向獲授權人作出披露一般。此舉可保障認可機構僱員，當他們向僱主指定人士報告所知悉或懷疑的洗錢交易後，不會因沒有向獲授權人作出披露而受到檢控。

3.12 根據該兩項條例第 25A(5)條，任何人士如知道或懷疑已有人作出披露，而仍向其他人士披露任何可能會影響洗錢活動調查的事宜，即構成「告密」罪名。「告密」罪名的最高刑罰爲入獄 3 年及罰款 50 萬元。

3.13 《2000 年有組織及嚴重罪行（修訂）條例》於 2000 年 6 月 1 日生效。除其他規定外，是項修訂條例要求匯款代理人及貨幣兌換商記錄有關客戶身分，以及 8,000 港元或以上或等值外幣的匯款和兌換交易的資料。雖然認可機構已獲豁免記錄該等資料的要求，然而，銀行業亦應實行相應的措施以確保業內對於打擊洗黑錢所遵行的標準能配合政府的有關政策。

4. 打擊洗錢活動的基本政策和原則

4.1 金融管理專員完全同意巴塞爾委員會於一九八八年十二月發出的原則聲明內，有關打擊洗錢活動的基本政策和原則。該項聲明引用以下原則，使有關人士無法透過銀行體系進行洗錢活動：

(a) 認識你的客戶：銀行應採取合理措施，確定客戶的真正身分，並制訂有效程序，查證新客戶的身分。

(b) 遵守法例：銀行的管理層應確保銀行按照嚴謹的道德標準經營業務，並遵守法例和規定。此外，認可機構如有充分理由懷疑某些交易與洗錢活動有關，便不予提供任何服務[2]。

(c) 與執法機關合作：在有關客戶資料保密規則的限制範圍內，銀行應與國家執法單位充分合作，包括在有合理理由懷疑有關客戶進行洗錢活動時，按照法例規定採取適當措施。

(d) 政策、程序和訓練：所有銀行均應正式採用符合巴塞爾聲明所載原則的政策，並確保所有在不同地點工作的有關員工均會知悉銀行的有關政策。此外，在員工訓練方面，銀行應留意巴塞爾聲明涉及的事項。銀行應在識別客戶身分及保留內部交易記錄方面實施具體程序，以確保能遵守這些原則。此外，銀行或需作出安排，擴充內部查核功能，以制訂有效機制，俾能全面符合巴塞爾聲明。

4.2 其後，國際金融特別行動組進一步發展巴塞爾委員會訂定的原則。一九九零年二月，國際金融特別行動組提出 40 項建議，旨在改善各國法制、加強金融體系所擔當的角色，以及促進國際間的合作，打擊洗錢活動。中國香港是國際金融特別行動組成員之一，並全面遵守該 40 項建議。

4.3 金融管理專員認爲，認可機構應遵守巴塞爾委員會發出的原則聲明，及國際金融特別行動組提出的建議所包含的基本政策和原則。具體來說，金融管理專員預期認可機構會備有下述政策、程

[2] 第 9.9 段描述將此原則應用於認可機構的實際情況。

序和監管措施：

(a) 認可機構應採納現行的法規要求，發出關於洗錢活動的明確政策聲明。銀行應以書面方式把這項聲明傳達予各分行、部門或附屬公司的全體管理層和有關員工，並應定期檢討該項聲明。

(b) 認可機構應根據本指引以下各章的建議編製指示手冊，列出有關以下各方面的程序：

- 開設戶口；
- 查證業務申請人的身分；
- 保存記錄；
- 舉報可疑交易。

(c) 認可機構應主動促進與執法機關的緊密合作關係，並須在其機構內定出單一的控制處（通常爲條例執行主任），指示職員向控制處迅速報告涉嫌洗錢的交易。這個控制處應與聯合財富情報組建立聯絡方法，確保涉嫌與販毒或其他可公訴罪行有關的洗錢交易得以迅速轉介至有關單位。此外，有關機構應清楚界定該控制處在舉報程序中所擔當的角色和承擔的責任。

(d) 認可機構應採取措施，在員工入職時，及其後定期就本指引所載事項教育及培訓員工。制訂這些措施的目的，是爲了培養員工對洗錢活動的認識，並保持一定程度的警覺性，能夠在有懷疑時作出舉報。

(e) 認可機構應指示內部查核／視察部門，定期查核員工有否遵行打擊洗錢活動的政策、程序和監察措施。

(f) 雖然有關方面瞭解治外法權規例的敏感性質，並明白認可機構的海外業務必須按當地法律和規例進行，但是認可機構仍應確保其海外分行和附屬公司認識集團對於洗錢活動的政策，並在適當情況下，指示其分行向當地的有關當局報告可疑個案。

第二部分
詳盡指引

5. 查證業務申請人的身分

5.1 一般而言，認可機構不應爲客戶開立匿名戶口或讓客戶以明顯是虛假的名義開戶。對於申請與機構建立業務關係（如開立存款戶口）的人士，機構應根據可靠的文件或其他資料來源，充分核實有關該等人士的身分以及其合法性，並把該等人士的身分和其他有關資料記錄在案。此外，任何申請人如聲稱代表他人行事，則認可機構也應確定該申請人獲得正式授權。

5.2 就本指引而言，在下列情況下，有關身分的證明應可視作足夠：

(a) 可合理確定業務申請人的身分正是他所聲稱的身分；及

(b) 取得證明的認可機構按照其所訂立的程序，滿意其已確立有關事實。

5.3 已廢除。[參閱《防止清洗黑錢活動指引補充文件》（《補充文件》）第 12 節]

<u>個人申請人</u>

5.4 認可機構應訂立有效程序，以充分核實業務申請人的身分，這包括取得有關姓名、永久地址、出生日期和職業等資料的程序。

5.5 認可機構應從官方或其他聲譽良好機關所簽發的文件（例如護照或身分證）證實業務申請人的身分。就香港居民而言，證明身分的最主要資料來源是身分證，而法例規定本港居民須隨身攜帶身分證。認可機構應將客戶的身分證明文件副本存檔。

5.6 不過，認可機構必須認識到，無論是任何形式的身分證明文件，都不能完全保證是真確的或是代表有關人士的真正身分。入境事務處設有熱線電話(28241551)，認可機構可利用熱線電話查詢該

身分證是否有效。假如對身分證明文件是否真確有懷疑，應立即使用此熱線查詢。

5.7 認可機構可循適當途徑，查核客戶的地址，例如要求查閱最近的公用事業或差餉單據。

5.8 認可機構如要求個人銀行服務申請人在有關申請書內提供已同意作諮詢人的人士的姓名和個人資料，認可機構應遵行由香港銀行公會和存款公司公會聯合發出的銀行營運守則內諮詢人一節列載的處理方法和程序。

公司申請人

5.9 即使是經營正當貿易業務的公司，公司戶口仍有可能成爲洗錢工具之一。因此，認可機構必須獲得足夠證明以核實主要股東[3]、董事和戶口簽署人的身分以及公司的業務性質。最基本的原則爲與該公司建立業務關係是安全可靠的。

5.10 認可機構與公司申請人建立業務關係前，應採取措施進行公司查冊及／或其他商業查詢，以確保有關的公司申請人並非已解散、被除名、清盤或結束營業，或正在進行解散、除名、清盤或結束營業。此外，如認可機構其後知悉公司的結構或擁有權有所變更，或經公司戶口進行的支付模式有所改變，因而引起懷疑，認可機構便應作出進一步查核。

5.11 認可機構應就於香港註冊的公司申請人，取得以下文件（如公司申請人在香港以外地方註冊，則應取得相應文件，而且這些文件最好經由註冊地的律師或會計師等合資格人士加以證明）：

(a) 公司註冊證書和商業登記證；

(b) 公司組織章程大綱及細則；

(c) 董事局議決開戶及授權有關人士處理該戶口的決議案；及

[3] 建議「主要股東」應包括有權行使或控制如何行使公司 10%或以上的投票權的人士。

(d) 於公司註冊處進行查冊。

5.12 已廢除。[參閱《補充文件》第 4 節]

5.13 已廢除。[參閱《補充文件》第 4 節]

會社、會所和慈善組織

5.14 如屬會社、會所和慈善組織開設的賬戶，認可機構應確定有關組織的合法目的，例如機構可要求查看組織的章程。認可機構應按照對個人申請人的要求，充分核實機構並不認識的獲授權簽署人的身分。

並未註冊爲法團的企業

5.15 對於合夥業務及其他並未註冊爲法團的企業，如銀行不認識該等商號的合夥人，則應按照對個人申請人的要求，充分核實最少兩位合夥人和所有獲授權簽署人的身分。如果訂有正式合夥協議，銀行應取得合夥商號發出授權開戶以及授權有關人士處理該戶口的委託書。

空殼公司

5.16 空殼公司是可以進行金融交易的法律個體，不過這些公司本身並不具有實質的商業業務。儘管空殼公司可用於合法用途，但國際金融特別行動組對於越來越多人利用這些公司進行洗錢活動的情況（罪犯可利用空殼公司處理實質上是匿名的戶口），表示關注。認可機構應注意洗錢人可能濫用空殼公司，因此在處理空殼公司事宜上，要十分謹慎。認可機構應遵從「認識你的客戶」的原則，充分核實空殼公司的實益擁有人、董事和獲授權簽署人的身分。如果空殼公司是由代表空殼公司的專業顧問人作中間人，介紹予認可機構，認可機構便應遵從下文第 5.17 段至 5.22 段的指引。

業務申請人代表他人行事的情況

5.17 罪犯經常利用信託戶口和代名人戶口來逃避身分查證程序，掩飾犯罪得來的金錢的來源，以進行洗錢活動。因此，認可機構應向業務申請人取得確認，確定該申請人是否以他人的受託人、代名人或代理人的身分行事。

5.18 任何代他人開戶或進行交易的申請，如申請人沒有表明其受託人或代名人身分，認可機構應視有關申請爲有可疑，並進一步查詢相關委託人的身分和有關的業務交易的性質。

5.19 認可機構應充分核實受託人、代名人和戶口簽署人的身分，以及其受託人或代名人身分的性質和責任，例如認可機構可索取信託契據副本。認可機構也應查證業務申請人是否受官方機構監管（例如是等同金融管理局的機構）。

5.20 假如信託所屬的司法地區沒有等同香港的洗錢法例，認可機構便應加倍留意。

5.21 已廢除。[參閱《補充文件》第 6 節]

5.22 已廢除。[參閱《補充文件》第 6 節]

專業事務所客戶戶口

5.23 已廢除。[參閱《補充文件》第 7 節]

避免接受郵遞方式開戶

5.24 已廢除。[參閱《補充文件》第 8 節]

5.25 已廢除。[參閱《補充文件》第 8 節]

爲非戶口持有人（非經常客戶）進行的交易

5.26 認可機構如替非戶口持有人辦理交易，例如要求電匯，或將資金存入現有戶口，而該存款人士的姓名不在該戶口的委託書上，則須謹慎處理和提高警覺。如交易涉及大量現金，或是屬於不尋常的交易，則應要求申請人出示上文所述機關發出的明確身分證明文件，又如屬外籍人士，則應記錄其國籍。機構須將該等身分證明文件副本存檔。

5.27 已廢除。[參閱《補充文件》第 3.12 至 3.16 段]

提供保管和保管箱服務

5.28 認可機構須謹慎處理保管盒子、包裹和密封信封的要求。假如非戶口持有人亦可使用這些服務，則須遵循上文所述的身分證明程序辦理。

6. 匯款

6.1 已廢除。[參閱《補充文件》第 9 節]

6.2 已廢除。[參閱《補充文件》第 9 節]

6.3 已廢除。[參閱《補充文件》第 9 節]

7. 保存記錄

7.1 《販毒（追討得益）條例》及《有組織及嚴重罪行條例》賦予法庭權力，審查被告過往所有有關交易，以評估被告曾否從販毒或其他可公訴罪行中獲利。

7.2 調查當局需確保對涉嫌洗錢交易備有足夠的查帳線索，並能夠確立涉嫌戶口的財務概況。舉例來說，爲達到這些要求，調查當局可尋求以下資料：

(a) 戶口的實益擁有人（關於代第三者開立的戶口，請參閱第 5.17 至 5.23 段）；

(b) 經由該戶口提存的資金的數額；

(c) 就某些交易而言：

- 資金的來源（如知道）；
- 提存資金的方式，如以現金、支票等；
- 進行交易的人的身分；
- 資金目的地；及
- 指示和授權的方式。

7.3 一個重要的目標是認可機構在交易進行中的任何階段，都能找到有關資料（以能夠獲得的資料爲限），並且不會造成不必要的延誤。

7.4 認可機構訂立保留文件政策時，必須權衡法律規定與調查當局的需要，以及正常商業考慮。不過，認可機構應盡量遵循以下保留文件的時限：

(a) 開戶記錄--身分證明文件副本須由結束戶口起計保存 6 年[4]；

(b) 帳簿記錄--由交易記帳起計 6 年[4]；及

(c) 各種形式的記帳憑據，如存款單／提款單、支票和其他形式的單據--由作出記錄起計 6 年[4]。

---

[4] 6 年是《時效條例》所訂若干類別申索的法定期限。

(d) 替非戶口持有人辦理的電匯和貨幣兌換交易的憑據—由作出記錄起計 6 年[4]。

7.5 保留的方式可以是文件正本、以縮微膠卷儲存，或以電腦儲存，只要這些方式是在《證據條例》第 20 至 22 條下可被接納爲證據的。如記錄是與進行中的調查有關，或與已經披露予有關當局的交易有關，則須加以保留，直至證實該宗調查已經結束爲止。

8 識別可疑交易

8.1 由於洗錢人可利用的交易類別不可勝數，故難以界定何爲可疑交易。不過，可疑交易往往與客戶的已知的合法業務或個人活動，或該類戶口的正常業務不符。因此，要識別洗錢活動的首要條件，是要對客戶的業務有足夠認識，這樣才可以識別某宗交易或某一連串交易屬於不尋常。

8.2 附件五載有可能屬於可疑交易的例子。這些例子無法盡列，只屬洗錢活動最基本途徑的例子。不過，當認可機構認出附件五所列的任何交易類別時，應進行進一步調查，及最低限度對其資金來源作出初步查詢。

9. 舉報可疑交易

9.1 根據《販毒（追討得益）條例》及《有組織及嚴重罪行條例》，由警務處和香港海關共同組成的聯合財富情報組是接受披露資料的機關。

9.2 聯合財富情報組除了負責接受機構或個人披露資料外，亦在一般洗錢活動方面擔當本港和國際顧問，並就洗錢活動問題向金融界提供實際指引和協助。

9.3 個別人士如懷疑有洗錢交易，即有責任舉報。每間機構應委任一名或多名指定人員（條例執行主任），負責在有需要時按照《販毒（追討得益）條例》及《有組織及嚴重罪行條例》第 25A 條，向聯合財富情報組舉報，而所有內部報告亦應向指定人員提出。

9.4 條例執行主任應保存所有向聯合財富情報組作出報告的記錄，僱員向他們作出的所有報告，亦應保存記錄。條例執行主任應以書面確認收到僱員向他們作出的報告，此等書面認收文件可作爲部分證明文件，證實報告是遵照內部程序而作出的。

9.5 認可機構的僱員如知悉客戶進行販毒或其他可公訴罪行，而該客戶又存入、調動或意圖投資資金或以這些資金作抵押而取得信貸，或機構代這些客戶持有資金，有關僱員必須從速向條例執行主任報告有關詳情，而條例執行主任必須隨即向聯合財富情報組舉報。

9.6 認可機構的僱員若懷疑或有合理理由相信客戶進行販毒，或其他可公訴罪行，而該客戶又存入、調動或意圖投資資金或以這些資金作抵押而取得信貸，或機構代這些客戶持有資金，有關僱員必須從速向條例執行主任報告。條例執行主任必須迅速評定這種想法是否有合理理由。除非他認爲並無合理理由，並將其意見記錄在案，否則必須隨即向聯合財富情報組舉報。

9.7 認可機構必須採取步驟，確保所有與資金的持有、收取、傳送或投資（不論以現金或其他方式）有關的僱員，或以這些資金作抵押而給予貸款有關的僱員，都知道這些程序，並了解在知道或遇有認爲有合理理由相信有違法行爲存在的情況而未有舉報，即屬

刑事罪行。

9.8 認可機構應在合理情況下盡快向聯合財富情報組舉報可疑交易。有關方面鼓勵使用附件六所載標準格式舉報，或若爲「STREAMS」註冊用戶，可透過該電子渠道舉報。假如需要作緊急披露，特別是有關正接受調查的戶口，應以電話作初步通知。

9.9 認可機構如知道或懷疑交易與洗錢活動有關，應避免進行這些交易，直至它們通知聯合財富情報組，並獲得情報組同意進行該等交易。如機構無法避免進行這些交易，或如避免進行這些交易會使追查涉嫌洗錢活動的受益人的努力白費，則認可機構可繼續進行交易，並應在合理時間內盡快主動通知聯合財富情報組。

9.10 認可機構有時候會基於極度懷疑個別人士的誠信，和擔心可能會涉及犯罪活動，而拒絕爲業務申請人開戶，或拒絕受理非戶口持有人的要求。認可機構必須根據正常的商業準則及內部政策來作出上述決定。然而，爲了防止出現洗錢活動，認可機構有必要確立對可疑資金的查帳線索。因此，在切實可行的情況下，認可機構應嘗試取得及保留其可取得的有關身分證明文件，並把可疑資金向聯合財富情報組舉報。

9.11 如認可機構已得悉或懷疑聯合財富情報組已接獲舉報，並需要對客戶進行進一步的查詢時，認可機構應加倍小心，確保客戶不會察覺其資料已爲執法單位所注意。

9.12 聯合財富情報組收到披露資料及予以研究後，所披露的資料便會交由警務處和香港海關轄下受過訓練的財富調查人員作進一步調查，包括向作出披露的機構和其他來源尋求補充資料。有關人員接著會進行謹慎的調查，以確立懷疑的依據。

9.13 只有警務處和香港海關轄下的財富調查人員才可以取閱所披露的資料。如果會提出檢控，有關人員便會取得提交令，以便將該等物料呈上法庭。《販毒（追討得益）條例》及《有組織及嚴重罪行條例》第 26 條，均對公開根據第 25A 條作出披露的人士的身分，訂有嚴格限制。有關方面認爲維持各執法單位與機構所建立的互相信任關係是極爲重要的。

10. 調查當局的回應

10.1 對於認可機構根據《販毒（追討得益）條例》及《有組織及嚴重罪行條例》第 25A 條及《聯合國（反恐怖主義措施）條例》第 12 條作出的披露，聯合財富情報組在收到舉報後會予以確認。如無逼切需要採取行動，例如對戶口發出限制令，有關方面通常會同意讓該機構根據《販毒（追討得益）條例》及《有組織及嚴重罪行條例》第 25A(2)條的規定操作該戶口。本指引附件七載有認收函件樣本。若以「STREAM」電子渠道提交披露資料，該渠道將發出電子收據。

10.2 雖然法例並無規定要向作出披露的人士提供有關調查的資料，但警務處和香港海關了解訂立有效回應程序的重要性。聯合財富情報組現時設有一項服務，在披露機構提出要求時，會提供有關調查的現況。

11. 職員教育及訓練

11.1 職員必須認識本身在《販毒（追討得益）條例》、《有組織及嚴重罪行條例》及《聯合國（反恐怖主義措施）條例》下的個人責任，他們個人可能要對沒有向有關當局舉報資料負上法律責任。認可機構必須鼓勵他們與執法單位充分合作，迅速舉報可疑交易。此外機構應告知其職員，遇有可疑交易，即使他們未能確切知道所涉及的主要犯罪活動或所發生的非法活動，也應向其機構的條例執行主任舉報。

11.2 因此，認可機構必須引入全面的措施，確保職員完全認識他們的責任。

11.3 認可機構應爲本地及海外職員提供防範洗錢活動的適當訓練。個別機構將因應本身的需要，爲各部門職員編訂訓練計劃的時間和內容。不過，以下的建議可能會適用：

(a) 新僱員

所有新僱員如果會接觸客戶或會處理其交易，則不論職位高低，機構均應向其解釋洗錢活動的背景，識別可疑交易和向適當的指定單位報告可疑交易的需要，以及「告密」罪行等資料。他們應認識到法例規定機構須舉報與販毒及其他可公訴罪行有關的可疑交易，而僱員本身在這方面亦有個人法定責任。

(b) 出納員／櫃員／外匯人員／顧問人員

凡需直接與公眾接觸的職員，就可能成爲洗錢人的首個接觸對象，因此，他們的努力對機構打擊洗錢活動的策略極爲重要。他們應認識本身的法律責任，以及機構內舉報這些可疑交易的制度。

認可機構應訓練職員如何識別會引起懷疑的交易，以及在發覺交易有可疑時要採取的程序。最重要的是前線職員要認識機構處理非經常客戶的政策，特別是涉及大量現金交易的情況時，需特別提高警覺。

(c) 開戶／處理新客戶的人員

凡負責處理開戶工作，或接受業務申請人的申請的職員，

必須接受上文第(b)段所述給予出納員等的訓練。此外，機構必須令他們了解查證申請人身分的需要，並就機構開立戶口和客戶身分查證程序給予訓練。這些職員應認識到，遇有客戶提供可疑資金，或要求進行可疑交易，不論資金獲接納與否，或該等交易進行與否，都需要向有關當局舉報，並且必須知道在這方面所要遵循的程序。

(d) 行政／營業主管和經理

認可機構應向負責督導和管理職員的人員，提供涵蓋洗錢程序各有關方面的較高層次及深入的指示。這包括《販毒（追討得益）條例》及《有組織及嚴重罪行條例》內的罪行和刑罰；與送達提交令和限制令有關的程序；以及保存記錄的規定。

(e) 持續訓練

認可機構亦須定期安排複修訓練，以確保職員不會忘記其責任。

(f) 訓練計劃

香港銀行公會製作了專供訓練前線職員之用的材料，認可機構應購備充足數量。

附件一

已廢除

附件二

已廢除

附件三

已廢除

附件四

已廢除

附件五

可疑交易舉例

1. 利用現金交易進行洗錢活動

a) 個別人士或公司存入異常龐大的現金，而其表面業務活動通常是透過支票及其他工具進行。

b) 任何個人或公司的現金存款在沒有明顯原因下大量增加，特別是假如這些存款其後在短期內自戶口調走及／或轉至一個通常與該客戶沒有關連的目的地。

c) 客戶利用許多存款單存入現金，使到每項存款的總額並不引人注目，但所有存款合計則數目非常龐大。

d) 公司戶口的交易，包括存款及提款，均以現金進行，而不利用一般與商業運作有關的付款和入帳方式（例如支票、信用證、匯票等）。

e) 客戶經常支付或存入現金，藉以要求銀行發出銀行匯票，進行貨幣轉移或取得其他可轉讓及隨時可出售的貨幣票據。

f) 客戶要求將大量細面額現鈔轉爲大面額現鈔。

g) 經常將現金轉換爲其他貨幣。

h) 分行的現金交易較平常的大幅增加（總行的統計數字應可察覺現金交易的異常情況）。

i) 客戶的存款中有僞鈔或僞造工具。

j) 客戶將大筆金錢轉到海外地點或從海外地點轉入大筆金錢，並指定以現金付款。

k) 利用夜間保管設施存入大量現金，藉此避免與機構直接接觸。

l) 儘管客戶在機構設有戶口，仍利用現金結算方式購入或出售大量外幣。

m) 客戶經常存入大量現金，但戶口支票則大多發給通常與其零售業務沒有關連的個別人士及公司。

2. 利用銀行戶口進行洗錢活動

a) 客戶希望保持多個似乎與其業務種類（包括涉及名義上的交易）不符的受託人或客戶戶口。

b) 客戶擁有多個戶口，並把現金存入每個戶口，而這些存款合計起來金額非常龐大。

c) 任何個人或公司戶口顯示幾乎沒有一般個人銀行或與商業有關的活動，而是用來接收或支付大量沒有明顯用途或與戶口持有人及／或其業務沒有明顯關係的金錢（例如，戶口的來往數額大幅增加）。

d) 開立戶口時不願意提供一般資料、提供極少或虛假資料，或在申請開立戶口時，提供機構難以查證或需昂貴費用方可查證的資料。

e) 客戶似乎在同一地區的多間機構開有戶口，特別是如機構察覺客戶通常是從這些戶口集中存款，才要求將資金轉往他處。

f) 支出額與同日或前一天的現金存款額互相吻合。

g) 存入經背書轉予客戶的大額第三者支票。

h) 從一個原本不活動的戶口或剛從海外突然收到一大筆存款的戶口，提取大量現金。

i) 多名客戶一同在同一時間要求不同的出納員處理大額現金交易或外匯交易。

j) 個別人士較多使用保管設施，而且利用密封包裹進行提存。

k) 公司代表避開與分行接觸。

l) 專業公司利用客戶戶口或公司內部戶口或信託戶口存入的現金或可轉讓票據數額大幅上升，特別是假如這些存款迅速在其他客戶公司及信託戶口間轉帳。

m) 客戶拒絕提供有關資料，而在一般情況下，這些資料是會使客戶有資格獲得信貸或其他被視爲重要的銀行服務。

n) 多位人士在沒有足夠理由的情況下，將款項存入同一戶口。

o) 客戶以其宣稱從事的業務類型爲理由，擁有異常大量的戶口，並／或在此等戶口之間進行過度頻密的資金轉撥。

p) 資金周轉速度迅速，即戶口每日開始與結終時的結餘均不多，並不能反映該戶口的巨額資金流量。

q) 多名存戶同時使用單一銀行戶口。

r) 戶口以一外幣兌換商名義開立，並接受有規律的存款。

s) 戶口以一離岸公司名義運作，其資金流動屬有規律性質。

3. 利用與投資有關的交易進行洗錢活動

a) 購入證券而交由機構保管，但從該客戶表面情況看來，此舉似乎並不適合。

b) 與人所共知的販毒地區內的海外金融機構附屬公司或聯號進行對銷存款／貸款交易。

c) 客戶要求提供投資管理服務（外幣或證券），而資金來源並不明確或與客戶的表面情況不符。

d) 以現金結算較大數額或不尋常的證券交易。

e) 沒有明顯目的或在似乎不尋常的情況下買賣證券。

4. 涉及離岸國際活動的洗錢活動

a) 由設於製毒或販毒活動可能十分猖獗的國家的海外分行、聯號或其他銀行介紹的客戶。

b) 利用信用證或其他貿易金融方法在國家間調動金錢，而這種貿易與客戶的日常業務不符。

c) 客戶定期將大筆不能明確地鑑定爲真正交易的款項（包括電傳交易）支付予通常和毒品的製造、處理或銷售有關的國家，或定期從這些國家收到大筆款項。

d) 累積大量結餘，與客戶的已知業務營業額不符，而這些款項其後轉入客戶在海外的戶口。

e) 客戶以存入及支出的方式或沒有透過戶口進行原因不明的電子資金轉帳。

f) 經常要求發給旅行支票、外幣匯票或其他可轉讓票據。

g) 經常存入旅行支票及外幣匯票存款，特別是這些支票及匯票是海外發出的。

h) 戶口收到許多電傳轉帳，但每宗轉帳數額均低於匯款國家中的申報規定。

i) 客戶從避稅天堂的國家接受電傳轉帳，或向此等國家發出電傳轉帳，尤其是客戶並沒有明顯商業理由進行此等轉帳，又或此等轉帳與客戶的業務或過往情況不符合。

5. 涉及認可機構僱員及代理人的洗錢活動

a) 僱員個性有所轉變，例如生活奢華。

b) 任何與代理人進行的交易，但未能獲悉最終受益人或對方的身分，違反了有關業務種類的正常程序。

6. 利用有抵押及無抵押貸款進行洗錢活動

a) 客戶突然能夠清償問題貸款。

b) 要求將資產抵押予機構或第三者，以便獲得貸款，但資產的來源不詳或資產與客戶的情況不符。

c) 客戶要求機構提供或安排資金，但客戶在有關交易所提供資金的來源並不明確，特別是如其中涉及物業。

d) 客戶不願意或拒絕說明貸款的目的，或償還款項的來源，又或提供一個可疑的目的或來源。

附件六

根據《販毒（追討得益）條例》及《有組織及嚴重罪行條例》第 25A 條向聯合財富情報組作出報告

日期：
檔號：

(A) 來源

機構名稱：	
報告人員：	電話號碼：
簽署：	圖文傳真：

(B) 懷疑

（請提供引起懷疑的交易的詳情及任何其他有關資料，並請附上該交易的副本以供參考。帳戶持有人或辦理該項交易的人士的個人資料請填在第二頁。）

(C) 其他資料

這是一項新披露的資料：	是／否	聯合財富情報組編號：
這項資料與以前披露的一項資料有關：	聯合財富情報組編號：	銀行檔號：

(D) 對象(1)

姓名：	中文姓名電碼：	出生日期：
香港身分證／護照號碼：	性別：男／女	國籍：
地址：		
職業：	公司：	
擔任職位：	公司地址：	

對象(2)

姓名：	中文姓名電碼：	出生日期：
香港身分證／護照號碼：	性別：男／女	國籍：
地址：		
職業：	公司：	
擔任職位：	公司地址：	

對象(3)

姓名：	中文姓名電碼：	出生日期：
香港身分證／護照號碼：	性別：男／女	國籍：
地址：		
職業：	公司：	
擔任職位：	公司地址：	

(E) 有關銀行戶口

	(1)	(2)
帳號：		
帳戶類別：		
開立日期：		
帳戶結餘：		
帳戶持有人：		

	(3)	(4)
帳號：		
帳戶類別：		
開立日期：		
帳戶結餘：		
帳戶持有人：		

附件七

Example of Acknowledgement of Receipt by JFIU

Date:

The Compliance Officer
[ ] Bank Ltd.

Fax No. :

Dear Sir/Madam,

Acknowledgement of Receipt of
Suspicions Transaction Report(s) ("STR")

I acknowledge receipt of the attached STR made in accordance with the provisions of section 25A(1) of the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap 405) / Organized and Serious Crimes Ordinance (Cap 455) and section 12(1) of the United Nations (Anti-Terrorism Measures) Ordinance(Cap 575).

Based upon the information currently in hand, consent is given under the provisions of section 25A(2) & (3) of Cap 405 and 455 and section 12(2) & (3) of Cap 575.

If you have any queries, please feel free to contact the undersigned on telephone number (852)xxxxxxxx.

Yours faithfully,

( )
Joint Financial Intelligence Unit

附件八

已廢除

防止清洗黑錢活動指引

補充文件

金融管理專員根據《銀行業條例》

第 **7(3)** 條發出的指引

2010 年 7 月修訂

目錄

1. 引言

1.1 現行的《防止清洗黑錢活動指引》(指引)是金管局在 1997 年發出，並於 2000 年予以修訂，主要是把《2000 年有組織及嚴重罪行（修訂）條例》的規定納入指引內。

1.2 其後這個範疇有多項重要發展，需要把防止清洗黑錢活動的標準提高。這些發展包括巴塞爾銀行監管委員會在 2001 年 10 月發出一份《銀行仔細查證客戶身分》的文件，以及打擊清洗黑錢財務行動特別組織（特別組織）在 2003 年 6 月發出經修訂的 40 項建議。此外，「九一一」事件將打擊清洗黑錢活動的範疇擴闊至包括打擊恐怖分子的籌資活動。

1.3 鑑於這些發展及國際組織的有關推動措施，金管局認爲有必要修訂這方面的監管要求。金管局認爲暫時適宜以補充文件來反映有關修訂，以待金管局修訂指引，納入自 2000 年以來的所有變動，並使指引與其他金融監管機構的規定更趨一致。

1.4 本補充文件的內容主要反映上述巴塞爾委員會的文件所建議的監管標準，同時亦包含特別組織經修訂的 40 項建議的有關規定。此外，本補充文件亦載有金管局自 2000 年發出的其他有關建議。關於恐怖分子籌資活動，及香港最近頒布的反恐法例的建議亦包括在內。

1.5 除非另有說明，本補充文件中的規定應與指引中的相關內容（2010 年 7 月版載於金管局的網頁 ***http://www.info.gov.hk/hkma/chi/guide/index.htm***）以及隨附的闡釋備註（備註）一併閱讀或解釋。

1.6 除非另有說明，本補充文件的規定適用於所有新客戶及現有客戶按照本補充文件第 12 節的規定而需要進行的查核。

1.7 如屬在香港註冊的認可機構，本補充文件的規定亦適用於其境外分行或附屬公司[備註 1]。若當地的規定與本補充文件的規定有所不同，有關的境外業務單位應在當地法律許可的範疇內採用較高的標準。若境外分行或附屬公司未能遵行其集團標準，有關認可機構應知會金管局。

1.8 本經修訂的補充文件於 **2010 年 11 月 1 日**生效，屆時將取代 2009 年 7 月 17 日發出的版本。

2. 客戶接納政策

2.1 本節是新的部分，指引目前並未載有有關規定。

2.2 認可機構應制定客戶接納政策及程序，以識別清洗黑錢風險較高的客戶類型（見備註「一般指引」部分內的風險爲本方法）。認可機構應對高風險客戶採取更爲詳盡的客戶查證程序。此外，認可機構亦應定有清晰的內部指引，說明需要哪一級的管理層的批准才可與該類客戶建立業務關係。

2.3 認可機構在判斷某位客戶或某類型客戶的風險狀況時，應考慮以下因素：

(a) 客戶的國籍、公民身分及居民身分（如屬公司客戶，客戶的註冊地）、客戶業務的所在地、客戶交易對手及業務夥伴的所在地，以及客戶是否與較高風險地區、沒有執行或沒有充

分執行特別組織建議的地區（見下文第 14 節）或據認可機構所知並沒有制定適當的防止清洗黑錢活動標準或客戶查證程序的地區有關連[備註 3]；

(b) 客戶的背景或概況，例如客戶是政界人士或與政界人士有關連（見下文第 10 節），或屬於富有人士而其存入戶口的資金來源（初時及其後）並不清晰；

(c) 客戶業務的性質，特別是面對較高清洗黑錢風險的行業，例如貨幣兌換商或賭場等處理大量現金的行業；

(d) 如屬公司客戶，其所有權結構是否過度複雜而又沒有充分理由；及

(e) 反映客戶屬風險較高類型的任何其他資料（例如客戶遭另一家機構拒絕與其建立銀行業務關係的資料）。

2.4 在接納客戶後，若其戶口活動模式與認可機構對該客戶的認識並不相符，認可機構便應考慮把有關客戶重新歸類爲高風險類型。

3. 客戶查證

3.1 本節加強指引第 5.1 及 5.2 段的規定並引入新規定。

3.2 客戶查證程序應包含以下各項：

(a) 識別直接客戶，即要知道有關個人或法律實體的身分；

(b) 透過可靠及獨立來源所得的文件、數據或資料核實客戶身分[備註 4]；

(c) 識別實益擁有權及控制權，即確定最終擁有或控制直接客戶的個人及／或代表其進行交易的人士；

(d) 採取合理措施核實客戶的實益擁有人及／或代表其進行交易的人士的身分，並與(c)項所提供的資料對證；

(da) 獲取有關客戶開設戶口或建立業務關係的目的和理由的資料（除非客戶開設戶口或建立業務關係的目的和理由是明顯的）；及

(e) 持續進行查證及審察，即在維持業務關係期間內持續審察所進行的交易以確保這些交易與認可機構對客戶以及其業務及風險狀況的認識是一致，包括如有需要應確認資金來源。

3.3 個人的身分包括其姓名（以及其舊名或別名）、出生日期、國籍及香港身分證號碼[備註 5]。爲方便持續進行查證及審察，認可機構亦須取得有關個人的職業[備註 7]或業務的資料。認可機構亦應記錄及核實與其有業務關係的直接客戶的地址[備註 6]。至於有關連人士（即戶口簽署人、董事、主要股東等）或替非戶口持有人進行的交易，認可機構應按照風險水平及重要性來決定是否需要核實這些人士的地址。

3.4 如客戶在沒有充分理由的情況下，不願意提供認可機構所要求的資料及與認可機構合作進行客戶查證程序，這已是認可機構理應懷疑的因素。

3.5 若認可機構設有保密號碼戶口（即認可機構知悉戶口持有人士的姓名／名稱，但其後的有關文件均以戶口號碼或代號來取代戶口持有人士的姓名／名稱），則即使有關交易是由指定員工進行，認可機構亦應進行同樣的客戶查證程序。認可機構應讓相當數目的職員可知悉戶口持有人士身分以進行適當的查證程序。在任何情況下，該等戶口都不應用作向認可機構的條例遵行部門或金管局隱瞞客戶的身分。

3.6 一般而言，認可機構應待至順利完成查證程序後才與新客戶建立業務關係。然而，認可機構在核實身分的程序完成前開戶亦是可接受的做法，但必須能迅速取得所需的身分證明文件。在類似的情況下，認可機構在圓滿核實客戶身分之前，不應允許資金從該客戶戶口支付給第三方[備註 8]。

3.7 若開戶後未能順利完成核實身分程序，認可機構應結束有關戶口及把戶口內任何款項退還予該等款項的來源處[備註 9] 。此外，認可機構亦應考慮是否需要向聯合財富情報組（情報組）舉報。認可機構是否退還款項，應視乎情報組有否要求凍結有關款項。

3.8 認可機構與客戶建立業務關係後，應定期檢討有關客戶的現有記錄，以確保該等記錄載有最新及相關的資料。正如第 12.3 段所載，在遇有某些觸發事件時便應進行有關檢討。

非戶口持有人進行的交易

3.9 本節補充指引第 5.26 段。

3.10 若認可機構爲與其沒有業務關係的客戶（即非戶口持有人）執行超過 120,000 港元的交易[備註 9a]，則不論該交易只牽涉單一個程序

或多個有明顯相連關係的程序來進行，認可機構亦應完成以下各項：

(i) 識別及核實該直接客戶的身分；
(ii) 識別及核實代表該客戶的任何個人的身分，包括該等人士所獲的行事授權；
(iii) 查詢是否有任何實益擁有人，並採取合理措施核實該實益擁有人的身分；
(iv) 若該客戶是一間公司，則採取合理措施了解其所有權結構；以及
(v) 查明該交易的原擬性質及目的，除非這兩方面已很明顯則無此需要。

3.11 若有懷疑清洗黑錢或恐怖分子籌資活動，則不論是否超過 120,000 港元的門檻，認可機構爲非戶口持有人執行任何交易時均應進行第 3.10(i)至(v)段所列的程序。

非戶口持有人電匯及貨幣兌換交易的額外規定

3.12 本節取代指引第 5.27 段。

3.13 儘管以上第 3.10 段訂明有關門檻，電匯及貨幣兌換交易均須遵守下述規定：

電匯

3.14 若作爲電匯的付款機構，不論金額多少，認可機構均應記錄匯款人的身分及地址。若電匯金額相當於 8,000 港元或以上，認可機構應透過查驗匯款人的身分證或旅行證件核實其身分[備註 9b]。

3.15 若作爲電匯的收款機構而收款人並非戶口持有人，不論金額多少，認可機構均應記錄收款人的身分及地址。若電匯金額相當於 8,000 港元或以上，認可機構應透過查驗收款人的身分證或旅行證件核實其身分[備註 9b]。

貨幣兌換交易

3.16 若代客戶辦理相當於 8,000 港元或以上的貨幣兌換交易，而該客戶並非戶口持有人，認可機構必須記錄該人士的身份及地址並透過查驗該名人士的身分證或旅行證件核實其身分[備註 9b]。

4. 公司客戶

4.1 本節取代指引第 5.12 及 5.13 段，但不適用於當客戶是另一家銀行的情況(有關規定見下文第 11 節）。

4.2 若客戶是在認可證券交易所上市的公司[備註 10]或是國有企業，或是上市公司或國有企業的附屬公司，該客戶本身可以被視爲身分有待核實的人士。因此，若認可機構已取得及保存足夠資料以有效地識別及核實該客戶的身分（包括其在認可證券交易所的上市地位的證明）、獲委任代該客戶行事的人士及身分，以及其獲有關授權的證明，則在一般情況下應已足夠[備註 11]。

4.3 若上市公司實際上是由一名個人或一小撮個人控制，則認可機構應考慮是否需要核實該等個人的身分。

4.4 若一家非銀行金融機構是獲證券及期貨事務監察委員會(證監會)、保險業監理處(保監處)或特別組織的成員國／地區或對等標準地區

[備註 14]的同等監察機構認可並受其監管，則認可機構一般只需核實該等機構是在有關地區的獲認可（及受監管）金融機構名單上。認可機構應獲取並保留任何代表金融機構的個人其具備所需授權的證明文件。

4.5 若一家公司並非在認可證券交易所上市[備註 15]（或並非該等上市公司的附屬公司）或並非國有企業，或不是上文第 4.4 段提及的非銀行金融機構，則認可機構應查看該公司的背景[備註 16]，以識別其實益擁有人以及對資金擁有控制權的人士。即是說認可機構除了取得指引第 5.11 段註明的文件外，亦應核實[備註 17]該公司的所有主要股東[備註 13]、最少一位董事及其所有戶口簽署人[備註 19]的身分。認可機構應按照風險水平及重要性來考慮是否需要核實額外董事的身分。

4.6 若認可機構的直接客戶並非上市公司，而其所有權結構爲多個層次的公司所組成，則認可機構當然無需逐一查核所有權結構內的每家中間公司（包括其董事）的詳情。認可機構的目標應該是隨著所有權結構追查其直接客戶的最終主要實益擁有人，並核實該等實益擁有人的身分[備註 20]。若客戶在其所有權結構中有下述其中一個實體，則在一般情況下認可機構只須按照上文第 4.2 及 4.4 段的建議核實該實體的身分。然而，認可機構仍須核實在所有權結構中沒有與下述實體有關連的實益擁有人的身份。

(a)在某個認可證券交易所上市的公司或是該上市公司的附屬公司；

(b) 國有企業或國有企業的附屬公司；

(c) 受金管局、證監會或保監處監管的機構；或

(d) 受特別組織成員國／地區或對等標準地區就打擊清洗黑錢及恐怖分子籌資活動的目的履行相當於金管局、證監會或保監處的職能的監管機構所監管的金融機構。

4.7 認可機構應了解非上市公司客戶的所有權結構，並了解其資金來源[備註 21]。正如第 2.3(d)段所述，過度複雜而又沒有充分理由的所有權結構就是認可機構需要考慮的風險因素。

4.8 認可機構與具有名義股東的公司開始進行業務交易時應特別謹慎，並應取得該等公司的實益擁有人身分的足夠證明。

4.9 認可機構在與股本中有重大比例屬於不記名股票的公司交易時亦應特別謹慎。認可機構應制定程序監察所有主要股東的身分。認可機構可能需要考慮是否以託管形式持有不記名股票，使有關公司不能隨意轉移該等股票[備註 22]。

5. 信託及代名人戶口

5.1 本節應與指引第 5.17 至 5.20 段一併閱讀。

5.2 認可機構在處理信託或代名人戶口時，應了解有關各方的關係。認可機構應取得受託人或代名人及受託人或代名人所代表行事的人士身分的足夠證明[備註 23]，以及有關的信託或其他類似安排的性質的詳情。

5.3 具體來說，認可機構應就信託取得有關受託人、保護人[備註 24]、財產授予人／資產提供者[備註 25]及受益人身分的滿意證明。若有

指定受益人，則認可機構應盡可能識別該等受益人身分[備註 26 及 27]。

5.4 與其他類型的客戶一樣，認可機構應就信託及與信託有關連的人士採取風險爲本方法。因此，查證程序涉及的範圍應視乎有關的信託安排的性質及複雜程度而定。

6. 倚賴中介人查證客戶身分

6.1 本節取代指引第 5.21 及 5.22 段。本節內容是關於向認可機構介紹客戶的中介人。但這不涵蓋外判或代理關係（即代理人按照合約代認可機構執行客戶查證程序），或金融機構（按照特別組織定義）之間的業務關係、代客戶處理的戶口或執行的交易。

6.1a 就本節而言，中介人被界定爲：

(i) 受金管局、證監會或保監處監管的金融機構；
(ii) 在香港專業或合法註冊爲律師、審計師、會計師、信託公司或特許秘書，並在香港以這些身分進行業務的人士；
(iii) 在對等標準地區經營業務的人士而該人：
  (A) 爲金融機構、律師、公證人、審計師、會計師、稅務顧問、信託公司或特許秘書；
  (B) 須按法律認可的方式辦理強制性專業註冊、申領牌照或接受規管；
  (C) 須遵守符合特別組織標準的規定；以及
  (D) 須就是否符合該等規定接受監察。

6.2 認可機構可倚賴中介人進行客戶查證程序。然而，認可機構仍然負有認識客戶的最終責任。

6.3 認可機構應評估其所倚賴的中介人是否爲「適當人選」，以及該等中介人所採用的客戶查證程序是否足夠。就此而言，認可機構應根據以下準則判斷某位中介人是否可予倚賴[備註 28]：

(a) 中介人的客戶查證程序應如認可機構自行查證有關客戶的程序一樣嚴謹；

(b) 認可機構必須信納中介人核實客戶身分的制度的可靠性；及

(c) 認可機構必須與中介人達成協議，准許認可機構在任何時期也可核實該中介人所進行的查證程序。

6.4 已廢除。

6.5 認可機構應定期進行檢討，確保其所倚賴的中介人繼續符合上文所列準則。此舉可包括檢討中介人的有關政策與程序，以及抽查所進行的查證個案。

6.6 認可機構應取得由中介人妥爲簽署的業務中介人證明書（見附件）及所有有關客戶身分證明的資料及其他文件[備註 29]。相關文件應爲文件正本，或經適合的證明人予以證明的副本（最好是前者）。

6.7 取得相關文件的目的，是要確保認可機構或金管局及情報組等有關當局可即時查閱，以及能持續監察有關客戶。此外，認可機構亦可

藉此核實中介人有否妥善進行其工作。但此舉的目的並不是要認可機構利用相關文件重複中介人所進行的查證程序。

非直接會面的文件核實

6.8 適合的證明人會證明其已查閱文件正本，而該文件的副本爲該正本的完整及真確副本。證明人應在文件副本首頁簽署及蓋上正式印章，並註明頁數。適合的證明人可爲中介人本身或：

(a) 發出身分證明文件的國家的大使館、領使館或高級專員公署；

(b) 特別組織成員國／地區或對等標準地區的法官、高級政府官員或現任警察或海關人員；

(c) 特別組織成員國／地區或對等標準地區的律師、公證人、精算師、會計師或特許秘書；或

(d) 在特別組織成員國／地區或對等標準地區註冊成立或經營的受監管金融機構的董事、高級職員或經理。

7. 客戶戶口

7.1 本節取代指引第 5.23 段。本節內容是關於以專業中介人[備註 30]或專業中介人作爲代理人管理的單位信託、互惠基金或任何其他投資計劃（包括員工的公積金及退休計劃）的名義開設的戶口。

7.2 若客戶戶口是代表單一客戶開設，或每名個別客戶都開有一個附屬戶口，資金並沒有匯集在一個戶口內，則認可機構除了核實開設戶口的中介人的身分外，亦應識別相關客戶的身分。

7.3 若個別客戶的資金匯集在一個客戶戶口內[備註 31]，則認可機構當然無需查證個別客戶的身分，但須符合以下條件（請同時參考上文第 6.1a 段）：

(a) 認可機構信納該中介人備有可靠的制度以核實客戶身分；及

(b) 認可機構信納中介人備有妥善的制度及管控措施，把匯集戶口內的資金分配予個別相關客戶。

7.4 若中介人未能符合上述條件，而且以專業保密守則等理由拒絕提供相關客戶身分的資料，則認可機構不應批准該中介人開設客戶戶口。

7.5 若經客戶戶口進行的交易引起認可機構關注或懷疑，認可機構應作出合理查詢或舉報。

8. 非直接會面客戶

8.1 本節取代指引第 5.24 及 5.25 段。

8.2 作爲客戶查證程序的一部分，認可機構應盡可能直接與新客戶會面，以查明新客戶的身分及背景資料。認可機構可親自與新客戶會面，或由可倚賴進行妥善客戶查證程序的中介人與新客戶會面（見上文第 6 節）。

8.3 如客戶屬於高風險類別，直接會面尤爲重要。認可機構應要求有關的高風險客戶親自出席會面。

8.4 認可機構若未能與客戶直接會面（例如因爲客戶透過互聯網開戶），認可機構應進行適用於直接會面客戶的同樣有效的客戶身分查證程序及持續監察標準。

8.5 認可機構可用以減輕與非直接會面客戶相關的風險的具體方法舉例如下：

(a) 由適合的證明人（見上文第 6.8 段）提供的身分證明文件；

(b) 要求提供較直接會面客戶所需爲多的文件以作補充；

(c) 完成需要提供廣泛類別而又可以獨立核實（例如由政府部門確認）的資料的網上開戶申請問卷調查；

(d) 認可機構親自接觸客戶；

(e) 由符合上文第 6.1a 及 6.3 段所列準則的中介人進行第三方介紹；

(f) 要求從帳戶作出的第一次付款是經由以該客戶名義在另一家認可機構或與認可機構奉行類同客戶查證標準的境外銀行開設的戶口進行；

(g) 更頻密地更新非直接會面客戶的資料；及

(h) 在非常的情況下，認可機構可拒絕與沒有直接會面的高風險客戶建立業務關係。

9. 電匯信息

9.1 本節取代指引第 6.1 至 6.3 段。本節的規定是根據特別組織提出的打擊恐怖分子籌資活動特別建議（見第 15.3 段）中有關電匯的建議及相關的闡釋備註而作出的。

9.2 若電匯金額達 8,000 港元或以上（或等值外幣），付款認可機構必須確保該電匯隨附下述資料：匯款人的姓名／名稱及戶口號碼（若沒有戶口號碼，則爲獨有的參考號碼），以及(i)地址[備註 32a]；或(ii)國民身分證號碼[備註 32bb]；或(iii)出生日期及地點。認可機構應確保隨附的資料經過核實[備註 32b]。

9.3 如電匯金額不足 8,000 港元或等值外幣[備註 32c]，付款認可機構可選擇不在隨附的電匯信息中載有以上所有資料。然而，無論如何（以及即使有指引第 5.27 段的規定[備註 33]）付款認可機構都應記錄及保留匯款人的有關資料，並且必須在收款金融機構或有關當局提出要求後 3 個營業日內提供有關資料。

9.4 付款認可機構應採取風險爲本方法，以查核在考慮到收款人姓名／名稱、收款地點及電匯金額等因素後，某些電匯交易是否可疑。

9.5 尤其若付款認可機構懷疑客戶是代表第三方進行電匯交易，便應特別謹慎。若電匯付款人是屬於第三方的姓名／名稱，或電匯似乎與該客戶的慣常業務／活動不符，付款認可機構便應要求客戶就電匯的性質作進一步解釋。

9.6 認可機構若在連串電匯中作中介人，應確保電匯信息在所有連串付款中都載有第 9.2 段所述的資料。

9.7 若認可機構爲收款人處理匯入款項，應特別留意及監察並未列明匯款人完整資料的電匯信息。認可機構可以透過風險爲本方法進行有關的監察，並要考慮到可疑的因素（例如電匯來自哪個國家）。如有需要，認可機構可以在進行有關交易（特別是經直接通遞程序處理的項目）後進行監察。

9.8 收款認可機構應考慮是否應向情報組舉報不尋常電匯交易。此外，收款認可機構亦可能要考慮限制或終止其與未能達到特別組織有關標準的匯款銀行的業務關係。

10. 政界人士

10.1 本節是新的部分，指引目前並未載有有關規定。

10.2 認可機構若與擔任重要公職的個人及明顯與該些個人有關連的人士或公司（即家人、有密切聯繫人士等）建立業務關係，認可機構便會面對特別重大的信譽或法律風險。認可機構應加強對該等政界人士的查證程序。雖然這點對私人銀行業務尤爲重要，但認可機構應在所有業務範圍內均對政界人士採用同等嚴格的查證程序。

10.3 政界人士是指現時或曾經爲主要公職人員的個人，例如國家或政府首長、資深政客、高級官員、司法人員或軍官、公營機構的高級人員及政黨的要員。需要關注的是，特別是在一些貪污相當普遍的國

家，這些政界人士可能會濫用職權，透過收受賄賂等非法途徑斂財。

10.4 認可機構應制定適當制度及管控措施，盡可能確定準客戶、客戶，或準客戶或直接客戶的關連人士[備註 34a]是否政界人士。例如，認可機構可在建立業務關係前，或代非戶口持有人執行相當於120,000 港元或以上的一次過交易前，利用公開資料或商用電子資料庫篩查該客戶及關連人士的姓名，以確定該客戶及關連人士是否政界人士，並在其後定期進行篩查。

10.5 認可機構在與被確定爲政界人士的客戶或實益擁有人建立業務關係前，必須獲得高級管理層核准。若現有客戶或實益擁有人被確定爲政界人士，認可機構亦須盡快取得高級管理層核准。

10.5a 認可機構應採取合理措施查核被確定爲政界人士的客戶的財富及資金來源[備註 34b]，並確保在與其保持業務關係期間貫徹加強監察該客戶及其與認可機構進行的業務，其中包括定期（至少每年一次）查核該業務關係（及戶口活動）。

10.6 認可機構在處理與政界人士的業務關係（或可能建立的業務關係）時應考慮的風險因素包括：

(a) 政界人士擔任公職或曾受委履行公職的國家有否引起任何特別關注，並要考慮到有關人士的職位；

(b) 任何無法解釋來源的財富或收入（即有關政界人士所擁有的資產價值與其收入水平不相稱）；

(c) 預計會收到來自政府機構或國營企業的大額款項；

(d) 財富來源被描述爲就政府合約所賺取的佣金；

(e) 政界人士要求認可機構就交易作出任何形式的保密安排；及

(f) 以在政府擁有的銀行開設的戶口或政府戶口作爲某項交易中的資金來源。

11. 代理銀行

11.1 本節是新的部分，指引目前並未載有有關規定。

11.2 代理銀行業務指一家銀行（代理銀行）向另一家銀行（所代理的銀行）提供信貸、存款、收款、結算、支付或其他類似服務[備註 35]。

11.3 認可機構若提供代理銀行服務，應收集有關所代理的銀行的足夠資料，以便能充分了解其業務性質。無論認可機構會否向所代理的銀行提供信貸融資，都應進行基本的客戶查證程序。認可機構在建立新的代理銀行業務關係前應先獲得高級管理層的批准[備註 36]，並以記錄每家機構的有關責任。

11.4 所收集的資料[備註 37]應包括有關所代理的銀行的管理層、主要業務、所在地、就防止清洗黑錢活動所採取的措施[備註 38]、該行所在國家的銀行規管及監管制度，以及戶口的用途等方面的詳情。

11.5 一般來說，認可機構只有在信納一家境外銀行受到有關當局有效監管的情況下，才應與該銀行建立或繼續維持代理銀行關係。

11.6 認可機構尤其不應與一些在其註冊地區沒有經營銀行業務而又不附屬於任何受監管金融集團的銀行（即空殼銀行）建立或繼續維持代理銀行關係。

11.7 若認可機構與設於不符合打擊清洗黑錢活動國際標準的地區的銀行維持代理銀行關係，便需加倍留意。在這些情況下，認可機構一般需加強客戶查證程序，包括取得有關該等銀行的實益擁有權的詳細資料，以及有關其防止清洗黑錢活動的政策與程序的更詳盡資料。此外，認可機構亦應加強持續監察經由這些代理戶口所進行的活動的程序，例如編製交易報告並交由條例遵行主任檢討，以及嚴密監察可疑資金轉撥等。

11.8 若認可機構所代理的銀行容許客戶直接利用代理戶口自行處理交易（直接付款戶口），認可機構也應特別留意。因此認可機構應確定所代理的銀行的客戶是否可以使用代理銀行服務，若是可以，認可機構便應採取措施要求核實該等客戶的身分。在這些情況下，認可機構應採用第 6 節所列載的程序。

11.9 認可機構應採取合理措施，確保不會與已知有准許空殼銀行使用其戶口的銀行建立或繼續維持代理銀行關係。

12. 現有戶口

12.1 本節取代指引第 5.3 段。

12.2 認可機構應採取措施確保現有客戶的記錄載有最新及相關的資料。如有需要，認可機構應取得現有客戶的額外身分證明文件，以確保對客戶的了解符合其現行標準。

12.3 爲達到這個目的，認可機構應定期檢討客戶的現有記錄。若遇有某些觸發事件時，便是認可機構採取上述行動的適當時機。這些事件包括：

(a) 即將進行一項重大[備註 39]交易；

(b) 戶口的操作模式出現重大轉變；

(c) 認可機構對客戶的文件標準作出頗大的修訂；或

(d) 認可機構知悉其缺乏足夠客戶資料。

12.4 爲免造成疑問，即使無出現觸發事件，認可機構仍應至少每年查核[備註 39a]所有高風險客戶一次，以確保客戶記錄常保更新及準確。這些查核每隔多少時間進行，應清楚載於認可機構的政策及程序內。

13. 持續監察

13.1 本節所述內容並未在指引內具體列載，但應與指引第 8 及 9 節一併閱讀。

13.2 認可機構必須備有制度以識別及舉報可疑交易，以履行其在法定及規管方面的責任。然而，單單倚賴前線職員作出特別報告並不足夠。認可機構亦應備有管理資訊系統，定期向經理及條例遵行主任提供適時的資料，以便他們能察覺特別是與高風險戶口有關的不尋常或可疑活動的模式。

13.3 爲達到以上目的，認可機構亦要對特定類別客戶的正常及合理活動（考慮到客戶的業務性質）有充分認識。此外，認可機構應採取適當措施，使其能信納存入客戶戶口資金的來源及合法性。在涉及大額款項及／或高風險客戶時，這一點尤其重要。

13.4 在涉及來自香港境外的資金時，認可機構還需注意轉撥該等資金有否違反有關國家的外匯管制規例。

13.5 用作進行持續監管的管理資訊系統報告應能識別在款額（例如參照有關客戶的預先設定限額或類似客戶的比較數字）或交易類別方面屬於不尋常的交易或其他相關風險因素。例如，相對於戶口的結餘，戶口的交易活動屬偏高或戶口的不尋常活動(例如以現金提早償還分期貸款)可能意味着資金正經由該戶口進行「清洗」，應做進一步調查。認可機構應對管理資訊系統報告中所鑒別出的任何不尋常活動作出跟進。有關的結果及跟進行動應適當地以書面記錄，而有關文件須保存不少於由有關不尋常活動被發現後六年。

13.6 對現金交易特別留意固然重要，但不應只限於此。認可機構不應忽略非現金交易，例如戶口間的轉撥或銀行間的轉撥。因此上文提及的管理資訊系統報告不應單是涵蓋現金交易，還應包括其他形式的交易。目的是要對客戶的交易及與認可機構的整體關係有全面理解。就此而言，在可行情況下以及利用風險爲本方法，整體關係應包括客戶在認可機構境外業務單位所開設的戶口及與那些單位進行的交易。

14. 沒有執行或沒有充分執行特別組織建議的地區

14.1 本節是新的部分，指引目前並未載有有關規定。

14.2 已廢除。

14.3 已廢除。

14.4 認可機構應對沒有執行或沒有充分執行特別組織建議的地區採用特別組織經修訂的 40 項建議中的第 21 項：

「金融機構應特別留意與來自沒有執行或沒有充分執行特別組織建議的國家的人士（包括公司及金融機構）的業務關係及交易。若這些交易沒有明確的經濟或合法目的，金融機構便應盡可能查證有關的背景及目的，並把有關調查結果以書面記錄，及可隨時提供予主管當局以協助其進行調查。」

14.5 因此，對於來自沒有執行或沒有充分執行特別組織建議或會引致認可機構面對較高風險的地區的客戶（包括實益擁有人[備註 40]），認可機構應格外謹慎[備註 3 及 41]。除按照上文第 3.2(da)段所要求確定及記錄開設戶口或建立業務關係的商業理據外，認可機構還應能完全信納該等客戶的資金來源[備註 21]的合法性。

14.5a 用以決定某些地區是否沒有執行或沒有充分執行特別組織建議或會引致認可機構面對較高風險的因素包括：

(a) 該地區或其相當多數量的個人或實體是否受到例如由聯合國所實施的制裁，禁令或類似的措施。此外基於某些組織的地位或某些措施的性質，認可機構亦可能須要在某些情況下考慮一些由與聯合國相似但未被全球公認的組織所實施的制裁或措施；

(b) 該地區是否被一些可靠消息來源認定爲缺乏適當防止清洗黑錢及打擊恐怖分子籌資活動的法律或規例和其他措施；

(c) 該地區是否被一些可靠消息來源認定爲支持恐怖活動、向恐怖分子提供資金或有指定恐怖主義組織在其境內運作；及

(d) 該地區是否被一些可靠消息來源認定爲有嚴重程度的貪污或其他犯罪活動。

“可靠消息來源”是指由一些廣爲人知和有良好聲譽的組織所提供及被廣泛流傳的資訊。除特別組織及其區域性組織以外，這些來源可包括（但並不限於）超國家或國際組織例如國際貨幣基金組織，由不同的財富情報組所組成的埃格蒙特集團及有關的政府組織和非政府機構。由這些可靠消息來源提供的資訊並沒有相同於法律或規例的效用，亦不應被視爲決定風險較高的當然因素。

14.6 對於出現嚴重缺失而在改善其情況方面進展不足的地區，特別組織可能會建議採取進一步的針對措施。金管局會按個別情況決定具體的針對措施，這些措施會是漸進式的，並會因應有關地區的具體問題而定。這些措施一般會側重於更嚴格的客戶查證程序及加強監察／舉報交易。認可機構應按金管局不時作出的決定，對這些地區採取所訂定的針對措施。

14.7 認可機構應知悉在沒有執行或沒有充分執行特別組織建議的地區或已知在防止清洗黑錢及恐怖分子籌資活動方面標準較低的其他地區開展業務時潛在的信譽風險。

14.8 若在香港註冊的認可機構於該等地區設有業務單位，該認可機構便應特別謹慎，確保這些業務單位實施有效的防止清洗黑錢及恐怖分

子籌資活動的管控措施。認可機構尤其應確保這些境外業務單位採用等同香港的政策及程序。此外，香港總辦事處的職員亦應對境外業務單位進行條例遵行及內部審計查核。在非常的情況下，認可機構應考慮從該等地區撤離。

15. 恐怖分子籌資活動

15.1 本節是新的部分，指引目前並未載有有關規定。

15.2 恐怖分子籌資活動一般指進行涉及由恐怖分子擁有、曾經或計劃用作協助進行與恐怖活動有關的資金交易。這一點過去並未曾列入任何防止清洗黑錢活動體制內，因爲有關體制的重點是處理犯罪活動得益，即資金來源是關鍵元素。在恐怖分子籌資活動中，重點是資金的目的地或用途，而有關資金可能是從合法途徑得來的。

15.3 自「九一一」事件後，特別組織已把其工作範圍擴展至包括與恐怖分子籌資活動有關的事項，並就此制定了 9 項恐怖分子籌資活動特別建議。有關建議參見特別組織的網頁（***http://www.fatf-gafi.org***）。

15.4 聯合國安全理事會（安理會）已通過多項決議案，要求對某些被指定的恐怖分子及恐怖組織實施制裁。香港方面，根據《聯合國（制裁）條例》發出的規例，使這些由安理會作出的決議得以在本港生效。尤其是《聯合國制裁（阿富汗）規例》，其中規定禁止向被指定的恐怖分子提供資金。被指定的恐怖分子的名單會不時刊載於憲報。

15.5 此外，《聯合國（反恐怖主義措施）條例》已於 2002 年 7 月 12 日頒布。該條例把安理會第 1373 號決議案內的強制性內容付諸實行。這項決議案的目的是從不同方面打擊國際恐怖主義，其中包括推出措施打擊恐怖分子籌資活動。該條例亦落實特別組織的 9 項特別建議中最緊迫的部分。

15.6 該條例中亦規定禁止向恐怖分子或與恐怖分子有聯繫人士（按條例的定義）供應或提供資金。該條例亦規定，任何人士如知悉或懷疑任何財產爲恐怖分子的財產，均有法定責任作出舉報。與上文所述的規例一樣，被指定的恐怖分子的名單會爲此不時刊載於憲報。

15.7 認可機構應採取措施確保機構遵行有關打擊恐怖分子籌資活動的規例及法例。認可機構及其職員應充分了解其各自的法定責任，並應向職員提供足夠的指示與培訓。識別可疑交易的制度與機制應涵蓋恐怖分子籌資活動及清洗黑錢活動。

15.8 特別重要的一點是，認可機構應能識別及舉報與涉嫌恐怖分子有關的交易。爲此，認可機構應設立貯存有關涉嫌恐怖分子的姓名／名稱及詳細資料的資料庫，該資料庫應綜合其曾經獲悉的有關名單。認可機構亦可作出安排，確保能使用由第三方服務供應商提供的同類資料庫。

15.9 該等資料庫更應包括憲報公布的名單，以及美國總統在 2001 年 9 月 23 日發出的行政指令列出的指定名單。有關資料庫應不時更新，並應容易使用，以便認可機構的職員能識別可疑交易。

15.10 認可機構應根據資料庫所載名單查核現有客戶與新客戶的姓名／名稱。認可機構應特別留意可疑的電匯，並應謹記非牟利機構在恐怖

分子籌資活動中曾經扮演的角色。若出現引起認可機構懷疑的情況，便應盡可能在處理交易前加緊查核工作。

15.11 特別組織在 2002 年 4 月發出文件，就偵查恐怖分子籌資活動向金融機構提供指引。該文件說明了恐怖分子籌資活動的普遍特點，並列出個案研究，說明執法機關根據金融機構所舉報的資料確定恐怖分子籌資活動連繫的方法。該文件附件 1 載有過去曾與恐怖活動有關連的財務交易的多項特點。

15.12 認可機構應對該份特別組織文件有所了解，並將其作爲其員工培訓材料的一部分。該文件載於特別組織的網頁（***http://www.fatf-gafi.org***）。

15.13 有一點需要注意的是，該列有特點的文件只用作顯示若存在一項或以上所述特點，認可機構便可能需要進行額外監察的交易類型。認可機構亦應留意交易涉及的有關各方，特別是若有關個人或實體名列涉嫌恐怖分子名單上。

15.14 若認可機構懷疑某項交易與恐怖分子有關，應向情報組及金管局舉報。即使沒有證據證明交易直接與恐怖分子有關，但若交易因其他原因而顯得可疑，認可機構仍應向情報組舉報。此交易與恐怖分子的連繫可能會日後浮現出來。

16. 風險管理

16.1 本節應與指引第 9 節有關條例遵行主任的職責的部分一併閱讀。

16.2 認可機構的高級管理層應全力建立適當的防止清洗黑錢活動政策與程序，及確保其成效，並應在認可機構內分配有關的明確職責。

16.3 認可機構應委任條例遵行主任以作爲舉報可疑交易的中心點。條例遵行主任的職責不應單是被動地接收有關可疑交易的特別報告，而且要積極參與識別及舉報可疑交易的工作，包括定期檢討由認可機構的管理資訊系統編製有關大額或不尋常交易的特殊報告及前線職員提交的特別報告。根據認可機構的組織架構情況，檢討有關報告的具體工作也可交由其他指定職員負責，但條例遵行主任應監察整個檢討程序。

16.4 條例遵行主任應仔細考慮有關情況，然後就是否向情報組舉報不尋常或可疑交易作出決定。條例遵行主任向情報組舉報時，應確保其報告提供所有相關的詳細資料及就調查事宜充分與情報組合作。若決定不向情報組舉報看來是可疑的交易，條例遵行主任應詳細記錄有關的理由。即使曾就有關客戶過去的交易向情報組作出舉報，若出現新的可疑交易，認可機構仍應向情報組作出新的舉報。

16.5 一般來說，條例遵行主任應有責任持續查核認可機構備有的政策與程序，以確保遵守法定及監管規定，並測試有關的遵行情況。

16.6 因此，認可機構應確保條例遵行主任在機構內具有一定地位及備有足夠資源，以便能執行其職能。

16.7 內部審計在定期獨立評估認可機構的防止清洗黑錢活動政策與程序方面亦具有重要作用。這包括查證條例遵行主任的職能的成效、有關大額或可疑交易的管理資訊報告是否足夠及舉報可疑交易的質素。對前線職員在防止清洗黑錢活動方面的責任的警覺性亦應予以

檢討。與條例遵行主任的情況一樣，內部審計部門應具有足夠的專門知識及資源，以執行其職責。

香港金融管理局

2010 年 7 月

附件

業務中介人證明書

本人／本公司擬申請代表以下*人士／公司開戶：

客戶名稱

_____

地址_____

_____

1. 本人／本公司確認本人／本公司已查證客戶的身分及地址，並按照金管局的《防止清洗黑錢活動指引》（包括其補充文件及隨附的闡釋備註）的規定，隨附*載有身分證明資料的簡要附頁/以下身分證明文件(或該等文件的經證明副本)：

    (a) *客戶／公司的所有授權簽署人、董事（包括董事總經理在內，至少兩名董事）及所有主要股東的身分證／護照；
    (b) 董事局議決開戶及授權予有關人士操作帳戶的決議案；
    (c) 公司註冊證書；
    (d) 商業登記證；
    (e) 公司組織章程大綱及細則；
    (f) 公司註冊處查冊記錄；
    (g) 地址證明；
    (h) 其他有關文件。

2. 本人／本公司確認客戶的*職業／業務爲：

    _____

3. 本人／本公司信納用作開戶的資金的來源沒有問題。有關詳情如下：

_____

4. 本人／本公司隨附已填妥的開戶文件，並確認開戶文件上的簽署是客戶的簽名。

5. 本人／本公司隨附客戶授權本人／本公司代表客戶申請開戶及／或操作帳戶的證明文件。

*請將不適用者刪去。

簽署：_____

姓名：_____

職位：_____ 公司名稱：_____

日期：_____

闡釋備註

一般指引

特別組織的經修訂 40 項建議及巴塞爾委員會的仔細查證客戶身分的要求：特別組織及巴塞爾委員會的要求均適用於香港的銀行界。特別組織的要求列明適用於金融機構及非金融機構的基本架構，而巴塞爾委員會的要求（其中部分環節被認爲比特別組織的要求更爲嚴格）則具體地指向銀行的審慎監管，並且是針對銀行所承受的風險而定出。因此，基於銀行業務的性質，銀行業應採納更嚴格的仔細查證客戶身分（客戶查證）的標準。然而，鑑於推行措施時遇到的實際問題，以及要求中包含的元素並未全數得到充分發展，需要一段時間才能備妥（例如專業中介人的監管制度），因此在實施這些要求時，需要靈活變通。若清洗黑錢風險低，可採納特別組織的方法，並利用簡化的客戶查證程序。

風險爲本方法：認可機構應就高風險客戶採用更全面及詳盡的客戶查證程序。相反，認可機構可以就低風險客戶使用簡化的客戶查證程序。一般來說，認可機構在沒有清洗黑錢的疑點[1]，及下述情況下，可以對一名或一類客戶使用簡化的客戶查證程序[第 2.2 段]：

- 清洗黑錢風險[2]被評估爲低；或
- 有足夠關於客戶的公開資料。

首要原則：就遵行《防止清洗黑錢活動指引》及其補充文件而言，指導原則是認可機構應能充分證明它們已採取合理措施，以信納其客戶（包括實益擁有人）的真正身分。從第三方的角度來看，這些措施應客觀合

[1] 有些個案即使其固有風險可能低，但有關的情況仍會令人產生懷疑。
[2] 這是指某類客戶的內在或固有風險。

理。尤其，若認可機構信納任何事宜，便應能向金管局或任何其他有關當局證明其評估是合理的。這即是說，除其他事項外，認可機構需記錄其評估結果及有關的理由。

詞彙

「客戶」一詞指在認可機構開有戶口或與認可機構進行交易的人士（即直接客戶[3]），或由代理爲其持有戶口或進行交易的人士（即實益擁有人）。如屬跨境交易：

- 若本地辦事處與一名在其海外辦事處設有戶口的人士僅有推銷關係，則本地辦事處可被視爲中介人，而該名人士是其海外辦事處的「客戶」[4]；及
- 若本地辦事處爲一名戶口設於其海外辦事處的人士進行交易，則該名人士應被視爲本地辦事處及其海外辦事處的「客戶」[5]。

「實益擁有人」指最終擁有或控制一名客戶的個人及／或由代理爲其進行交易的人士。此外，這個用語亦包括對一名法人或一項法律安排行使最終有效控制的人士。

[3] 一般來說，這並不包括交易的第三方。例如在一宗電匯交易中，付款認可機構不會視受益人（與該認可機構沒有任何其他關係）爲其客戶。

[4] 海外辦事處將負責按集團的認識客戶政策及有關國家的監管規定對客戶進行客戶查證程序，並持續監察客戶。不過，海外辦事處可能會要求本地辦事處代其進行查證身分及持續監察客戶的程序。

[5] 若在同一銀行／集團基礎上是運用一套共同的並與特別組織標準一致的客戶查證標準，本地辦事處可倚賴海外辦事處作爲中介人進行客戶查證程序及持續監察。只要在本地辦事處提出要求時，海外辦事處可立即提供有關客戶身分的文件及其交易的記錄，本地辦事處可以不索取身分証明文件的副本及本地辦事處爲有關客戶執行的交易記錄，但最低限度必須取得客戶身分的資料(一些本地辦事處或可無限制地從集團的資料庫取得所有相關的客戶身分資料)。

具體指引

集團的客戶查證要求

1. 一般原則是整個銀行集團應在綜合基礎上運用一套共同的客戶查證標準。不過，集團公司可以對業務性質屬於低風險的某類客戶使用簡化的客戶查證程序。此外，使用簡化的客戶查證程序應有充分理據，並要妥善記錄及經高級管理層妥爲批准。集團政策亦應清楚列明這種風險爲本方法。若有合理理由未能應用集團標準，例如是因爲法律或監管原因，則應記錄有關的偏離集團標準的情況，並運用減低風險措施。[第 1.7 段]

客戶查證

2. 已廢除。

3. 認可機構面對來自沒有執行或沒有充分執行特別組織建議的地區的客戶時，應採取持平的態度，並要按常理作出判斷。雖然認可機構在處理這類個案時格外謹慎是很合理的，但並非要求認可機構拒絕與這類客戶有任何業務關係，或自動把這類客戶列爲高風險客戶，要進行更爲嚴謹的客戶查證程序。相反，認可機構應衡量有關個案的所有環節，評估清洗黑錢的風險是否比正常情況高。[第 2.3(a)及 14.5 段]

4. 若客戶來自其公民沒有任何正式身分證明文件的國家，認可機構應按常理作出判斷，決定可接納哪些獨有的身分證明文件作爲代替。[第 3.2(b)段]

5. 若爲香港永久性居民[6]，認可機構應憑其身分證核實其姓名、出生日期及身分證號碼。若爲非永久性居民，認可機構應透過查驗其旅行證件額外核實其國籍。

認可機構應憑非居民客戶的旅行證件核實其身分[備註 9b]。

認可機構在識別不能親身出現在香港的非居民人士時，應憑以下証件核實其身分：(i)有效旅行證件；(ii)載有該人照片的國民身分證；或(iii)載有該人照片的有效國民駕駛執照，而該執照是由有關國家主管機關發出，並在發出執照前已核實其身分。[第 3.3 段]

6. 本指引提及某人士的「地址」時，均指其住址（如有不同，則兼指其永久地址）。

認可機構應按常理處理未能提供地址證明的客戶（如學生及家庭主婦）。

除指引第 5.7 段建議的方法外（例如要求出示最近的公用事業或差餉單據），認可機構可利用其他適當方法，例如對私人銀行客戶進行家居探訪，以核實客戶的居住地址。[第 3.3 段]

7. 有關職業或僱主的資料是與客戶相關的資料，但並不構成核實客戶身分所必須的部分資料。[第 3.3 段]

8. 在下述情況下，可例外地容許向第三方進行支付：

- 沒有清洗黑錢的疑點；
- 清洗黑錢風險被評估爲低；

[6] 這些客戶擁有香港永久性居民身分證。香港永久性居民身分證註明持有人出生日期的位置下方有英文大寫字母「A」，背面則註明持有人擁有香港居留權。

- 交易經高級管理層批准，而高級管理層應考慮過客戶的業務性質後才批准交易；
- 收款人的姓名／名稱並非在涉嫌恐怖分子及政界人士等需要關注的名單上；及
- 核實程序應在建立業務關係當日起計 1 個月內完成。[第 3.6 段]

9. 一般來說，款項應退回予戶口持有人。認可機構可自行決定以哪種方法退回款項，但認可機構必須防範清洗黑錢的風險，因爲這是可將款項「轉變」的方法之一，例如把現金轉爲本票。因此，認可機構必須確保它們有合理理由相信可以在一段合理時間內妥善完成有關的客戶查證程序，才爲客戶開戶。[第 3.7 段]

9a. 爲非戶口持有人執行的交易可包括：電匯、貨幣兌換、購買本票或禮券。[第 3.10 段]

9b. 「旅行證件」指附有持證人照片的護照，或其他足以令入境事務主任或入境事務助理員信納持證人的身分、國籍，以及居籍或永久居留地的文件。就身分核實的目的而言，以下文件可被接納爲旅行證件：

- 澳門特別行政區永久性居民身分證；
- 《台灣居民來往大陸通行證》；
- 海員身分證（根據及按照《國際勞工公約》／1958年《海員身分證書公約》的規定簽發）；
- 《大陸居民來往台灣通行證》；
- 入境事務處處長簽發的澳門居民通行證；
- 《因公往來香港澳門特別行政區通行證》；
- 《往來港澳通行證》。[第 3.14、3.15 及 3.16 段]

公司客戶

10. 認可證券交易所是指在特別組織成員國／地區的證券交易所或在《證券及期貨條例》附表 1 中所界定的指明證券交易所，但不包括在沒有執行或沒有充分執行特別組織建議的地區的證券交易所（本段取代指引附件 2）。[第 4.2 段]

11. 若屬下述情況，可採取簡化的客戶查證程序：

(a) 國有企業及其附屬公司，其所屬地區的清洗黑錢風險被評估爲低，而認可機構對企業的擁有權又沒有懷疑；或

(b) 在認可證券交易所上市的公司及其附屬公司。

認可機構應識別及核實這些公司至少兩名戶口簽署人的身分，並可採用風險爲本方法來決定是否需要識別及核實更多戶口簽署人的身分。[第 4.2 段]

12. 已廢除。

13. 一名人士如有權控制一家公司 10%或以上的投票權，或對該等投票權行使控制權，應被視爲有關公司的主要股東。[第 4.5 段]

14. 對等標準地區是指（除特別組織成員國／地區以外）認可機構認爲有充分執行相等於特別組織防止清洗黑錢及打擊恐怖分子籌資活動標準的地區。

在決定某一個地區是否有充分執行特別組織的防止清洗黑錢及打擊恐怖分子籌資活動標準和符合對等標準地區的標準時，認可機構應：

(a) 對該地區的防止清洗黑錢及打擊恐怖分子籌資活動標準作出評估。此評估可根據認可機構對該地區的認識及經驗或市場情報

作出。一個地區的風險越高，認可機構便應在與來自該地區的客戶進行業務時採取更爲詳盡的查證措施；

(b) 留意由制訂標準機構例如特別組織或如國際貨幣基金組織的國際金融機構所作出的評估。除了由特別組織及其區域性組織所作出的相互評估以外，國際貨幣基金組織及世界銀行均在它們對個別國家或地區所進行的金融穩定評估中，就該國家或地區遵守特別組織的防止清洗黑錢及打擊恐怖分子籌資活動建議進行評估；及

(c) 就與它們的客戶有所聯繫的地區的清洗黑錢風險保持適當和持續的警惕及考慮在合理情況下可得到有關這些地區的防止清洗黑錢及打擊恐怖分子籌資活動的管控系統及措施的資料。[第 4.4 段]

15. 如屬由富有人士（即最終實益擁有人）擁有的離岸投資公司，而該人士以該等公司作爲訂約方，與認可機構建立私人銀行業務關係，則可就取得有關公司客戶的擁有權、董事及戶口簽署人的獨立證明文件的要求作出例外處理。這即是說，若該等投資公司的註冊成立地並沒有公司查冊或職權證明書（或等同文件），或未能提供有關其董事及主要股東的具體資料，而認可機構又確信：

- 它們知悉最終實益擁有人的身分；及
- 沒有清洗黑錢的疑點，

則認可機構可接受由最終實益擁有人或訂約方發出有關上述各方的身分及與上述各方的關係的自我聲明書。

容許例外處理的條件是已就最終實益擁有人進行全面及詳盡的客戶查證程序。一般來說，有關這類客戶的全面及詳盡的客戶查證程序應包括附件 2 列出的程序。

所作出的例外處理應經高級管理層批准，並予以妥善記錄。[第 4.5 段]

16. 若客戶在沒有公司查冊的國家註冊成立，認可機構可信賴香港的專業第三方（如律師、公證人、精算師、會計師及提供公司秘書服務的人士或機構）代表該客戶提供的文件，但認可機構所收集的其他資料必須沒有疑點，而有關的專業第三方亦能符合補充文件第 6.1a 及 6.3 段以及下文備註 28 列出的準則。[第 4.5 段]

17. 認可機構可採用風險爲本方法，決定應否核實與某法人或某法律安排有關的個人（即主要股東、董事、簽署人、財產授予人／資產提供者／創立人、保護人，或法律安排的已知受益人）的居住地址，但認可機構的政策必須清楚列明有關的風險爲本程序，豁免必須按照政策規定給予，就該等豁免所作出的決定須妥善記錄，以及該客戶涉及清洗黑錢的風險不高。認可機構不應因爲核實程序存在實際困難而給予豁免。明示式的信託本身不能構成業務關係或執行一次過的交易，而是信託的受託人會代有關信託成爲業務關係的一方或執行一次過的交易，所以受託人應被視爲客戶，因此認可機構必須核實直接客戶關係的受託人的地址。[第 4.5 段]

18. 已廢除。

19. 認可機構應記錄所有戶口簽署人的身分[備註 5]（此項責任不適用於認可機構以其職務身分行事的員工）。認可機構可採用風險爲本方法，決定應否核實這些資料（包括被指派代表公司客戶批准資金轉撥或其他電子銀行交易的用戶），但認可機構的政策必須清楚列明有關的風險爲本程序，豁免必須按照政策規定給予以及就該等豁免所作出的決定須妥善記錄。無論如何，認可機構應核實至少兩名戶口簽署人的身分。認可機構不應因爲核實程序存在實際困難而給予豁免。[第 4.5 段]

20. 如屬多層擁有權結構的公司客戶，認可機構只須識別擁有權架構中的每個層次，以充分了解有關的公司結構，但認可機構需要核實位於架構最頂層的個人（即並非中間擁有人）的身分。[第 4.6 段]

21. 除補充文件具體列明的客戶外，認可機構亦應採用風險爲本方法，以決定哪些類別的客戶的資金來源亦需確定。[第 4.7 及 14.5 段]

22. 若限制不記名股票的轉移存在着實際困難，認可機構應向公司客戶的每名實益擁有人（即持有全部股份的 5%或以上的人士）取得其持股比例的聲明。該等擁有人亦應每年再作出聲明，同時若出售、出讓或轉讓股份，須即時通知認可機構。[第 4.9 段]

信託及代名人戶口

23. 若信託是由屬於一家認可機構的附屬公司（或聯營公司）的信託公司管理，該認可機構可倚賴其信託附屬公司進行客戶查證程序，只要：

- 認可機構取得該信託附屬公司的書面保證，確認已取得、記錄及保留有關委託人的證明文件，並確信資金來源沒有問題；
- 信託附屬公司遵行與特別組織標準一致的認識你的客戶的集團政策（認識客戶政策）；及
- 認可機構提出要求時可立即提供有關文件而不會有任何延誤。[第 5.2 段]

24. 認可機構可採用風險爲本方法，決定是否需要核實保護人的身分[7]。[第 5.3 段]

[7] 「保護人」的身分是需要核實的相關資料，原因是在某些情況下，這些人士可以行使權力撤換現有受託人。

25. 如已就財產授予人／資產提供者進行適當的客戶查證程序，認可機構可接受受託人或其他訂約方的聲明，以確認與財產授予人／資產提供者的聯繫或關係。[第 5.3 段]

26. 認可機構應盡可能取得有關受益人身分的資料，不過有關受益人的概略說明（例如受益人爲 XYZ 先生的家人）亦可接受。[第 5.3 段]

27. 若認可機構並未曾核實受益人的身分，一旦認可機構知悉自信託戶口向受益人支付任何款項，或代表受益人由信託戶口付款，便應評估是否需要核實受益人的身分。認可機構在作出有關評估時，應採取風險爲本方法，考慮到涉及的金額及是否有任何清洗黑錢的疑點。若決定不進行核實，有關決定必須經高級管理層批准。[第 5.3 段]

倚賴中介人查證客戶身分

28. 認可機構應採取合理措施，以確信中介人備有足夠的客戶查證程序及系統，但可採取風險爲本方法以決定應採取哪些措施。就評估中介人的客戶查證標準而言，相關的因素包括按照特別組織要求中介人受監管的程度，以及有關地區要求中介人舉報可疑交易的法律規定。[第 6.3 段]

29. 若認可機構已採取適當措施，確保中介人一旦接到要求會立即向認可機構提供有關客戶身分的文件副本而不會有任何延誤，則認可機構可決定不立即取得該等文件。然而，所有相關的身分證明的資料卻必須取得 。[第 6.6 段]

客戶戶口

30. 專業中介人可包括律師、會計師、基金經理、託管人及受託人。[第 7.1 段]

31. 在某些類型業務中（例如託管、證券交易或基金管理），常常會有連串縱向聯繫的單一客戶戶口或分戶口，該等戶口最終聯繫至一個匯集客戶基金戶口。認可機構可視該等戶口爲匯集戶口，而第 7.3 段的規定適用於該等戶口。[第 7.3 段]

電匯信息

32a. 認可機構可在電匯信息內列出有關匯款客戶的“通訊地址”，但認可機構必須確保該地址已被核實。[第 9.2 段]

32b. 如屬本地電匯交易，匯款信息內無需列明有關匯款客戶的額外資料，但付款認可機構應能在收款認可機構及有關監管當局提出要求後 3 個營業日內提供該等資料。至於要獲取較早（即超過 6 個月）前進行的交易的資料，認可機構應在切實可行的情況下盡快提供該等資料。[第 9.2 段]

32bb. 國民身分證號碼指香港身分證號碼或旅行證件號碼。[第 9.2 段]

32c. 在考慮運用 8,000 港元的最低金額時，認可機構應顧及本身電匯業務的操作特性。金管局鼓勵認可機構盡可能在所有電匯交易的隨附信息中載有有關匯款人的資料。 [第 9.3 段]

33. 無論是否戶口持有人，有關的匯款客戶資料都應予以記錄及保留。[第 9.3 段]

政界人士

34. 已廢除。

34a. 直接客戶的有關連人士包括該客戶的實益擁有人及有權指揮該客戶的活動的任何人士。爲免造成疑問，「有關連人士」一詞包括董事、主要股東、實益擁有人、簽署人、受託人、財產授予人／資產提供者／創立人、保護人，以及法律安排的訂明受益人。[第 10.4 段]

34b. 認可機構亦應根據風險評估考慮是否適合採取相關措施，核實某政界人士的資金及財富來源。[第 10.5a 段]

代理銀行

35. 無論所代理的銀行本身是委託人或是代表其客戶，這都包括就證券交易或資金轉撥而建立的代理銀行關係。[第 11.2 段]

36. 只要有正式的授權及適當的文件，認可機構可採用風險爲本方法以決定機構內部就批准建立新的代理銀行關係所需要的適當級別。[第 11.3 段]

37. 認可機構可透過公開資料（例如公開網站及年報）取得所代理的銀行的認可資格及其他資料，包括其所屬國家的銀行規管及監管制度。[第 11.4 段]

38. 認可機構在評估位於海外國家的所代理的銀行在打擊清洗黑錢方面的行動時，應留意所代理的銀行是否獲准爲空殼銀行開戶或與空殼銀行進行交易。[第 11.4 段]

現有戶口

39. 「重大」不一定要與金額有關，可包括不尋常交易或與認可機構對客戶的認識不相符的交易。[第 12.3(a)段]

39a. 除非懷疑以往取得的證明的真實性，否則認可機構無須重新核實現有個人客戶或現有公司客戶的個人關連人士的身分或地址。[第 12.4 段]

沒有執行或沒有充分執行特別組織建議的地區

40. 若一位客戶有一位或以上來自沒有執行或沒有充分執行特別組織建議的地區的（主要）實益擁有人，一般的原則是若該實益擁有人對有關客戶具有主要影響力，認可機構應格外謹慎。[第 14.5 段]

41. 認可機構可視特別組織的成員國／地區爲有充分執行特別組織建議的地區。[第 14.5 段]

附件 1：已廢除。

附件 2：<u>對私人銀行客戶進行全面的客戶查證程序</u>

對私人銀行客戶進行全面的客戶查證程序一般包括以下範圍：

- **<u>客戶資料</u>**

(a) 除了有關客戶身分的基本資料外（見上文備註 5 及備註 6），認可機構亦就每位私人銀行客戶取得以下的客戶資料：

- 開戶的目的及理由；
- 業務或就業資料；
- 估計資產淨值；
- 財富來源；
- 家庭背景，例如配偶、父母（如財富是承繼得來）的資料；
- 資金來源（即就開戶而言爲可接受的款項來源以及過戶款項的方式）；
- 預計的戶口活動情況；及
- 推薦資料（例如介紹人以及何時與介紹人認識及與介紹人的關係有多久）或其他可證明客戶的信譽的資料來源。

上述有關私人銀行客戶的所有資料應妥善記錄在客戶檔案內。

- **<u>認識客戶的全球政策</u>**

(b) 爲方便處理由海外辦事處介紹的客戶，認可機構應訂有認識客戶的全球政策，以確保相同的客戶查證標準適用於集團的所有私人銀行客戶。

- **<u>接納客戶</u>**

(c) 一般而言，認可機構不會接納沒有介紹人的客戶。因此，街客必須至少有銀行的推薦，否則不會獲認可機構接納爲其客戶。

(d) 同時，除非在下文(h)段所列的探訪政策適用的比較少見的情況下，否則認可機構若未能與客戶直接會面，就不會爲客戶開設私人銀行戶口。

(e) 接納私人銀行客戶須經高級管理層批准。如屬高風險或敏感客戶[8]，可能需要高級管理層及條例遵行部或獨立的監控部門（如屬在香港經營的境外附屬公司或分行，則爲所屬銀行或總行）的額外批准。

- **<u>專責關係管理</u>**

[8] 私人銀行業務的敏感客戶包括：
- 政界人士；
- 從事賭博、夜總會、賭場、外匯公司、貨幣兌換商、藝術品買賣及寶石交易商等向來容易涉及清洗黑錢的行業的人士；
- 居住在或資金來自被識別爲對特別組織的建議採納不足或犯罪及貪污風險高的國家或地區的人士；及
- 認可機構認爲屬於敏感人士的任何其他人士。

(f) 每位私人銀行客戶是由一位指定的關係經理負責提供服務，該名經理有責任對客戶進行客戶查證及持續監察。

(g) 認可機構應確保關係經理有足夠時間及資源對私人銀行客戶進行加強的客戶查證程序及持續監察。

- **監察**

(h) 認可機構盡可能定期與私人銀行客戶直接會面。

(i) 認可機構應對每位私人銀行客戶定期進行客戶查證檢討。對屬高風險或敏感客戶，應每年或更頻密的進行該等檢討，更可能需要高級管理層參與檢討工作。然而，不活躍戶口應有不同的處理方法。這類戶口應在進行交易前立即進行客戶查證檢討。

(j) 認可機構應備有有效的監察系統（例如以資產規模、資產交投量、客戶敏感度或其他相關準則爲根據），以能及時發現任何不尋常或可疑交易。

Guidance Note on Prevention of Money Laundering and Terrorist Financing

October 2010

Office of the Commissioner of Insurance

CONTENTS

PART I OVERVIEW

1. INTRODUCTION

1.1 This Guidance Note aims to prevent criminal use of the insurance industry for the purposes of money laundering and terrorist financing. It presents the background information on money laundering and terrorist financing and summarizes the relevant legislations in Hong Kong. It also sets out the expectation of the Office of the Commissioner of Insurance ("OCI") of the internal policies and procedures of authorized insurers, reinsurers, insurance agents and insurance brokers carrying on or advising on long term business (hereinafter referred to as "insurance institutions") to guard against money laundering and terrorist financing.

1.2 This Guidance Note applies to all insurance institutions which are not financial institutions authorized by the Hong Kong Monetary Authority under the Banking Ordinance (Cap. 155) ("authorized financial institutions"). Insurance institutions that are authorized financial institutions are subject to the Hong Kong Monetary Authority's guidelines on prevention of money laundering ("the HKMA's guidelines"). However, to the extent that there are some insurance specific requirements and examples of suspicious transactions or money laundering cases in this Guidance Note which may not be shown in the HKMA's guidelines, the insurance institutions that are authorized financial institutions are required to have regard to paragraphs 2.2, 5, 6.1-6.3, 6.6.1-6.6.3, 6.7-6.8, 7.2.4 and 8.2.12 as well as Annexes 2, 3, 4 and 5 of this Guidance Note.

1.3 This Guidance Note does not have the force of law and should not be interpreted in any manner which would override the provisions of any applicable law or other regulatory requirements. However, failure to follow the requirements of this Guidance Note by insurance institutions may reflect adversely on the fitness and properness of their directors and controllers. Similarly, failure to follow the requirements of the HKMA's guidelines by the insurance institutions that are authorized financial institutions may reflect adversely on the fitness and properness of their directors and controllers. The OCI may take any appropriate interventionary actions empowered by the Insurance Companies Ordinance (Cap. 41) or other administrative sanctions if an insurance institution is found to be not in compliance with this Guidance Note.

1.4 The scope of this Guidance Note covers the activities of all insurance institutions to the extent that such activities are within the jurisdiction of Hong Kong. Where a Hong Kong incorporated insurance institution has branches or subsidiaries overseas, the requirements also apply to their overseas branches and subsidiaries. Where the local requirements differ

from these requirements, the overseas operations should apply the higher standard to the extent that the local laws permit. Where an overseas branch or subsidiary is unable to observe group standards, the OCI should be informed.

1.5 This Guidance Note will be regularly reviewed and revised in the light of developments in international standards on prevention of money laundering and terrorist financing.

2. BACKGROUND

2.1 What is money laundering and terrorist financing?

2.1.1 Money laundering is the processing of the illicit proceeds of crime to disguise their illegal origin. Once these proceeds are successfully laundered, the criminal is able to enjoy these monies without revealing their original illegitimate source.

2.1.2 Financing of terrorism can be defined as the wilful provision or collection, by any means, directly or indirectly, of funds with the intention that the funds should be used, or in the knowledge that they are to be used, to facilitate or carry out terrorist acts. Terrorism can be funded from legitimate income.

2.2 Vulnerabilities in insurance

2.2.1 The insurance industry is vulnerable to money laundering and terrorist financing. When a life insurance policy matures or is surrendered, funds become available to the policy holder or other beneficiaries. The beneficiary to the contract may be changed possibly against payment before maturity or surrender, in order that payments can be made by the insurer to a new beneficiary. A policy might be used as collateral to purchase other financial instruments. These investments in themselves may be merely one part of a sophisticated web of complex transactions with their origins elsewhere in the financial system.

2.2.2 Examples of the type of long term insurance contracts that are vulnerable as a vehicle for laundering money or financing terrorism are products such as:

(a) unit-linked or with profit single premium contracts;

(b) single premium life insurance policies that store cash value;

(c) fixed and variable annuities; and

(d) (second hand) endowment policies.

2.2.3 Money laundering and the financing of terrorism using reinsurance could occur either by establishing fictitious (re)insurance companies or reinsurance intermediaries, fronting arrangements and captives or by the misuse of normal reinsurance transactions. Examples include:

- the deliberate placement via the insurer of the proceeds of crime or terrorist funds with reinsurers in order to disguise the source of funds;

- the establishment of bogus reinsurers, which may be used to launder the proceeds of crime or to facilitate terrorist funding;

- the establishment of bogus insurers, which may be used to place the proceeds of crime or terrorist funds with legitimate reinsurers.

2.2.4 Insurance intermediaries are important for distribution, underwriting and claims settlement. They are often the direct link to the policy holder and therefore, intermediaries should play an important role in anti-money laundering and combating the financing of terrorism. The same principles that apply to insurers should generally apply to insurance intermediaries. The person who wants to launder money or finance terrorism may seek an insurance intermediary who is not aware of or does not conform to necessary procedures, or who fails to recognize or report information regarding possible cases of money laundering or financing of terrorism. The intermediaries themselves could have been set up to channel illegitimate funds to insurers.

2.3 Stages of money laundering

2.3.1 There are three common stages of money laundering during which numerous transactions may be made by the launderers that could alert an insurance institution to potential criminal activity:

(a) Placement – the physical disposal of cash proceeds derived from illegal activity;

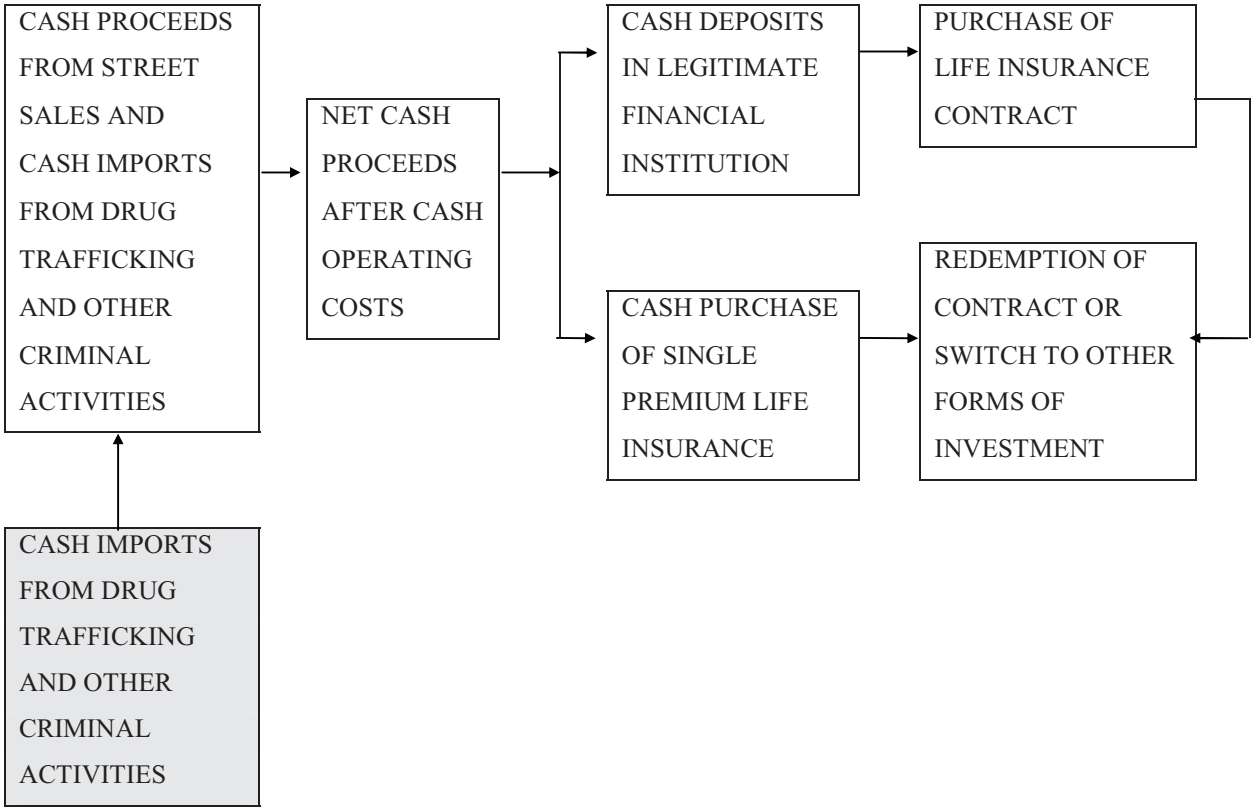
(b) Layering – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of money, subvert the audit trail and provide anonymity; and

(c) Integration – creating the impression of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way

that they re-enter the financial system appearing to be normal business funds.

2.3.2 The following chart illustrates the laundering stages in more detail.

LAUNDERING OF PROCEEDS



Domestic

Foreign

2.4 International initiatives

2.4.1 The Financial Action Task Force ("FATF") was established in 1989 in an effort to thwart attempts by criminals to launder the proceeds of criminal activities through the financial system. In November 1990, Hong Kong was invited to participate as an observer in FATF, and has, since December 1990, attended FATF meetings and played an active role in its deliberations. Hong Kong was admitted as a full member in March 1991.

2.4.2 The FATF has, among other things, put forward 40 Recommendations[1] which cover the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation against money laundering. The latest version of 40 Recommendations was released in June 2003. In October 2001, the FATF expanded its scope of work to cover matters relating to terrorist financing and promulgated Special Recommendations on Terrorist Financing[2] (further updated in October 2004). These two sets of Recommendations set out the international framework to detect, prevent and suppress money laundering and terrorist financing activities. As a member of the FATF, Hong Kong is obliged to follow the measures in the Recommendations.

2.4.3 To keep in line with the development of prevention of money laundering and terrorist financing standards in the financial sectors, the International Association of Insurance Supervisors ("IAIS") issued a Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism[3] in October 2004 which adapts the standards in the FATF Recommendations to the specific practices and features of the insurance business. The OCI's Guidance Note has taken into account the relevant measures in the FATF Recommendations and the IAIS Guidance Paper.

[1] The 40 Recommendations can be downloaded from FAFT website at ***http://www.fatf-gafi.org***

[2] The Special Recommendations on Terrorist Financing can be downloaded from FAFT website at ***http://www.fatf-gafi.org***

[3] The Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism can be downloaded from IAIS website at ***http://www.iaisweb.org***

3. LEGISLATION

3.1 The legislation concerning money laundering in Hong Kong

3.1.1 Legislation has been enacted in Hong Kong to address problems associated with the laundering of proceeds from drug trafficking and serious crimes. The Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) ("DTROP") provides for the tracing, freezing and confiscation of the proceeds of drug trafficking and creates a criminal offence of money laundering in relation to such proceeds. Under section 4 of DTROP, proceeds are not limited solely to the actual profits of drug sales or distribution, but may constitute any payments or other rewards received by a person at any time in connection with drug trafficking carried on by him or another, and property derived or realized therefrom.

3.1.2 The Organized and Serious Crimes Ordinance (Cap. 455) ("OSCO"), which was modelled on the DTROP, extends the money laundering offence to cover the proceeds of indictable offences in addition to drug trafficking.

3.1.3 The key money laundering provisions in the two Ordinances are summarized below. This does not constitute a legal interpretation of the provisions of the legislation referred to, for which appropriate legal advice should be sought where necessary.

3.1.4 Sections 3 to 5 of the OSCO provide that the Secretary for Justice or an authorized officer, for the purpose of investigating an organized crime, may apply to the Court of First Instance for an order to require a person to provide information or produce material that reasonably appears to be relevant to the investigation. The Court may make an order that the person makes available the material to an authorized officer. An authorized officer may also apply for a search warrant under the OSCO. A person cannot refuse to furnish information or produce material under sections 3 or 4 of the OSCO on the ground of self-incrimination or breach of an obligation to secrecy or other restriction on the disclosure of information imposed by statute or other rules or regulations.

3.1.5 Authorized officer includes any police officer, any member of the Customs and Excise Service established by section 3 of the Customs and Excise Service Ordinance (Cap. 342); or any officer in the Joint Financial Intelligence Unit ("JFIU") which

was established and is operated jointly by the Police and the Customs and Excise Department.

3.1.6 Section 25(1) of DTROP and OSCO create the offence of dealing with any property, knowing or having reasonable grounds to believe it in whole or in part directly or indirectly represents the proceeds of drug trafficking or of an indictable offence respectively. The offence carries a maximum sentence of 14 years' imprisonment and a maximum fine of HK$5 million.

3.1.7 It is a defence under section 25(2) of both Ordinances for a person to prove that he intended to disclose as soon as it is reasonable such knowledge, suspicion or matter to an authorized officer or has a reasonable excuse for his failure to make a disclosure in accordance with section 25A(2) of both Ordinances.

3.1.8 Section 25A(1) of both Ordinances impose a statutory duty on a person, who knows or suspects that any property in whole or in part directly or indirectly represents the proceeds of drug trafficking or of an indictable offence, or was or is intended to be used in that connection, to make a disclosure to an authorized officer as soon as it is reasonable for him to do so. Section 25A(7) of both Ordinances make it an offence for a person failing to make such disclosure. The offence carries a maximum penalty of a fine of HK$50,000 and imprisonment for 3 months.

3.1.9 It should be noted that section 25(4) of OSCO provides that references to an indictable offence in sections 25 and 25A of OSCO include a reference to conduct which would constitute an indictable offence if it had occurred in Hong Kong. That is to say it shall be an offence for a person to deal with the proceeds of crime or fail to make the necessary disclosure under section 25A(1) of OSCO even if the conduct is not committed in Hong Kong, provided that it would constitute an indictable offence if it had occurred in Hong Kong.

3.1.10 Section 25A(2) of both Ordinances provide that if a person who has made the necessary disclosures does any act in contravention of section 25(1) and the disclosure relates to that act, he does not commit an offence if:

(a) the disclosure is made before he does that act and the act is done with the consent of an authorized officer; or

(b) the disclosure is made after the person does the act and the disclosure is made on the person's own initiative and as soon as it is reasonable for him to make it.

3.1.11 Section 25A(3) of both Ordinances provide that disclosure made under section 25A(1) shall not be treated as breach of contract or of any enactment restricting disclosure of information and shall not render the person making the disclosure liable in damages for any loss arising out of disclosure. Therefore, insurance institutions need not fear breaching their duty of confidentiality owed to customers when making a disclosure under the two Ordinances.

3.1.12 Section 25A(4) of both Ordinances provide that a person who is in employment can make disclosure to the appropriate person in accordance with the procedures established by his employer for the making of such disclosure. To the employee, such disclosure has the effect of disclosing the knowledge or suspicion to an authorized officer as required under section 25A(1).

3.1.13 A "tipping-off" offence is created under section 25A(5) of both Ordinances, under which a person commits an offence if knowing or suspecting that a disclosure has been made, he discloses to any other person any matter which is likely to prejudice an investigation into money laundering activities. The "tipping-off" offence carries a maximum penalty of a fine of HK$500,000 and an imprisonment for 3 years.

3.1.14 Insurance institutions may receive restraint orders and charging orders on the property of a defendant of a drug trafficking offence or an offence specified in OSCO. These orders are issued under sections 10 and 11 of the DTROP or sections 15 and 16 of the OSCO. On service of these orders, an authorized officer may require a person to deliver as soon as practicable documents or information, in his possession or control which may assist the authorized officer to determine the value of the property. Failure to provide the documents or information is an offence under DTROP or OSCO. In addition, a person who knowingly deals in any realizable property in contravention of a restraint order or a charging order also commits an offence under DTROP or OSCO.

3.2 The legislation concerning terrorist financing in Hong Kong

3.2.1 The United Nations Security Council ("UNSC") has passed various resolutions to require sanctions against certain designated terrorists and terrorist organizations. In Hong Kong, regulations issued under the United Nations Sanctions Ordinance (Cap. 537) give effect to these UNSC resolutions. In particular, the United Nations Sanctions (Afghanistan) Regulation (Cap. 537K) and the United Nations Sanctions (Afghanistan) (Amendment) Regulation provide, among other things, for a prohibition on making funds available to designated terrorists. The list of designated terrorists is published in the Gazette from time to time.

3.2.2 In addition, the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) ("UNATMO") was enacted in July 2002 and was subsequently amended through the enactment of the United Nations (Anti-Terrorism Measures) (Amendment) Ordinance 2004 in July 2004[4]. The legislation implements the mandatory elements of the UNSC Resolution 1373. The latter aims at combating international terrorism on various fronts, including the introduction of measures against terrorist financing. The UNATMO also implements the most pressing elements of the FATF Special Recommendations.

3.2.3 The key terrorist financing provisions in the amended UNATMO are summarized below. This does not constitute a legal interpretation of the provisions of the legislation referred to, for which appropriate legal advice should be sought when necessary.

3.2.4 Section 7 of the amended UNATMO prohibits the supply or collection of funds to carry out terrorist acts, and section 8 of the amended UNATMO prohibits making funds (or financial) or related services available to terrorists or terrorist associates. Sections 6 and 13 of the amended UNATMO further permit terrorist property to be frozen and subsequently forfeited.

3.2.5 Section 12(1) of the amended UNATMO requires a person to report his knowledge or suspicion of terrorist property to an authorized officer (e.g. the JFIU). Failure to make a disclosure under this section constitutes an offence under section 14(5). The maximum penalty upon conviction of this offence is a fine of HK$50,000 and imprisonment for 3 months.

[4] A substantial part of this Amendment Ordinance has come into operation in January 2005.

3.2.6 The term "funds" includes funds mentioned in Schedule 1 to the amended UNATMO. It covers cash, cheques, claims on money, deposits with financial institutions or other entities, balances on accounts, securities and debt instruments (including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures, debenture stock and derivatives contracts), interest, dividends or other income on or value accruing from or generated by property, letters of credit, documents evidencing an interest in funds or financial resources, etc.

3.2.7 A list of terrorist or terrorist associate names is published in the Gazette from time to time pursuant to section 10 of the United Nations Sanctions (Afghanistan) Regulation and section 4 of the amended UNATMO. The published lists reflect designations made by the United Nations Committee that were established pursuant to UNSC Resolution 1267. The amended UNATMO provides that it shall be presumed, in the absence of evidence to the contrary, that a person specified in such a list is a terrorist or a terrorist associate (as the case may be).

3.2.8 Regarding the obligations under section 12(1) of the amended UNATMO to disclose knowledge or suspicion that property is terrorist property, section 12(2) of the amended UNATMO states that if a person who has made such a disclosure does any act in contravention of section 7 or 8 of the amended UNATMO either before or after such disclosure and the disclosure relates to that act, the person does not commit an offence if:

(a) the disclosure is made before he does that act and he does that act with the consent of the authorized officer; or

(b) the disclosure is made after he does that act, is made on his own initiative and is made as soon as it is practicable for him to make it.

3.2.9 Section 12(3) provides that a disclosure made under the amended UNATMO shall not be treated as a breach of any restriction upon the disclosure of information imposed by contract or by any enactment, rule of conduct or other provision. The person making the disclosure shall not be liable in damages for any loss arising out of the disclosure or any act done or omitted to be done in relation to the property concerned in consequence of the disclosure.

3.2.10 Section 12(4) of the amended UNATMO provides that a person who is in employment can make disclosure to the appropriate person in accordance with the procedures established by his employer for the making of such disclosure. To the employee, such disclosure has the effect of disclosing the knowledge or suspicion to an authorized officer as required under section 12(1).

3.2.11 Sections 12A, 12B and 12C of the amended UNATMO provide that the Secretary for Justice or an authorized officer, for the purpose of investigating an offence under the Ordinance, may apply to the Court of First Instance for an order to require a person to provide information or produce material that reasonably appears to be relevant to the investigation. The Court may make an order that the person makes available the material to an authorized officer. An authorized officer may also apply for a search warrant under the amended UNATMO. A person cannot refuse to furnish information or produce material under section 12A or 12B of the amended UNATMO on the ground of breaching an obligation to secrecy or other restriction on the disclosure of information imposed by statute or other rules or regulations.

4. POLICIES AND PROCEDURES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

4.1 The senior management of an insurance institution should be fully committed to establishing appropriate policies and procedures for the prevention of money laundering and terrorist financing and ensuring their effectiveness. The OCI expects that insurance institutions should have in place the following policies, procedures and controls:

(a) Insurance institutions should issue a clear statement of group policies in relation to money laundering and terrorist financing and communicate the group policies to all management and relevant staff whether in branches, departments or subsidiaries and be reviewed on a regular basis.

(b) Insurance institutions should develop instruction manuals setting out their procedures for:

- Customer acceptance
- Customer due diligence
- Record-keeping
- Recognition and reporting of suspicious transactions
- Staff screening and training

based on the guidance in Part II of this Guidance Note.

(c) Insurance institutions should comply with relevant legislations and seek actively to promote close co-operation with law enforcement authorities.

(d) Insurance institutions should instruct their internal audit/inspection departments to verify, on a regular basis, compliance with policies, procedures and controls against money laundering and terrorist financing activities.

(e) Insurance institutions should regularly review the policies and procedures on money laundering and terrorist financing to ensure their effectiveness.

(f) Whilst appreciating the sensitive nature of extra-territorial regulations, and recognizing that their overseas operations must be conducted in accordance with local laws and regulations, insurance institutions should ensure that their overseas branches and subsidiaries are aware of the group policies concerning money laundering and terrorist financing and, where appropriate, have been instructed to report to the local reporting point for their suspicions.

PART II DETAILED GUIDELINES

5. CUSTOMER ACCEPTANCE

5.1 Prior to the establishment of a business relationship, insurance institutions should assess the characteristics of the required product, the purpose and nature of the business relationship and any other relevant factors in order to create and maintain a risk profile of the customer relationship. Based on this assessment, the insurance institution should decide whether or not to accept the business relationship.

5.2 Insurance institutions should develop customer acceptance policies and procedures that aim to identify the types of customers[5] and/or beneficial owners[6] that are likely to pose a higher than average risk of money laundering and terrorist financing. There should be clear internal guidelines on which level of management is able to approve a business relationship with such customers and/or beneficial owners. Decisions taken on establishing relationships with higher risk customers and/or beneficial owners should be taken by senior management.

5.3 In assessing the risk profile of a customer relationship, an insurance institution should consider the following factors[7]:

(a) nature of the insurance policy, which is susceptible to money laundering risk, such as single premium policies;

(b) frequency and scale of activities;

(c) the customer's and/or beneficial owner's nationality, citizenship and resident status (in the case of a corporate customer, the customer's place of incorporation), the place where the customer's and/or beneficial owner's business is established, the location of the counterparties with whom the customer and/or beneficial owner conducts business, and whether the customer and/or beneficial owner is otherwise connected with higher risk jurisdictions or jurisdictions which do not or insufficiently apply the FATF Recommendations (paragraph 6.6.6), or which are known to the insurance institution to be lack of proper standards in the prevention of money laundering

[5] For the purpose of this Guidance Note, the term "customer" refers to policy holder.

[6] For the purpose of this Guidance Note, the term "beneficial owner" refers to the owner/controller of the policy holder, i.e. the natural person(s) who ultimately owns or controls a policy holder/potential policy holder or the person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

[7] These are relevant factors that insurance institutions should consider in assessing the risk profile of their customers and/or beneficial owners. They, however, do not form part of the customer due diligence procedures (unless explicitly mentioned in this Guidance Note).

or customer due diligence process;

(d) background or profile of the customer and/or beneficial owner, such as being, or linked to, a politically exposed person (paragraph 6.6.5);

(e) nature of the customer's and/or beneficial owner's business, which may be particularly susceptible to money laundering risk, such as money changers or casinos that handle large amounts of cash;

(f) for a corporate customer and/or beneficial owner, unduly complex structure of ownership for no good reason;

(g) means of payment as well as type of payment (cash, wire transfer, third party cheque without any apparent connection with the prospective customer and/or beneficial owner);

(h) the source of funds/wealth;

(i) the delivery mechanism, or distribution channel, used to sell the product (e.g. non face-to-face transactions (paragraph 6.6.4), business sold through insurance intermediaries (paragraph 6.8)); and

(j) any other information that may suggest that the customer and/or beneficial owner is of higher risk (e.g. knowledge that the customer and/or beneficial owner has been refused to enter a relationship by another financial institution).

5.4 Following the initial acceptance of the customer and/or beneficial owner, a pattern of account activity that does not fit in with the insurance institution's knowledge of the customer and/or beneficial owner may lead the insurance institution to reclassify the customer and/or beneficial owner as higher risk.

6. CUSTOMER DUE DILIGENCE

6.1 General principle

6.1.1 Insurance institutions should not keep anonymous accounts or accounts in obviously fictitious names. They should perform due diligence process for customers and/or beneficial owners and/or beneficiaries. The measures should comprise the following:

(a) identify the customer and/or beneficiary and verify the customer's and/or beneficiary's identity using reliable, independent source documents, data or information;

(b) ask and determine whether the customer is acting on behalf of another person for the purpose of identifying the insured and/or beneficial owner, and then take reasonable steps to obtain sufficient identification data to verify the identity of that other person, if applicable;

(c) identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner such that the insurance institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, insurance institutions should take reasonable measures to understand the ownership and control structure of the customer;

(d) obtain information on the purpose and intended nature of the business relationship between the customer and the insurance institution; and

(e) conduct on-going due diligence and scrutiny i.e. perform on-going scrutiny of the transactions and accounts throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the insurance institution's knowledge of the customers and/or beneficial owners, their businesses and risk profile, including, where necessary, identifying the source of funds.

6.1.2 Unwillingness of the customer, for no good reason, to provide the information requested and to cooperate with the insurance institution's customer due diligence process may itself be a factor that should trigger suspicion.

6.1.3 The general rule is that customers and/or beneficial owners and/or beneficiaries are subject to the full range of customer due diligence measures. Insurance institutions should however determine the extent of such measures on a risk based approach depending on the type of customer and/or beneficial owner and/or beneficiary, business relationship or transaction (factors for deciding the risk profile are set out in paragraph 5.3). Enhanced due diligence is called for with respect to higher risk categories. Conversely, it is acceptable for insurance institutions to apply simplified due diligence for lower risk categories as outlined in paragraphs 6.1.4, 6.3.2 and 6.3.4. Specific customer due diligence requirements applicable to different types of customers are outlined in paragraphs 6.2 to 6.7.

6.1.4 In general, insurance institutions may apply simplified due diligence in respect of a corporate customer where there is no suspicion of money laundering and terrorist financing, and:

- the risk of money laundering and terrorist financing is assessed to be low; or
- there is adequate public disclosure in relation to the customers; or
- there are adequate checks and controls exist elsewhere in national systems.

6.1.5 The guiding principle of applying the risk based approach is that the insurance institutions should be able to justify that they have taken reasonable steps to satisfy themselves as to the true identity of their customers and/or beneficial owners and/or beneficiaries. These measures should be objectively reasonable in the eyes of a third party. In particular, where an insurance institution is satisfied as to any matter it should be able to justify its assessment to the OCI or any other relevant authority. Among other things, this would require the insurance institution to document its assessment and the reasons for it.

6.1.6 If claims, commissions, and other monies are to be paid to persons or companies other than the customers or beneficiaries, then the proposed recipients of these monies should also be the subjects of identification and verification.

6.1.7 Insurance institutions should pay special attention to all complex, unusual large transactions and all unusual patterns of

transactions which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. In this respect, "transactions" should be interpreted in a broad sense, meaning inquiries and applications for an insurance policy, premium payments, requests for changes in benefits, beneficiaries, duration, etc.

6.1.8 As to reinsurance, due to the nature of the business and the lack of a contractual relationship between the policy holder and the reinsurer, it is often impractical for the reinsurer to carry out verification of the policy holder and/or the beneficial owner and/or the beneficiary. Therefore, for reinsurance business, reinsurers should only have business with ceding insurers that are authorized and supervised by the OCI or an equivalent authority in a jurisdiction that is a FATF member or that applies standards of prevention of money laundering and terrorist financing equivalent to those of the FATF.

6.1.9 In principle, identification and verification of customers and beneficial owners should take place when the business relationship with those persons is established. This means that the customers and beneficial owners need to be identified and their identity verified before, or at the moment when, the insurance contract is concluded.

6.1.10 Insurance institutions may permit the identification of beneficiary to take place after having established the business relationship, provided that the money laundering risks and financing of terrorism risks are effectively managed. Notwithstanding the above, the verification of the beneficiary should occur at the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

6.1.11 Where a customer and/or beneficial owner is permitted to utilize the business relationship prior to verification, insurance institutions should be required to adopt risk management procedures concerning the conditions under which this may occur. These procedures should include measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

6.1.12 Where the insurance institution is unable to satisfy itself on the identity of the customer and/or beneficial owner, it should not

commence business relationship or perform the transaction and should consider making a suspicious transaction report.

6.1.13 Where the insurance institution has already commenced the business relationship and is unable to satisfy itself on the identity of the customer and/or beneficial owner, it should consider terminating the business relationship, if possible, and making a suspicious transaction report. The return of premiums should be subject to any request from the JFIU to freeze the relevant premiums.

6.2 Individuals

6.2.1 Insurance institutions should institute effective procedures for obtaining satisfactory evidence of the identity of individual customers and/or beneficial owners and/or beneficiaries including obtaining information about:

(a) true name and/or name(s) used;
(b) identity card/passport number;
(c) current permanent address;
(d) date of birth;
(e) nationality[8]; and
(f) occupation/business[9].

6.2.2 Identification documents such as current valid passports or identity cards should be produced as identity proof. For Hong Kong residents, the prime source of identification will be the identity cards. File copies of identification documents should be retained.

6.2.3 In principle, copies of the identification documents of individual customers should be collected before, or at the moment when, the insurance contract is concluded. However, as far as an individual beneficiary is concerned, copy of his/her identification document should only be collected at the time of payout or the time when he/she intends to exercise vested rights under the policy.

6.2.4 Having considered the difficulty for insurance institutions to obtain copies of the identification documents of individual customers when the sales process occurs outside the office, insurance institutions may obtain and keep copies of the identification documents after having established the business

[8] For an individual who is a holder of Hong Kong Permanent Identity Card, the verification of nationality is not mandatory.

[9] Information about occupation/business is a relevant piece of information about a customer and/or beneficial owner and/or beneficiary but does not form part of the identification information requiring verification.

relationship provided that the money laundering risks and financing of terrorism risks are effectively managed. In all such circumstances, copies of identification documents of individual customers should be obtained and copied for retention as soon as possible after the insurance contract is concluded and, in any cases, no later than the time of payout or the time when the beneficiary intends to exercise vested rights under the policy. Paragraph 6.1.11 provides guidance for adopting the risk management procedures.

6.2.5 It must be appreciated that no form of identification can be fully guaranteed as genuine or representing correct identity. If there is doubt about whether an identification document is genuine, contact should be made with the Immigration Department or the relevant consulates in Hong Kong to ascertain whether the details on the document are correct.

6.2.6 Insurance institutions should check the address [10] of the applicant by appropriate means, e.g. by requesting sight of a recent utility or rates bill or a recent bank statement.

6.2.7 Insurance institutions should also identify the source of funds of customers and/or beneficial owners if the customers and/or beneficial owners are assessed to be of higher risk based on the factors set out in paragraph 5.3.

6.3 Corporations

6.3.1 The following documents or information should be obtained in respect of corporate customers and/or beneficial owners and/or beneficiaries which are registered in Hong Kong, not being financial institutions as mentioned in paragraph 6.3.4 (comparable documents, preferably certified by qualified persons such as lawyers or accountants in the country of registration, should be obtained for those customers and/or beneficial owners and/or beneficiaries which are not registered in Hong Kong, not being financial institutions as mentioned in paragraph 6.3.4):

(a) copies of certificate of incorporation and business registration certificate;

[10] Insurance institutions should, however, use a common sense approach to handle cases where the customers and/or beneficial owners (e.g. students and housewives) are unable to provide address proof. Apart from the method suggested in paragraph 6.2.5, insurance institutions may use other appropriate means, such as home visits, to verify the residential address of a customer and/or beneficial owner.

(b) copies of memorandum and articles of association (if insurance institution considers necessary having regard to the risk of the particular transaction);

(c) copy of resolution of the board of directors to enter into insurance contracts or other evidence conferring authority to those persons who will operate the insurance policy as well as the identification information of those persons;

(d) a search of the file at Companies Registry, if there is a suspicion about the legitimacy of the legal entity.

6.3.2 It will generally be sufficient for an insurance institution to adopt simplified due diligence in respect of a corporate customer and/or beneficial owner and/or beneficiary by obtaining the documents specified in paragraph 6.3.1 if the risk of money laundering and terrorist financing is assessed to be low. Some examples of lower risk corporate customers and/or beneficial owners and/or beneficiaries are:

(a) the company is listed in Hong Kong or on a recognized stock exchange (Annex 1) (or is a subsidiary of such listed company);

(b) the company is a state-owned enterprise in a jurisdiction where the risk of money laundering is assessed to be low and where the insurance institution has no doubt as regards the ownership of the enterprise;

(c) the company acquires an insurance policy for pension schemes which does not have surrender clause and the policy cannot be used as collateral; or

(d) the company acquires a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

6.3.3 Where a listed company is effectively controlled by an individual or a small group of individuals, an insurance institution should consider whether it is necessary to verify the identity of such individual(s).

6.3.4 Where a corporate customer and/or beneficial owner and/or beneficiary is a financial institution which is authorized and supervised by the OCI, HKMA, the Securities and Futures

Commission of Hong Kong or an equivalent authority in a jurisdiction that is a FATF member or that applies standards of prevention of money laundering and terrorist financing equivalent to those of the FATF, it will generally be sufficient for an insurance institution to verify that the institution is on the list of authorized (and supervised) financial institutions in the jurisdiction concerned. Evidence that any individual representing the institution has the necessary authority to do so should be sought and retained.

6.3.5 In relation to a corporate customer and/or beneficial owner and/or beneficiary which does not fall into the descriptions of paragraphs 6.3.2 and 6.3.4, an insurance institution should look behind the company to identify the beneficial owners and those who have control over the funds. This means that, in addition to obtaining the documents specified in paragraph 6.3.1, the insurance institution should verify the identity of all the principal shareholders (a person entitled to exercise or control the exercise of 10% or more of the voting rights of a company), at least two directors[11] (including the managing director) of the company and all authorized signatories designated to sign insurance contracts. The insurance institution should also identify the source of funds. Besides, a search of the file at Companies Registry should be performed.

6.3.6 Where a corporate customer which does not fall into the descriptions of paragraphs 6.3.2 and 6.3.4; and which is a non-listed company and has a number of layers of companies in its ownership structure, the insurance institution should follow the chain of ownership to the individuals who are the ultimate principal beneficial owners of the customer of the insurance institution and to verify the identity of these individuals. The insurance institution, however, is not required to check the details of each of the intermediate companies (including their directors) in the ownership chain.

6.3.7 An insurance institution should understand the ownership structure of non-listed corporate customers and determine the source of funds. An unduly complex ownership structure for no good reason is a risk factor to be taken into account (paragraph 5.3 (f)).

6.3.8 An insurance institution should exercise special care in initiating business transactions with companies that have

[11] In case of one-director companies, insurance institutions are only required to verify the identity of that director.

nominee shareholders. Satisfactory evidence of the identity of beneficial owners of such companies should be obtained.

6.3.9 An insurance institution should also exercise special care in dealing with companies which have a significant proportion of capital in the form of bearer shares. The insurance institution should have procedures to monitor the identity of all principal shareholders. This may require the insurance institution to consider whether to immobilize the shares, such as by holding the bearer shares in custody.

6.3.10 Where it is not practical to immobilize the bearer shares, insurance institutions should obtain a declaration from each owner (i.e. who holds 5% or more of the total shares) of the corporate customer on the percentage of shareholding. Such owners should also provide a further declaration on annual basis and notify the insurance institution immediately if the shares are sold, assigned or transferred.

6.4 Unincorporated businesses

6.4.1 In the case of partnerships and other unincorporated businesses whose partners are not known to the insurance institution, satisfactory evidence should be obtained of the identity of at least two partners and all authorized signatories designated to sign insurance contracts in line with the requirements for individual applicants in paragraph 6.2. In cases where a formal partnership arrangement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.

6.5 Trust accounts

6.5.1 Where trusts or similar arrangements are used, particular care should be taken in understanding the substance and form of the entity. Accordingly, insurance institutions should always establish, by confirmation from an applicant for insurance policy, whether the applicant is acting on behalf of another person as trustee, nominee or agent. Where the customer is a trust, the insurance institution should verify the identity of the trustees, any other person exercising effective control over the trust property, the settlors[12] and the beneficiaries[13]. Should it

[12] When the verification of the identity of the settlor is not possible, insurance institutions may accept a declaration from the trustee or other contractual party to confirm the link or relationship with the settlor.

[13] Insurance institutions should try as far as possible to obtain information about the identity of beneficiaries. A broad description of the beneficiaries such as family members of an individual may be accepted. Where the identity of beneficiaries has not previously been verified, insurance institutions should undertake

not be possible to verify the identity of the beneficiaries when the policy is taken out, verification of the beneficiaries should be carried out prior to any payments being made to them.

6.5.2 As with other types of customers, an insurance institution should adopt a risk based approach in relation to trusts and the persons connected with them. The extent of the due diligence process should therefore depend on factors such as the nature and complexity of the trust arrangement.

6.6 Higher risk customers

6.6.1 Insurance institutions should apply an enhanced due diligence in respect of higher risk customers and/or beneficial owners and/or beneficiaries. Some examples of higher risk customers and/or beneficial owners and/or beneficiaries are:

- customers and/or beneficial owners are assessed to be of higher risk based on the factors set out in paragraph 5.3;
- customers of non-face-to-face transactions;
- politically exposed persons as well as persons or companies clearly related to them; or
- customers and/or beneficial owners and/or beneficiaries in connection with jurisdictions which do not or insufficiently apply the FATF Recommendations.

6.6.2 Examples of additional measures applicable to enhanced due diligence are:

- obtaining senior management approval for establishing business relationship;
- obtaining comprehensive customer profile information e.g. purpose and reasons for entering the insurance contract, business or employment background, source of funds and wealth;
- assigning a designated staff to serve the customer who bears the responsibility for customer due diligence and on-

verification when they become aware that any payment out of the trust account is made to the beneficiaries or on their behalf. In making this assessment, insurance institutions should adopt a risk based approach which should take into account the amount(s) involved and any suspicion of money laundering or terrorist financing. A decision not to undertake verification should be approved by senior management.

going monitoring to identify any unusual or suspicious transactions on a timely basis;

- requisition of additional documents to complement those which are otherwise required; and

- certification by appropriate authorities and professionals of documents presented.

6.6.3 Apart from the above general additional measures, specific additional measures are also applicable to the customers of non-face-to-face transactions (paragraph 6.6.4); customers who are classified as politically exposed persons (paragraph 6.6.5); and customers in connection with jurisdictions which do not or insufficiently apply the FATF Recommendations (paragraph 6.6.6).

6.6.4 New or developing technologies: Customers of non-face-to-face transactions

6.6.4.1 An insurance institution should whenever possible conduct a face-to-face interview with a new customer to ascertain the latter's identity and background information, as part of the due diligence process. This can be performed either by the insurance institution itself or by an intermediary that can be relied upon to conduct proper customer due diligence (paragraph 6.8).

6.6.4.2 This is particularly important for higher risk customers. In this case, the insurance institution should ask the customer to make himself available for a face-to-face interview.

6.6.4.3 New or developing technologies that might favour anonymity can be used to market insurance products. E-commerce or sales through internet is an example. Where face-to-face interview is not conducted, for example where the account is opened via the internet, an insurance institution should apply equally effective customer identification procedures and on-going monitoring standards as for face-to-face customers.

6.6.4.4 Examples of specific measures that insurance institutions can use to mitigate the risk posed by such customers of non-face-to-face transactions include:

(a) certification of identity documents presented by suitable certifiers;

(b) requisition of additional documents to complement those required for face-to-face customers;

(c) completion of on-line questionnaires for new applications that require a wide range of information capable of independent verification (such as confirmation with a government department);

(d) independent contact with the customer by the insurance institution;

(e) third party introduction through an intermediary which satisfies the criteria in paragraph 6.8;

(f) requiring the payment for insurance premiums through an account in the customer's name with a bank;

(g) more frequent update of the information on customers of non-face-to-face transactions; or

(h) in the extreme, refusal of business relationship without face-to-face contact for higher risk customers.

6.6.5 Politically exposed persons ("PEPs")

6.6.5.1 PEPs are defined as individuals who are or have been entrusted with prominent public functions outside Hong Kong, such as heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and important political party officials. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories. The concern is that there is a possibility, especially in jurisdictions where corruption is widespread, that such PEPs may abuse their public powers for their own illicit enrichment through the receipt of bribes etc.

6.6.5.2 Business relationships with PEPs as well as persons or companies clearly related to them (i.e. families, close associates etc.) expose an insurance institution to

particularly significant reputation or legal risks. There should be on-going enhanced due diligence in respect of such PEPs and people and companies that are clearly related to them. The following CDD measures applicable to PEPs also apply to persons or companies that are clearly related to them.

6.6.5.3 An insurance institution should gather sufficient information from a new customer, and check publicly available information to establish whether or not the customer is a PEP. An insurance institution considering to establish a relationship with a person suspected to be a PEP should identify that person fully, as well as people and companies that are clearly related to him.

6.6.5.4 An insurance institution should also ascertain the source of funds before accepting a PEP as customer. The decision to establish business relationship with a PEP should be taken at a senior management level. Where a customer has been accepted and the customer and/or beneficial owner and/or beneficiary is subsequently found to be or become a PEP, an insurance institution should obtain senior management approval to continue the business relationship.

6.6.5.5 Risk factors that an insurance institution should consider in handling a business relationship (or potential relationship) with a PEP include:

(a) any particular concern over the jurisdiction where the PEP holds his public office or has been entrusted with his public functions, taking into account his position;

(b) any unexplained sources of wealth or income (i.e. value of assets owned not in line with the PEP's income level);

(c) unexpected receipts of large sums from governmental bodies or state-owned entities;

(d) source of wealth described as commission earned on government contracts;

(e) request by the PEP to associate any form of secrecy with a transaction; and

(f) use of accounts at a government-owned bank or of government accounts as the source of funds in a transaction.

6.6.5.6 Insurance institutions should determine and document their own criteria (including making reference to publicly available information or commercially available databases) to identify PEPs. A risk based approach may be adopted for identifying PEPs and focus may be put on persons from jurisdictions that are higher risk from a corruption point of view (reference can be made to publicly available information such as the Corruption Perceptions Index).

6.6.5.7 While paragraph 6.6.5.1 defines PEPs as individuals who hold prominent public functions outside Hong Kong, insurance institutions are encouraged to extend the relevant requirements on PEPs to individuals who hold prominent public functions in Hong Kong.

6.6.6 Jurisdictions which do not or insufficiently apply the FATF Recommendations

6.6.6.1 An insurance institution should apply Recommendation 21 of the FATF's revised Forty Recommendations to jurisdictions which do not or insufficiently apply the FATF Recommendations. This states that:

> "Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities."

6.6.6.2 Extra care should therefore be exercised by an insurance institution in respect of customers and/or beneficial owners and/or beneficiaries connected with jurisdictions which do not or insufficiently apply the FATF Recommendations or otherwise pose a higher risk to an insurance institution. In addition to ascertaining and documenting the business rationale for applying for insurance services as required under paragraph 6.1.1 (d)

above, an insurance institution should be fully satisfied with the legitimacy of the source of funds of such customers.

6.6.6.3 Factors that should be taken into account in determining whether jurisdictions do not or insufficiently apply the FATF Recommendations or otherwise pose a higher risk to an insurance institution include:

(a) whether the jurisdiction is, or a significant number of persons or entities in that jurisdiction are, subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN). In addition, in some circumstances, a jurisdiction subject to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized, may be given credence by an insurance institution because of the standing of the issuer and the nature of the measures;

(b) whether the jurisdiction is identified by credible sources as lacking appropriate anti-money laundering and counter-terrorist financing laws, regulations and other measures;

(c) whether the jurisdiction is identified by credible sources as providing funding or support for terrorist activities and has designated terrorist organizations operating within it; and

(d) whether the jurisdiction is identified by credible sources as having significant levels of corruption, or other criminal activity.

"Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supranational or international bodies such as the International Monetary Fund ("IMF"), and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-government organizations. The information provided by these credible sources does not have the effect of law or regulation and should

not be viewed as an automatic determination that something is of higher risk.

6.6.6.4 In assessing whether or not a jurisdiction (other than FATF members as shown in Annex 1) sufficiently applies FATF standards in combating money laundering and terrorist financing and meets the criteria for an equivalent jurisdiction, insurance institutions should:

(a) carry out their own jurisdiction assessment of the standards of prevention of money laundering and terrorist financing. This could be based on the insurance institutions' knowledge and experience of the jurisdiction concerned or from market intelligence. The higher the risk, the more stringent the due diligence measures that should be applied when undertaking business with a customer from the jurisdiction concerned; and

(b) pay particular attention to assessments that have been undertaken by standard setting bodies such as the FATF and by international financial institutions such as the IMF. In addition to the mutual evaluations carried out by the FATF and FATF-style regional bodies, as part of their financial stability assessments of countries and territories, the IMF and the World Bank have carried out country assessments in relation to compliance with prevention of money laundering and terrorist financing standards based on the FATF Recommendations.

(c) maintain an appropriate degree of on-going vigilance concerning money laundering risks and to take into account information that is reasonably available to them about the standards of anti-money laundering systems and controls that operate in the country with which any of their customers are associated.

6.6.6.5 For jurisdictions with serious deficiencies in applying the FATF Recommendations and where inadequate progress has been made to improve their position, the FATF may recommend the application of further counter-measures. The specific counter-measures, to be determined by the OCI in each case, would be gradual and proportionate to the specific problem of the

jurisdiction concerned. The measures will generally focus on more stringent customer due diligence and enhanced surveillance/reporting of transactions. An insurance institution should apply the counter-measures determined by the OCI from time to time.

6.6.6.6 An insurance institution should be aware of the potential reputation risk of conducting business in jurisdictions which do not or insufficiently apply the FATF Recommendations or other jurisdictions known to apply inferior standards for the prevention of money laundering and terrorist financing.

6.6.6.7 If an insurance institution incorporated in Hong Kong has operating units in such jurisdictions, care and on-going vigilance should be taken to ensure that effective controls on prevention of money laundering and terrorist financing are implemented in these units. In particular, the insurance institution should ensure that the policies and procedures adopted in such overseas units are equivalent to those adopted in Hong Kong. There should also be compliance and internal audit checks by staff from the head office in Hong Kong. In extreme cases the insurance institution should consider withdrawing from such jurisdictions.

6.7 On-going due diligence on existing customers and/or beneficial owners

6.7.1 Insurance institutions should take reasonable steps to ensure that the records of existing customers remain up-to-date and relevant. To achieve this, insurance institutions should perform on-going due diligence on the existing business relationship to consider re-classifying a customer as high or low risk. In general, the insurance institutions should pay attention to all requested changes to the policy and/or exercise of rights under the terms of the contract. They should assess if the change/transaction does not fit the profile of the customer and/or beneficial owner or is for some other reason unusual or suspicious. Enhanced due diligence is required with respect to higher risk categories. The customer due diligence programme should be established in such a way that insurance institutions are able to adequately gather and analyze information.

6.7.2 Examples of transactions or trigger events after establishment of the contract that require customer due diligence are:

(a) there is change in beneficiaries (for instance, to include non-family members, request for payments to persons other than beneficiaries);

(b) there is significant increase in the amount of sum insured or premium payment that appears unusual in the light of the income of the policy holder;

(c) there is use of cash and/or payment of large single premiums;

(d) there is payment/surrender by a wire transfer from/to foreign parties;

(e) there is payment by banking instruments which allow anonymity of the transaction;

(f) there is change of address and/or place of residence of the policy holder and/or beneficial owner;

(g) there are lump sum top-ups to an existing life insurance contract;

(h) there are lump sum contributions to personal pension contracts;

(i) there are requests for prepayment of benefits;

(j) there is use of the policy as collateral/security (for instance, unusual use of the policy as collateral unless it is clear that it is required for financing of a mortgage by a reputable financial institution);

(k) there is change of the type of benefit (for instance, change of type of payment from an annuity into a lump sum payment);

(l) there is early surrender of the policy or change of the duration (where this causes penalties or loss of tax relief);

(m) there is request for payment of benefits at the maturity date;

(n) the insurance institution is aware that it lacks sufficient information about the customer and/or beneficial owner; or

(o) there is a suspicion of money laundering and terrorist financing.

6.7.3 Occurrence of these transactions and events does not imply that (full) customer due diligence needs to be applied. If identification and verification have already been performed, the insurance institution is entitled to rely on this unless doubts arise about the veracity of that information it holds. As an example, doubts might arise if benefits from one insurance policy are used to fund the premium payments of the insurance policy of another unrelated person.

6.7.4 Even when there is no specific trigger event, an insurance institution should consider whether to require additional information in line with current standards from those existing customers and/or beneficial owners that are considered to be of higher risk. In doing so, the insurance institution should take into account the factors mentioned in paragraph 5.3.

6.8 Reliance on insurance intermediaries[14] for customer due diligence

6.8.1 Insurers, appointed insurance agents and authorized insurance brokers all have the responsibility to comply with the requirements relating to customer due diligence and record keeping as specified in paragraphs 6 and 7 of this Guidance Note. However, insurance intermediaries, that is agents and brokers, are usually the first line of contacts with the customer, before the customer is known, introduced or referred to an insurer. These insurance intermediaries may actually obtain the appropriate verification evidence in respect of the customer. To avoid duplication of efforts and unnecessary inconvenience to the customer, the insurer may rely on these insurance intermediaries to carry out part or all of the customer due diligence requirements.

6.8.2 For insurers which rely on insurance intermediaries to carry out part or all of the customer due diligence requirements, they must understand their related AML/CFT obligations in respect to these requirements. The ultimate responsibility for customer

[14] Insurance intermediaries refer to appointed insurance agents or authorized insurance brokers carrying on or advising on long term insurance business in Hong Kong.

identification and verification remains with the insurer relying on insurance intermediaries. The insurer concerned should therefore determine whether the intermediary in question possesses an acceptable level of reliability. In this regard, the following criteria should be used:

(a) the customer due diligence procedures of the insurance intermediary should be as rigorous as those which the insurer would have conducted itself for the customer and/or beneficial owner and/or beneficiary in accordance with paragraph 6 of this Guidance Note; and

(b) the insurer must satisfy itself as to the reliability of the systems put in place by the insurance intermediary to verify the identities of the customer and/or beneficial owner and/or beneficiary.

6.8.3 The insurer is expected to conduct periodic reviews to ensure that an insurance agent upon which it relies continues to conform to the criteria set out above. This may involve review of the relevant policies and procedures of the insurance agent and sample checks of the due diligence conducted.

6.8.4 Where reliance on insurance intermediaries for customer due diligence is permitted, the insurer should immediately obtain the necessary information concerning the relevant identification data and other documentation pertaining to the identity of the customer and/or beneficial owner and/or beneficiary from the insurance intermediary. The insurance intermediary should submit such information to the insurer upon request without delay.

6.8.5 The purpose of obtaining the underlying documentation is to ensure that it is immediately available on file for reference purposes by the insurer or relevant authorities such as the OCI and the JFIU, and for on-going monitoring of the customer and/or beneficial owner. It will also enable the insurer to verify that the insurance intermediary is doing its job properly. It is not the intention that the insurer should use the documentation, as a matter of course, to repeat the due diligence conducted by the insurance intermediary.

6.8.6 The insurer should undertake and complete its own verification of the customer and/or beneficial owner and/or beneficiary if it has any doubts about the ability of the insurance intermediary to undertake appropriate due diligence.

7. RECORD KEEPING

7.1 Requirements of the investigating authorities

7.1.1 The DTROP and the OSCO entitle the Court to examine all relevant past transactions to assess whether the defendant has benefited from drug trafficking or other indictable offences.

7.1.2 The investigating authorities need to ensure a satisfactory audit trail for suspected drug related or other laundered money and to be able to establish a financial profile of the suspected account.

7.1.3 An important objective of record keeping is to ensure that insurance institutions can, at all stages in a transaction, retrieve relevant information to the extent that it is available without undue delay.

7.2 Retention of records

7.2.1 Insurance institutions should keep records on the risk profile of each customer and/or beneficial owner and/or beneficiary and the data obtained through the customer due diligence process (e.g. name, address, the nature and date of the transaction, the type and amount of currency involved, and the type and identifying number of any account involved in the transaction), the copies of official identification documents (such as passports, identity cards or similar documents) and the account files and business correspondence, for at least six years after the end of the business relationship.

7.2.2 Insurance institutions should maintain, for at least six years after the business relationship has ended, all necessary records on transactions, both domestic and international, and be able to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amount and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

7.2.3 Insurance institutions should ensure that documents, data or information collected under the customer due diligence process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

7.2.4 Insurance institutions should ensure that they have in place adequate procedures:

(a) to provide initial proposal documentation including, where applicable, the customer financial assessment, analysis of needs, details of the payment method, illustration of benefits, and copy of documentation in support of verification by the insurance institutions;

(b) to retain all records associated with the maintenance of the contract post sale, up to and including maturity of the contract; and

(c) to provide details of the maturity processing and/or claim settlement which will include completed "discharge documentation".

7.2.5 Retention may be by way of original documents, stored on microfiche, or in computerized form provided that such forms are accepted as evidence under sections 20 to 22 of the Evidence Ordinance (Cap. 8). In situation where the records relate to on-going investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed.

8. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

8.1 Recognition of suspicious transactions

8.1.1 In order to satisfy an insurance institution's legal and regulatory obligations, it needs to have systems to enable it to identify and report suspicious transactions. In this regard, insurance institutions are encouraged to adopt the "SAFE" approach as recommended by the JFIU. Details of the "SAFE" approach are set out in Annex 2.

8.1.2 It is not enough to rely simply on the initiative of front-line staff to make ad hoc reports. An insurance institution should also have management information systems ("MIS") to provide managers and compliance officers with timely information on a regular basis to enable them to detect patterns of unusual or suspicious activity, particularly in relation to higher risk accounts.

8.1.3 This also requires the insurance institution to have a good understanding of what is normal and reasonable activity for particular types of customer and/or beneficial owner, taking into account the nature of its business. Among other things, an insurance institution should take appropriate measures to satisfy itself about the source and legitimacy of funds to be credited to a customer's and/or beneficial owner's account. This is particularly the case where large amounts are involved.

8.1.4 MIS reports used for monitoring purposes should be capable of identifying transactions that are unusual either in terms of amount (for example, by reference to predetermined limits for the customer in question or to comparative figures for similar customers) or type of transaction or other relevant risk factors.

8.1.5 To facilitate the identification of suspicious transactions, indicators of suspicious transactions are given in Annex 3 and examples of money laundering schemes involving life insurance industry are given in Annex 4. The indicators are not intended to be exhaustive and are for reference only. Identification of any of the types of transactions listed in Annex 3 should prompt further investigation and be a catalyst towards making at least initial enquiries about the source of funds.

8.1.6 In relation to terrorist financing, the FATF issued in April 2002 a Guidance for Financial Institutions in Detecting

Terrorist Financing[15]. The document describes the general characteristics of terrorist financing with case studies illustrating the manner in which law enforcement agencies were able to establish a terrorist financing link based on information reported by financial institutions. Annex 3 of the document contains a series of characteristics of financial transactions that have been linked to terrorist activity in the past. An insurance institution should acquaint itself with the FATF paper.

8.1.7 An insurance institution should maintain a database of names and particulars of terrorist suspects which consolidates the various lists that have been made known to it. Alternatively, an insurance institution may make arrangements to secure access to such a database maintained by third party service providers.

8.1.8 Such database should, in particular, include the lists published in the Gazette[16] under the relevant legislation and those designated under the US President's Executive Order 13224[17]. The database should also be subject to timely update whenever there are changes, and should be made easily accessible by staff for the purpose of identifying suspicious transactions.

8.1.9 An insurance institution should check the names of existing customers and/or beneficial owners and/or beneficiaries as well as new applicants for business against the names in the database. It should be particularly alert for suspicious remittances and should bear in mind the role which non-profit organizations are known to have played in terrorist financing. Enhanced checks should be conducted before processing a transaction, where possible, if there are circumstances giving rise to suspicion.

8.2 Reporting of suspicious transactions

8.2.1 The reception point for disclosures under the DTROP, the OSCO and the UNATMO is the JFIU, which is operated jointly by the Police and the Customs and Excise Department.

8.2.2 In addition to acting as the point for receipt of disclosures made by any organization or individual, the JFIU also acts as

[15] The Guidance for Financial Institutions in Detecting Terrorist Financing can be downloaded from FATF website at ***http://www.fatf-gafi.org/dataoecd/39/21/34033955.pdf***

[16] The Gazette can be downloaded from the website of the Government Logistics Department at ***http://www.gld.gov.hk/cgi-bin/gld/egazette/index.cgi?lang=e&agree=0***

[17] Lists designated under the US President's Executive Order 13224 can be downloaded from the United States Department of the Treasury website at ***http://www.ustreas.gov/offices/enforcement/ofac/programs/terror/terror.pdf***

domestic and international advisors on money laundering and terrorist financing generally and offers practical guidance and assistance to the financial sector on the subject of money laundering and terrorist financing.

8.2.3 The obligation to report is on the individual who becomes suspicious of a money laundering or a terrorist financing transaction. Each insurance institution should appoint a designated officer ("compliance officer") at the management level who should be responsible for reporting to the JFIU where necessary in accordance with the relevant legislation and to whom all internal reports should be made.

8.2.4 The role of the compliance officer should not be simply that of a passive recipient of ad hoc reports of suspicious transactions. Rather, the compliance officer should play an active role in the identification and reporting of suspicious transactions. This should involve regular review of exception reports of large or irregular transactions generated by the insurance institution's MIS as well as ad hoc reports made by front-line staff. Depending on the organization structure of the insurance institutions, the specific task of reviewing reports may be delegated to other staff but the compliance officer should maintain oversight of the review process.

8.2.5 Where an employee of an insurance institution becomes suspicious of a customer and/or beneficial owner and/or beneficiary, transaction or property, he must promptly report to the compliance officer.

8.2.6 The compliance officer should form a considered view on whether unusual or suspicious transactions should be promptly reported to the JFIU. In reporting to the JFIU, the compliance officer should ensure that all relevant details are provided in the report and cooperate fully with the JFIU for the purpose of investigation. If a decision is made not to report an apparently suspicious transaction to the JFIU, the reasons for this should be fully documented by the compliance officer. The fact that a report may already have been filed with the JFIU in relation to previous transactions of the customer and/or beneficial owner and/or beneficiary in question should not necessarily preclude the making of a fresh report if new suspicions are aroused.

8.2.7 The compliance officer should keep a register of all reports made to the JFIU and all reports made to him by employees. The compliance officer should provide employees with a written acknowledgement of reports made to him, which will

form part of the evidence that these reports were made in compliance with the internal procedures.

8.2.8 The compliance officer should have the responsibility for checking on an on-going basis that the insurance institution has policies and procedures to ensure compliance with legal and regulatory requirements and of testing such compliance.

8.2.9 It follows from this that the insurance institution should ensure that the compliance officer is of sufficient status within the organization, and has adequate resources, to enable him to perform his functions.

8.2.10 It is anticipated that an insurance agent or insurance broker who considers funds offered in settlement of a contract to be suspicious will share that suspicion with his insurer, in addition to reporting it directly to the JFIU. He could inform his insurer either at the time when the disclosure is made to the JFIU or when the documentation is passed to the insurer for processing.

8.2.11 Internal audit also has an important role to play in independently evaluating on a periodic basis an insurance institution's policies and procedures in combating money laundering and terrorist financing. This should include checking the effectiveness of the compliance officer function, the adequacy of MIS reports of large or irregular transactions and the quality of reporting of suspicious transactions. The level of awareness of front-line staff of their responsibilities in relation to the prevention of money laundering and terrorist financing should also be reviewed. As in the case of the compliance officer, the internal audit function should have sufficient expertise and resources to enable it to carry out its responsibilities. It is of importance that the auditor has direct access and reports directly to the management and the board of directors.

8.2.12 The use of a standard format for reporting (or adaptation of the format) is encouraged (Annex 5). In the event that urgent disclosure is required, an initial notification should be made by telephone. The contact details of the JFIU are at Annex 6.

8.2.13 The JFIU will acknowledge receipt of any disclosure made. If there is no imminent need for action e.g. the issue of a restraint order on an account, consent will usually be given for the institution to operate the account under the provisions of section 25A(2) of both the DTROP and the OSCO, or section 12(2) of

the UNATMO. An example of such a letter is shown at Annex 7 to this Guidance Note.

8.2.14 Insurance institutions should refrain from carrying out transactions which they know or suspect to be related to money laundering or terrorist financing until they have informed the JFIU which consents to the institutions carrying out the transactions. Where it is impossible to refrain or if this is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, institutions may carry out the transactions and notify the JFIU on their own initiative and as soon as it is reasonable for them to do so.

8.2.15 Access to the disclosed information is restricted to financial investigating officers within the Police and the Customs and Excise Department. In the event of a prosecution, production orders will be obtained to produce the material for the Court. Section 26 of the DTROP and the OSCO place strict restrictions on revealing the identity of the person making disclosure under section 25A.

8.2.16 Whilst there are no statutory requirements to provide feedback arising from investigations, the Police and the Customs and Excise Department recognize the importance of having effective feedback procedures in place. The JFIU may, on request, provide to a disclosing institution a status report on the disclosure.

8.2.17 Enhancing and maintaining the integrity of the relationship which has been established between law enforcement agencies and insurance institutions is considered to be of paramount importance.

9. STAFF SCREENING AND TRAINING

9.1 Screening

9.1.1 Insurance institutions should identify the key positions within their organizations with respect to anti-money laundering and combat of terrorist financing and should develop the following internal procedures for assessing whether employees taking up the key positions meet fit and proper requirements and are of high standards:

(a) verification of the identity of the person involved; and

(b) verification as to whether the information and references provided by the employee are correct and complete.

9.1.2 Insurance institutions should keep records on the identification data obtained from their employees mentioned in paragraph 9.1.1. The records should demonstrate the due diligence performed in relation to the fit and proper requirements.

9.2 Training

9.2.1 Staff must be aware of their own personal obligations under the DTROP, the OSCO and the UNATMO and that they can be personally liable for failing to report information to the authorities. They are advised to read the relevant sections of the DTROP, the OSCO and the UNATMO. They must be encouraged to co-operate fully with the law enforcement agencies and to provide prompt notice of suspicious transactions. They should be advised to report suspicious transactions to their institution's compliance officer if they do not know precisely what the underlying criminal activity is or whether illegal activities have occurred.

9.2.2 It is, therefore, imperative that insurance institutions introduce comprehensive measures to ensure that staff are fully aware of their responsibilities.

9.2.3 Timing and content of training packages for various sectors of staff will need to be adapted by individual insurance institutions for their own needs. However, it is recommended that the following might be appropriate:

(a) New employees

A general appreciation of the background to money laundering and terrorist financing, and the subsequent need for identifying and reporting of any suspicious transactions to the appropriate designated point, should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicions by the insurance institution, that there is a legal requirement to report, and that there is a personal statutory obligation in this respect.

(b) Sales/Advisory staff

Members of staff who are dealing directly with the public (whether as members of staff, agents or brokers) are the first point of contact with those who may commit money laundering or terrorist financing offence and the efforts of such staff are therefore vital to the strategy in the fight against money laundering and terrorist financing. They should be made aware of their legal responsibilities, including the insurance institution's reporting system for such transactions. Training should be provided on areas that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious. It is vital that "front-line" staff are made aware of the insurance institution's policy for dealing with non-regular customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

(c) Processing staff

Those members of staff who receive completed proposals and cheques for payment of the single premium contribution must receive appropriate training in the processing and verification procedures. The identification of the proposer and the matching against the cheque received in settlement are, for instance, key processes. Such staff should be aware that the offer of suspicious funds accompanying a request to undertake an insurance contract may need to be reported to the relevant authorities irrespective of whether or not the funds are accepted or the proposal proceeded with. Staff must know what procedures to follow.

(d) Management

A higher level of instruction covering all aspects of policies and procedures on prevention of money laundering and terrorist financing should be provided to those with the responsibility for supervising or managing staff and for auditing the system. The training will include their responsibility regarding the relevant policies and procedures, the offences and penalties arising from the DTROP, the OSCO and the UNATMO, internal reporting procedures and the requirements for verification and record keeping.

(e) Compliance officers

The compliance officers should receive in-depth training concerning all aspects of relevant legislation, guidances and policies and procedures on the prevention of money laundering and terrorist financing.

(f) On-going training

It will also be necessary to make arrangements for refresher training at regular intervals to ensure that staff do not forget their responsibilities. It is suggested that this might be best achieved by a twelve or six-monthly review of training or, alternatively, a review of the instructions for recognizing and reporting suspected money laundering or terrorist financing transactions.

RECOGNIZED STOCK EXCHANGE

Stock exchange of a country which is a member of FATF or a specified stock exchange as defined under the Securities and Futures Ordinance (Cap. 571) (but excluding exchanges in jurisdictions which do not or insufficiently apply the FATF Recommendations)

FATF members

Argentina
Australia
Austria
Belgium
Brazil
Canada
China
Denmark
Finland
France
Germany
Greece
Hong Kong, China
Iceland
India
Ireland
Italy
Japan
Luxembourg
Mexico
Kingdom of the Netherlands
New Zealand
Norway
Portugal
Republic of Korea
Russian Federation
Singapore
South Africa
Spain
Sweden
Switzerland
Turkey
United Kingdom
United States

Specified stock exchanges in non-FATF countries

Kuala Lumpur Stock Exchange
Stock Exchange of Thailand
Philippine Stock Exchange, Inc.

"SAFE" APPROACH RECOMMENDED BY THE JOINT FINANCIAL INTELLIGENCE UNIT

The "SAFE" Approach is an effective systemic approach to identify suspicious financial activity which involves the following four steps:

(a) Step one: **S**creen the account for suspicious indicators: Recognition of a suspicious activity indicator or indicators
(b) Step two: **A**sk the customer appropriate questions
(c) Step three: **F**ind out the customer's records: Review of information already known when deciding if the apparently suspicious activity is to be expected
(d) Step four: **E**valuate all the above information: Is the transaction suspicious?

Examination of the Suspicious Transactions Reporting ("STR") received by the JFIU reveals that many reporting institutions do not use the system outlined above. Commonly, institutions make a STR merely because a suspicious activity indicator has been recognized, i.e. only step one of the systemic approach is followed, steps two, three and four are not followed. This failure to use the systemic approach leads to a lower quality of STRs.

Each of the four steps of the systemic approach to suspicious activity identification is discussed in more detail in the following paragraphs. Insurance institutions should consider carefully the specific nature of their business, organizational structure, type of customer and transaction, etc. when designing their own systems for implementing the respective steps.

Step one: **S**creen the account for suspicious indicators: Recognition of a suspicious activity indicator or indicators

The recognition of an indicator, or better still indicators, of suspicious financial activity is the first step in the suspicious activity identification system. A list of suspicious activity indicators commonly seen within the insurance sector is shown at Annex 3.

Insurance institutions can use different methods in the recognition of suspicious activity indicators. The measures summarized below are recognized as contributing towards an effective overall approach to suspicious activity identification.

(a) Train and maintain awareness levels of all staff in suspicious activity identification.

This approach is most effective in situations in which staff have face-to-face contact with a customer who carries out a particular transaction which displays suspicious activity indicators. However,

this approach is much less effective in situations in which either, there is no face-to-face contact between customer and staff, or the customer deals with different staff to carry out a series of transactions which are not suspicious if considered individually.

(b) Identification of areas in which staff/customer face-to-face contact is lacking (e.g. sales through internet) and use of additional methods for suspicious activity identification in these areas.

(c) Use of a computer programme to identify accounts showing activity which fulfils predetermined criteria based on commonly seen money laundering methods.

(d) Insurance institutions' internal inspection system to include inspection of STR.

(e) Identification of "High Risk" customers, i.e. customers of the type which are commonly high risk in nature, e.g. PEP. Greater attention is paid to monitoring of the activity of these customers for suspicious transactions.

(f) Flagging of customers of special interest on the computer. Staff carrying out future transactions will notice the "flag" on their computer screens and pay extra attention to the transactions conducted by the customer. Customers to be flagged are those in respect of which a suspicious transaction report has been made and/or customers of high risk nature.

A problem with flagging is that staff who come across a large transaction involving a flagged customer may tend to make a report to the compliance officer whether or not the transaction is suspicious. This has the effect of overburdening compliance officers with low quality reports. Flagging may also lead to staff believing that if a customer is not flagged it is not suspicious. Staff must be educated on the proper usage of flagging if it is to work properly.

(g) Adopt more stringent policies in respect of customers who are expected to pay in large amount of cash or to purchase single premium policies, e.g. request customers for the expected nature of transactions and source of funds when establishing business relationship.

Step two: **A**sk the customer appropriate questions

If staff carry out a transaction or transactions for a customer bearing one or more suspicious activity indicators, they should question the customer on the reason for conducting the transaction(s) and the identity of the source

and ultimate beneficiary of the money being transacted. Staff should consider whether the customer's story amounts to a reasonable and legitimate explanation of the financial activity observed. If not, then the customer's activity should be regarded as suspicious and a suspicious transaction report should be made to the JFIU.

On occasions staff of insurance institutions may be reluctant to ask questions of the type mentioned above. Grounds for this reluctance are that the customer may realize that he, or she, is suspected of illegal activity, or regards such questions as none of the questioner's business. In either scenario the customer may be offended or become defensive and uncooperative, or even take his, or her, business elsewhere. This is a genuine concern but can be overcome by staff asking questions which are apparently in furtherance of promoting the services of the insurance institution or satisfying customer needs, but which will solicit replies to the questions above without putting the customer on his, or her, guard.

Appropriate questions to ask in order to obtain an explanation of the reason for conducting a transaction bearing suspicious activity indicators will depend upon the circumstances of the financial activity observed. For example, if a customer wishes to make a large cash transaction then staff can ask the customer the reason for using cash on the grounds that the staff may be able to offer advice on a more secure method to perform the transaction.

Persons engaged in legitimate business generally have no objection to, or hesitation in answering such questions. Persons involved in illegal activity are more likely to refuse to answer, give only a partial explanation or give an explanation which is unlikely to be true.

If a customer is unwilling, or refuses, to answer questions or gives replies which staff suspect are incorrect or untrue, this may be taken as a further indication of the suspicious nature of the financial activity.

Step three: **F**ind out the customer's records: Review of information already known when deciding if the apparently suspicious activity is to be expected

The third stage in the systemic approach to suspicious activity identification is to review the information already known to the insurance institution about the customer and his, or her, previous financial activity and consider this information to decide if the apparently suspicious activity is to be expected from the customer. This stage is commonly known as the "know your customer principle".

Insurance institutions hold various pieces of information on their customers which can be useful when considering if the customers'

financial activity is to be expected or is unusual. Examples of some of these information items and the conclusions which may be drawn from them are listed below:

(a) The customers' occupation. Certain occupations imply the customer is a low wage earner e.g. driver, hawker, waiter, student. The purchase of insurance policies with large transaction amounts from such customers would not therefore be expected.

(b) The customers' residential address. A residential address in low cost housing, e.g. public housing, may be indicative of a low wage earner.

Step four: **E**valuate all the above information: Is the transaction suspicious?

The final step in the suspicious activity identification system is the decision whether or not to make a STR. Due to the fact that suspicion is difficult to quantify, it is not possible to give exact guidelines on the circumstances in which a STR should, or should not, be made. However, such a decision will be of the highest quality when all the relevant circumstances are known to, and considered by, the decision maker, i.e. when all three of the preceding steps in the suspicious transaction identification system have been completed and are considered. If, having considered all the circumstances, staff find the activity genuinely suspicious then an STR should be made.

IMPORTANT NOTE

The above information is extracted from the relevant part of the website of the JFIU at ***http://www.jfiu.gov.hk/eng/suspicious_screen.html***. Insurance institutions are advised to regularly browse the website for latest information.

INDICATORS OF SUSPICIOUS TRANSACTIONS

1. A request by a customer to enter into an insurance contract(s) where the source of the funds is unclear or not consistent with the customer's apparent standing.

2. A sudden request for a significant purchase of a lump sum contract with an existing client whose current contracts are small and of regular payments only.

3. A proposal which has no discernible purpose and a reluctance to divulge a "need" for making the investment.

4. A proposal to purchase and settle by cash.

5. A proposal to purchase by utilizing a cheque drawn from an account other than the personal account of the proposer.

6. The prospective client who does not wish to know about investment performance but does enquire on the early cancellation/surrender of the particular contract.

7. A customer establishes a large insurance policy and within a short period of time cancels the policy, requests the return of the cash value payable to a third party.

8. Early termination of a product, especially in a loss.

9. A customer applies for an insurance policy relating to business outside the customer's normal pattern of business.

10. A customer requests for a purchase of insurance policy in an amount considered to be beyond his apparent need.

11. A customer attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments.

12. A customer refuses, or is unwilling, to provide explanation of financial activity, or provides explanation assessed to be untrue.

13. A customer is reluctant to provide normal information when applying for an insurance policy, provides minimal or fictitious information or, provides information that is difficult or expensive for the institution to verify.

14. Delay in the provision of information to enable verification to be completed.

15. Opening accounts with the customer's address outside the local service area.

16. Opening accounts with names similar to other established business entities.

17. Attempting to open or operating accounts under a false name.

18. Any transaction involving an undisclosed party.

19. A transfer of the benefit of a product to an apparently unrelated third party.

20. A change of the designated beneficiaries (especially if this can be achieved without knowledge or consent of the insurer and/or the right to payment could be transferred simply by signing an endorsement on the policy).

21. Substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policy holder.

22. The customer accepts very unfavourable conditions unrelated to his health or age.

23. An atypical incidence of pre-payment of insurance premiums.

24. Insurance premiums have been paid in one currency and requests for claims to be paid in another currency.

25. Activity is incommensurate with that expected from the customer considering the information already known about the customer and the customer's previous financial activity. (For individual customers, consider customer's age, occupation, residential address, general appearance, type and level of previous financial activity. For corporate customers, consider type and level of activity.)

26. Any unusual employment of an intermediary in the course of some usual transaction or formal activity e.g. payment of claims or high commission to an unusual intermediary.

27. A customer appears to have policies with several institutions.

28. A customer wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy.

29. The customer who is based in jurisdictions which do not or insufficiently apply the FATF Recommendations designated by the FATF from time to time or in countries where the production of drugs or drug trafficking may be prevalent.

30. The customer who is introduced by an overseas agent, affiliator or other company that is based in jurisdictions which do not or insufficiently apply the FATF Recommendations designated by the FATF from time to time or in countries where corruption or the production of drugs or drug trafficking may be prevalent.

31. A customer who is based in Hong Kong and is seeking a lump sum investment and offers to pay by a wire transaction or foreign currency.

32. Unexpected changes in employee characteristics, e.g. lavish lifestyle or avoiding taking holidays.

33. Unexpected change in employee or agent performance, e.g. the sales person selling products has a remarkable or unexpected increase in performance.

34. Consistently high activity levels of single premium business far in excess of any average company expectation.

35. The use of an address which is not the client's permanent address, e.g. utilization of the salesman's office or home address for the despatch of customer documentation.

IMPORTANT NOTE

The IAIS has published relevant examples and indicators involving insurance in a document called "Examples of money laundering and suspicious transactions involving insurance". The document can be downloaded from IAIS website at ***http://www.iaisweb.org/__temp/Examples_of_money_laundering.pdf***. The list will be updated periodically to include additional examples identified. Insurance institutions are advised to regularly browse the website for latest information.

EXAMPLES OF MONEY LAUNDERING SCHEMES[18]

LIFE INSURANCE

Case 1

In 1990, a British insurance sales agent was convicted of violating a money laundering statute. The insurance agent was involved in a money laundering scheme in which over US$1.5 million was initially placed with a bank in England. The "layering process" involved the purchase of single premium insurance policies. The insurance agent became a top producer at his insurance company and later won a company award for his sales efforts. This particular case involved the efforts of more than just a sales agent. The insurance agent's supervisor was also charged with violating the money laundering statute. This case has shown how money laundering, coupled with a corrupt employee, can expose an insurance company to negative publicity and possible criminal liability.

Case 2

A company director from Company W, Mr. H, set up a money laundering scheme involving two companies, each one established under two different legal systems. Both of the entities were to provide financial services and providing financial guarantees for which he would act as director. These companies wired the sum of US$1.1 million to the accounts of Mr. H in Country S. It is likely that the funds originated in some sort of criminal activity and had already been introduced in some way into the financial system. Mr. H also received transfers from Country C. Funds were transferred from one account to another (several types of accounts were involved, including both current and savings accounts). Through one of these transfers, the funds were transferred to Country U from a current account in order to make payments on life insurance policies. The investment in these policies was the main mechanism in the scheme for laundering the funds. The premiums paid for the life insurance policies in Country U amounted to some US$1.2 million and represented the last step in the laundering operation.

Case 3

Customs officials in Country X initiated an investigation which identified a narcotics trafficking organization utilized the insurance sector to launder proceeds. Investigative efforts by law enforcement agencies in several different countries

[18] Majority of the examples of money laundering schemes in this annex are extracted from the IAIS document "Examples of money laundering and suspicious transactions involving insurance". The document can be downloaded at ***http://www.iaisweb.org/__temp/Examples_of_money_laundering.pdf***.

identified narcotic traffickers were laundering funds through Insurance firm Z located in an off-shore jurisdiction.

Insurance firm Z offers investment products similar to mutual funds. The rate of return is tied to the major world stock market indices so the insurance policies were able to perform as investments. The account holders would over-fund the policy, moving monies into and out of the fund for the cost of the penalty for early withdrawal. The funds would then emerge as a wire transfer or cheque from an insurance company and the funds were apparently clean.

To date, this investigation has identified that over US$29 million was laundered through this scheme, of which over US$9 million has been seized. Additionally, based on joint investigative efforts by Country Y (the source country of the narcotics) and Country Z customs officials, several search warrants and arrest warrants were executed relating to money laundering activities involved individuals associated with Insurance firm Z.

Case 4

An attempt was made to purchase life policies for a number of foreign nationals. The underwriter was requested to provide life coverage with an indemnity value identical to the premium. There were also indications that in the event that the policies were to be cancelled, the return premiums were to be paid into a bank account in a different jurisdiction to the assured.

Case 5

On a smaller scale, local police authorities were investigating the placement of cash by a drug trafficker. The funds were deposited into several bank accounts and then transferred to an account in another jurisdiction. The drug trafficker then entered into a US$75,000 life insurance policy. Payment for the policy was made by two separate wire transfers from the overseas accounts. It was purported that the funds used for payment were the proceeds of overseas investments. At the time of the drug trafficker's arrest, the insurer had received instructions for the early surrender of the policy.

Case 6

A customer contracted life insurance of a 10 year duration with a cash payment equivalent to around US$400,000. Following payment, the customer refused to disclose the origin of the funds. The insurer reported the case. It appears that prosecution had been initiated in respect of the individual's fraudulent management activity.

Case 7

A life insurer learned from the media that a foreigner, with whom it had two life-insurance contracts, was involved in Mafia activities in his/her country. The contracts were of 33 years duration. One provided for a payment of close to the equivalent of US$1 million in case of death. The other was a mixed insurance with value of over half this amount.

Case 8

A client domiciled in a country party to a treaty on the freedom of cross-border provision of insurance services, contracted with a life-insurer for a foreign life insurance for 5 years with death cover for a down payment equivalent to around US$7 million. The beneficiary was altered twice: 3 months after the establishment of the policy and 2 months before the expiry of the insurance. The insured remained the same. The insurer reported the case. The last beneficiary - an alias - turned out to be a PEP.

REINSURANCE

Case 1

An insurer in country A sought reinsurance with a reputable reinsurance company in country B for its directors and officer cover of an investment firm in country A. The insurer was prepared to pay four times the market rate for this reinsurance cover. This raised the suspicion of the reinsurer which contacted law enforcement agencies. Investigation made clear that the investment firm was bogus and controlled by criminals with a drug background. The insurer had ownership links with the investment firm. The impression is that - although drug money would be laundered by a payment received from the reinsurer - the main purpose was to create the appearance of legitimacy by using the name of a reputable reinsurer. By offering to pay above market rate the insurer probably intended to assure continuation of the reinsurance arrangement.

INTERMEDIARIES

Case 1

A person (later arrested for drug trafficking) made a financial investment (life insurance) of US$250,000 by means of an insurance broker. He acted as follows. He contacted an insurance broker and delivered a total amount of US$250,000 in three cash instalments. The insurance broker did not report the delivery of that amount and deposited the three instalments in the bank. These actions raise no suspicion at the

bank, since the insurance broker is known to them as being connected to the insurance branch. The insurance broker delivers, afterwards, to the insurance company responsible for making the financial investment, three cheques from a bank account under his name, totalling US$250,000, thus avoiding the raising suspicions with the insurance company.

Case 2

Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client by way of an ID card, but these details were unable to be clarified by the providing institution locally, which was reliant on the intermediary doing the due diligence checks.

The policy was put in place and the relevant payments were made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the client stating that there was now a change in circumstances, and they would have to close the policy suffering the losses, but coming away with a clean cheque from the institution.

On other occasions the policy would be left to run for a couple of years before being closed with the request that the payment be made to a third party. This was often paid with the receiving institution, if local, not querying the payment as it had come from another reputable local institution.

Case 3

An insurance company was established by a well-established insurance management operation. One of the clients, a Russian insurance company, had been introduced through the management of the company's London office via an intermediary.

In this particular deal, the client would receive a "profit commission" if the claims for the period were less than the premiums received. Following an on-site inspection of the company by the insurance regulators, it became apparent that the payment route out for the profit commission did not match the flow of funds into the insurance company's account. Also, the regulators were unable to ascertain the origin and route of the funds as the intermediary involved refused to supply this information. Following further investigation, it was noted that there were several companies involved in the payment of funds and it was difficult to ascertain how these companies were connected with the original insured, the Russian insurance company.

Case 4

A construction project was being financed in Europe. The financing also provided for a consulting company's fees. To secure the payment of the fees, an investment account was established and a sum equivalent to around US$400,000 deposited with a life-insurer. The consulting company obtained powers of attorney for the account. Immediately following the setting up of the account, the consulting company withdrew the entire fee stipulated by the consulting contract. The insurer reported the transaction as suspicious. It turns out that an employee of the consulting company was involved in several similar cases. The account is frozen.

OTHER EXAMPLES

Single premiums

An example involves the purchase of large, single premium insurance policies and their subsequent rapid redemption. A money launderer does this to obtain payment from an insurance company. The person may face a redemption fee or cost, but this is willingly paid in exchange for the value that having funds with an insurance company as the immediate source provider.

In addition, the request for early encashment of single premium policies, for cash or settlement to an individual third party may arouse suspicion.

Return premiums

There are several cases where the early cancellation of policies with return of premium has been used to launder money. This has occurred where there have been:

(a) a number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time;

(b) return premium being credited to an account different from the original account;

(c) requests for return premiums in currencies different from the original premium; and

(d) regular purchase and cancellation of policies.

Overpayment of premiums

Another simple method by which funds can be laundered is by arranging for excessive numbers or excessively high values of insurance reimbursements by cheque or wire transfer to be made. A money launderer may well own legitimate assets or businesses as well as an illegal enterprise. In this method, the launderer may arrange for insurance of the legitimate assets and 'accidentally', but on a recurring basis, significantly overpay his premiums and request a refund for the excess. Often, the person does so in the belief that his relationship with his representative at the company is such that the representative will be unwilling to confront a customer who is both profitable to the company and important to his own success.

The overpayment of premiums, has been used as a method of money laundering. Insurers should be especially vigilant where:

- the overpayment is over a certain size (say US$10,000 or equivalent);
- the request to refund the excess premium was to a third party;
- the assured is in a jurisdiction associated with money laundering; and
- where the size or regularity of overpayments is suspicious.

High brokerage / third party payments / strange premium routes

High brokerage can be used to pay off third parties unrelated to the insurance contract. This often coincides with example of unusual premium routes.

Assignment of claims

In a similar way, a money launderer may arrange with groups of otherwise legitimate people, perhaps owners of businesses, to assign any legitimate claims on their policies to be paid to the money launderer. The launderer promises to pay these businesses, perhaps in cash, money orders or travellers cheques, a percentage of any claim payments paid to him above and beyond the face value of the claim payments. In this case the money laundering strategy involves no traditional fraud against the insurer. Rather, the launderer has an interest in obtaining funds with a direct source from an insurance company, and is willing to pay others for this privilege. The launderer may even be strict in insisting that the person does not receive any fraudulent claims payments, because the person does not want to invite unwanted attention.

IMPORTANT NOTE

Apart from the above examples of money laundering schemes, the FATF has also published annually detailed typologies involving insurance supported by useful case examples in documents called "Money Laundering & Terrorist Financing Typologies". The documents can be downloaded at the publications section of FATF website at ***http://www.fatf-gafi.org***. Insurance institutions are advised to regularly browse the website for latest information.

SAMPLE REPORT MADE TO THE JOINT FINANCIAL INTELLIGENCE UNIT

<table>
<tr><td colspan="3">Report made under section 25A of the Drug Trafficking (Recovery of Proceeds) Ordinance/Organized and Serious Crimes Ordinance or section 12 of the United Nations (Anti-Terrorism Measures) Ordinance to the Joint Financial Intelligence Unit</td><td colspan="3">Date :
Ref. No. :</td></tr>
<tr><td colspan="2">NAME AND ADDRESS OF INSURANCE INSTITUTION</td><td colspan="4"></td></tr>
<tr><td colspan="2">NAME OF SUSPICIOUS CUSTOMER (in full)</td><td colspan="4"></td></tr>
<tr><td colspan="2">DATE OF ISSUE OF INSURANCE POLICY (if applicable)</td><td></td><td colspan="2">DATE OF BIRTH / DATE OF INCORPORATION*</td><td></td></tr>
<tr><td colspan="2">OCCUPATION & EMPLOYER / NATURE OF BUSINESS*</td><td colspan="4"></td></tr>
<tr><td colspan="2">NATIONALITY / PLACE OF INCORPORATION*</td><td></td><td colspan="2">HKID / PASSPORT / BUSINESS REGISTRATION NO.*</td><td></td></tr>
<tr><td colspan="2">ADDRESS OF CUSTOMER</td><td colspan="4"></td></tr>
<tr><td>INFORMATION OF THE BENEFICIARY</td><td colspan="2">NAME & ADDRESS, RELATION WITH CUSTOMER</td><td>DATE OF BIRTH / DATE OF INCORPORATION*</td><td>HKID / PASSPORT NO.</td><td>NATIONALITY / PLACE OF INCORPORATION*</td></tr>
<tr><td>DETAILS OF TRANSACTION AROUSING SUSPICION, AND THE SUM INVOLVED INDICATING SOURCE & CURRENCY USE. PLEASE ALSO ENCLOSE COPY OF THE TRANSACTION AND OTHER RELEVANT DOCUMENT</td><td>PARTICULARS OF TRANSACTION</td><td>AMOUNT</td><td>DATE</td><td>SOURCE</td></tr>
<tr><td>OTHER RELEVANT INFORMATION INCLUDING REASON FOR SUSPICION AROUSED</td><td colspan="4"></td></tr>
<tr><td>REPORTING OFFICER / TEL. NO.</td><td colspan="2">SIGNATURE</td><td colspan="2">ENTERED RECORDS</td></tr>
</table>

** in the case of a corporation*

JOINT FINANCIAL INTELLIGENCE UNIT CONTACT DETAILS

Written report should be sent to the Joint Financial Intelligence Unit at either the address, fax number, e-mail or PO Box listed below:

The Joint Financial Intelligence Unit,
28/F, Arsenal House West Wing,
Hong Kong Police Headquarters,
Arsenal Street,
Hong Kong.

or

The Joint Financial Intelligence Unit,
GPO Box 6555,
Hong Kong Post Office,
Hong Kong.

Tel: 2866 3366

Fax: 2529 4013

Email: jfiu@police.gov.hk

Urgent reports should be made either by fax, e-mail or by telephone to 2866 3366.

SAMPLE ACKNOWLEDGEMENT LETTER ISSUED BY THE JOINT FINANCIAL INTELLIGENCE UNIT

Date:

The Compliance Officer
Any Insurance Co./Broker

Your ref.:

Dear Sir,

Drug Trafficking (Recovery of Proceeds) Ordinance
Organized and Serious Crimes Ordinance
United Nations (Anti-Terrorism Measures) Ordinance

I refer to your disclosure made to the Joint Financial Intelligence Unit on [ ] under the above references.

I acknowledge receipt of the information supplied by you under the provisions of Section 25A of the Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405 and the Organized and Serious Crimes Ordinance, Cap. 455 / Section 12 of the United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575.

Based upon the information currently available, consent is given for you to continue to operate the account(s) in accordance with normal insurance practice under the provisions of the Ordinance(s).

Thank you for your co-operation.

Yours faithfully,

Joint Financial Intelligence Unit

SECURITIES AND
FUTURES COMMISSION
證券及期貨事務監察委員會

Prevention of Money Laundering and Terrorist Financing Guidance Note

防止洗黑錢及恐怖分子籌資活動的指引

Hong Kong
September 2009

香港
2009 年 **9** 月

目錄

詞彙

本指引採用以下簡稱及詞彙：

《販毒(追討得益)條例》	指《販毒(追討得益)條例》(第 405 章)。
同等標準的地區	指所採用的防止洗黑錢及恐怖分子籌資活動的標準等同於財務行動特別組織的標準的司法管轄區。如要取得指引以評估某司法管轄區是否已充分應用財務行動特別組織的標準來打擊洗黑錢及恐怖分子籌資活動，請參閱第 6.2.6 分節。 就本指引而言，歐盟所有成員國(包括直布羅陀)、荷屬安的列斯及阿魯巴、萌島（又稱人島）、格恩西島（又稱耿濟島或根西島）及澤西島均被視爲同等標準的地區。
財務行動特別組織（FATF）	指 the Financial Action Task Force on Money Laundering ，即打擊洗黑錢財務行動特別組織。
財務行動特別組織成員	不時隸屬財務行動特別組織成員的司法管轄區。 財務行動特別組織成員包括阿根廷、澳大利亞、奧地利、比利時、巴西、加拿大、丹麥、芬蘭、法國、德國、希臘、中國香港、冰島、愛爾蘭、意大利、日本、盧森堡、墨西哥、荷蘭、紐西蘭、挪威、葡萄牙、俄羅斯聯邦、新加坡、南非、西班牙、瑞典、瑞士、土耳其、英國及美國。此外，財務行動特別組織的成員亦包括兩個國際組織，即歐洲委員會及海灣合作理事會。 財務行動特別組織現有成員的名單可於其網站 www.fatf-gafi.org 取覽，財務行動特別組織將會不時更新該名單。
財務中介人	指爲其客戶或代表他們進行財務交易的財務機構。
聯合財富情報組（JFIU）	指 the Joint Financial Intelligence Unit，即由香港警務處及香港海關的職員聯合運作的聯合財富情報組。
不合作國家及地區（NCCTs）	指non-cooperative countries and territories，即財務行動特別組織所識別，在防止洗黑錢制度方面有嚴重不足，或表明不願意合作推行防止洗黑錢措施的不合作國家及地區。不合作國家及地區的現行名單可於財務行動特別組織網站www.fatf-gafi.org 查閱，而財務行動特別組織將會不時更新該名單。

《有組織及嚴重罪行條例》	指《有組織及嚴重罪行條例》(第 455 章)。
政界人士	指目前或以往曾經擔任重要公職的人士，例如國家或政府首長、資深政客、高級政府官員、高級司法人員或高級軍官、政府擁有企業的高級行政人員及政黨的要員。此定義不擬涵蓋上述類別的中級或初級人員。
專業中介人	指爲其客戶或代表他們進行財務交易的律師或會計師。
《證券及期貨條例》	指《證券及期貨條例》(第 571 章)。
大股東	指根據《證券及期貨條例》附表 1 第 1 部第 6 條所界定的涵義。
《聯合國反恐條例》	指《聯合國(反恐怖主義措施)條例》(第 575 章)。

第I部　　概覽

1.　引言

1.1　本指引根據《證券及期貨條例》第 399 條發表，提供有關洗黑錢及恐怖分子籌資活動事宜的一般性背景資料，並簡介香港有關打擊洗黑錢及恐怖分子籌資活動的適用法例的主要條文，以及就該等法例的實際含意提供指引。本指引亦載列持牌法團或並非認可財務機構的有聯繫實體及其代表應落實的措施，以遏止及識別任何洗黑錢或恐怖分子籌資活動。證監會將持續檢討本指引的內容是否相關及適用，並可能需要不時作出修訂。

1.2　本指引旨在主要供根據《證券及期貨條例》獲發牌的法團及本身並非認可財務機構的有聯繫實體使用。在相關情況下，本指引同時適用於持牌代表。至於註冊機構及本身爲認可財務機構的有聯繫實體，則須遵從香港金融管理局就防止洗黑錢發出的指引(“金管局的指引”)。然而，對於本指引載有某些專爲證券或期貨業制定而在金管局的指引中可能沒有述及的指引，即當爲某客戶執行證券交易後未能以令人信納的方式完成有關的仔細查證客戶身分程序時應採取的風險管理程序、以某財務或專業中介人的名義開立綜合帳戶，以及與證券業有關的可疑交易例子等，在這些事宜的範圍內，註冊機構及身爲認可財務機構的有聯繫實體則須參考分別載於本指引第 6.1.10、6.6 分節及附錄 C(ii)相關部分的指引。

1.3　本指引沒有法律效力，及不應以任何方式詮釋爲凌駕任何適用於有關持牌法團、有聯繫實體或註冊機構的法規、守則或其他監管規定。如有不相符之處，應以規定較高行爲準則的條文爲準。然而，若任何持牌法團、持牌代表(如適用)或有聯繫實體未有遵從本指引的規定，假如沒有足以減輕責任的情況，便可能會對其適當人選資格產生負面影響。同樣，若註冊機構及身爲認可財務機構的有聯繫實體未有遵從金管局的指引或參考本指引第 6.1.10、6.6 分節及附錄 C(ii)相關部分的規定，假如沒有足以減輕責任的情況，亦可能會對其適當人選資格產生負面影響。

1.4　證監會職員在考慮某人是否未有符合本指引時將採取務實的方法，並會考慮所有相關情況。

1.5 除非另有指明或文意另有所指，否則本指引所載的詞彙及語句須參照該等詞彙或語句在《證券及期貨條例》附表 1 第 1 部的任何定義而加以詮釋。

2. 背景

2.1 洗黑錢及恐怖分子籌資活動的性質

2.1.1 “洗黑錢”一詞涵蓋廣泛系列的活動及過程，而這些活動和過程旨在改變從犯罪所得收益的來源的識別資料，從而掩飾其非法來源。

2.1.2 “恐怖分子籌資”一詞包括爲恐怖主義行爲、恐怖分子及恐怖主義組織進行的籌資活動，涵蓋來自合法或非法來源的資金。

2.1.3 恐怖分子或恐怖組織需要財政支援來達到目的。他們往往需要隱藏或掩飾他們與資金來源之間的連繫。因此，恐怖分子集團同樣必須尋找清洗資金的途徑(不論有關的資金來源是否合法)，以便能夠在不被有關當局發現的情況下使用資金。

2.2 洗黑錢的階段

2.2.1 洗黑錢通常有 3 個常見的階段，當中經常涉及多宗交易。持牌法團或有聯繫實體應留意可能涉及犯罪活動的徵兆。這些階段包括：

(a) 存放－以實物方式處置來自非法活動的現金收益；

(b) 掩藏－透過複雜多層的金融交易將不法收益抽離其來源，以隱藏款項的來源、擾亂審計線索和隱藏款項擁有人的身分；及

(c) 整合－營造假象使人以爲源自不法活動的財富是從表面合法的來源所得。如果上述的掩藏過程成功的話，整合計劃可以有效地把經清洗的收益融入一般金融體系之內，令人以爲有關收益來自或涉及合法的商業活動。

2.2.2 附錄 B 的圖表詳細說明洗黑錢的各個階段。

2.3 證券、期貨及槓桿式外匯交易業務在洗黑錢過程中的可能用途

2.3.1 由於證券、期貨及槓桿式外匯交易業務不再主要以現金作交易媒介，所以相對於其他金融業務（例如銀行業）來說，上述業務並不那樣適合用來初步存放從犯罪活動所得款項。然而，如該等交易以現金支付，這些業務被利用來存放黑錢的風險便不容忽視，因此必須進行仔細查證。

2.3.2 證券、期貨及槓桿式外匯交易業務較有可能被用於洗黑錢的第二個階段，即掩藏黑錢來源的過程。有別於透過銀行網絡清洗黑錢的做法，這些業務爲洗黑錢人士提供可行的途徑，令他們可以顯著地改變有關款項的形式。這些改變除了可以將手頭現金變爲現金存款之外，還可以將任何形式的款項轉化爲截然不同的資產或一系列的資產，例如證券或期貨合約。基於買賣這些金融工具的市場的流通性，上述轉變可以十分頻密地進行。

2.3.3 現金等值的投資工具(例如不記名債券及其他無需借助身分登記資料來證明所有權的投資)，對洗黑錢的人來說可能特別具吸引力。

2.3.4 正如先前所述，由於證券、期貨及槓桿式外匯交易市場的流通性，這些市場的交易對洗黑錢人士來說有其吸引力。由於有關交易能將利用合法和不法收益取得的投資組合隨時變現、可以隱藏不法收益的來源、有各種不同的投資媒介可供選擇，以及可以在各種投資媒介之間輕易地轉移資金，因此對洗黑錢人士提供具吸引力的途徑，從而有效地將犯罪收益融入一般經濟體系。

2.4 國際性措施

2.4.1 財務行動特別組織是在 1989 年成立的重要跨政府組織，旨在調查洗黑錢活動及就打擊這些活動的措施提供建議。財務行動特別組織的《40 項建議》列出打擊洗黑錢行動的框架，並且是爲了在全球應用而制訂的。香港自 1990 年起成爲財務行動特別組織的成員，肩負落實該等建議的義務。2001 年 10 月，財務行動

特別組織將其工作範圍擴展至涵蓋有關恐怖分子籌資活動的事宜。

2.4.2 在 1992 年，成員包括香港證監會的國際證券事務監察委員會組織(“國際證監會組織”)通過一項決議，要求國際證監會組織的成員考慮各項關乎盡量減低洗黑錢情況的措施，例如充分地識別客戶身分、備存紀錄、設立監察和合規程序，以及識別和舉報可疑的交易。

2.4.3 在 1996 年 6 月，財務行動特別組織就如何打擊洗黑錢活動發表經修訂的《40 項建議》。該《40 項建議》其後於 2003 年 6 月再作修訂[1]，以應付日益複雜的清洗犯罪所得款項的手法。經修訂的《40 項建議》不僅適用於洗黑錢活動，並且同時適用於恐怖分子籌資活動，若與財務行動特別組織於 2004 年 10 月修訂的《9 項特別建議》一併施行，將可爲打擊洗黑錢及恐怖分子籌資活動建立一套更嚴格、週全和穩健的措施架構(以下統稱爲“財務行動特別組織的各項建議”)。

2.4.4 鑑於財務行動特別組織及其他國際組織近期的工作，國際證監會組織於 2002 年 10 月成立一個專責小組，負責研究現行的證券監管制度，並制定有關識別客戶及實益擁有人身分的原則。國際證監會組織其後於 2004 年 5 月發表題爲《證券業有關識別客戶身分及實益擁有權的原則》[2] 的文件，對證券規管機構及證券業內的受規管商號提出有關落實仔細查證客戶身分規定的指引。

3. 與洗黑錢及恐怖分子籌資活動有關的法例

3.1 作爲全球其中一個主要的金融中心，香港必須維持有效的防止洗黑錢制度，以進一步鞏固本港金融制度的廉潔穩健及穩定性。洗黑錢活動可以對社會整體帶來嚴重的後果，不僅容許犯罪分子進行非法活動，更會削弱金融體系，對政府以至社會整體構成負面影響。

---

1 財務行動特別組織的各項建議可於財務行動特別組織網站www.fatf-gafi.org取覽。

2 國際證監會組織《證券業有關識別客戶身分及實益擁有權的原則》可於國際證監會組織網站www.iosco.org/library/index.cfm取覽。

3.2 在香港，與洗黑錢及恐怖分子籌資活動有關的 3 項主要法例爲《販毒(追討得益)條例》、《有組織及嚴重罪行條例》及《聯合國反恐條例》。附錄 A 撮述這些條例中有關打擊洗黑錢及恐怖分子籌資活動的主要條文。該撮要並非適用法例的法律詮釋。在適當情況下，應諮詢法律顧問的意見。

4. 打擊洗黑錢及恐怖分子籌資活動的政策和程序

4.1 指導原則

4.1.1 本指引已參考最新的財務行動特別組織的各項建議中適用於證券、期貨及槓桿式外匯交易業務的要求。第 II 部的詳細指引列出相關措施及程序，指導持牌法團及有聯繫實體如何防止洗黑錢及恐怖分子籌資活動。若干建議措施及程序未必適用於所有情況。各持牌法團或有聯繫實體應審慎考慮其業務、組織架構、客戶及交易類型等各方面的特定性質，使其信納所採取的措施能夠充分及適當地符合在第 II 部內所建議措施的精神。

4.1.2 在本指引中，凡提述持牌法團或有聯繫實體信納某項事宜，指該持牌法團或有聯繫實體必須能夠向證監會證明其評估是有充分理由支持的，並顯示從客觀角度看來，該評估按其作出的有關時間及情況來說是合理的。如適用，持牌法團或有聯繫實體也應能夠按照任何其他適用規則及規例，向任何其他相關機構證明其評估是有充分理由支持的。

4.2 制定政策和程序的責任

4.2.1 多項旨在打擊販毒、恐怖主義及其他有組織及嚴重罪行的國際性措施均達致結論，認爲財務機構[3] 必須設立內部監控程序，以防止及阻止洗黑錢及恐怖分子籌資活動。所有法定要求均訂明不得助長洗黑錢或恐怖分子籌資活動這個共同責任。財務機構亦需要設立制度，向執法機構舉報可疑的洗黑錢或恐怖分子籌資活動。

---

[3] 根據財務行動特別組織的各項項建議所界定，“財務機構”包括從事一系列金融活動的個人或實體。詳情請參閱財務行動特別組織的各項建議的詞彙表，網址爲www.fatf-gafi.org。

4.2.2 有鑑於此，持牌法團或有聯繫實體的高級管理層應盡全力設立適當的防止洗黑錢及恐怖分子籌資活動的政策和程序，並確保該等政策和程序是有效的和符合所有相關法定及監管規定。持牌法團及有聯繫實體應：

(a) 發出列明應付洗黑錢及恐怖分子籌資活動的政策及程序(如適用的話，該等政策及程序應以整個集團爲基準)的陳述，以反映現行的法定及監管要求，包括：

- 備存紀錄；及
- 與有關執法機構合作，包括及時披露資料；

(b) 確保所有職員都對本指引的內容(以適當的範疇爲限)有所理解，目的是培養職員的認知及警覺性，以防範洗黑錢及恐怖分子籌資活動；

(c) 定期檢討有關防止洗黑錢及恐怖分子籌資活動的政策和程序，以確保其效用。例如，由內部審計或監察職能進行審查，以確保與防止洗黑錢及恐怖分子籌資活動相關的政策、程序及監控機制獲得遵從[4]；

(d) 採用能夠充分顧及洗黑錢及恐怖分子籌資活動風險的客戶接納政策和程序；及

(e) 視乎客戶、業務關係或交易的類型而定，採納能充分顧及洗黑錢及恐怖分子籌資活動風險的仔細查證客戶身分(“客戶查證”)措施(見第6.1.2分節)。

4.3 在海外分行及附屬公司實施政策和程序

4.3.1 持牌法團及有聯繫實體必須了解境外法規的敏感性質，同時也須確保其海外分行及(在切實可行範圍內)附屬公司認識有關洗黑錢及恐怖分子籌資活動的集團

[4] 檢討範圍應包括：(i)評估用來偵察涉嫌洗黑錢交易的系統；(ii)評核及檢查有關大額及／或不尋常交易的例外情況報告是否充足；(iii)檢討可疑交易舉報的質量；及(iv)評估前線員工對其職責的認知程度。

政策，並在當地法規的範圍內盡量應用集團標準。如適當的話，應向海外分行及(在切實可行範圍內)附屬公司就供披露可疑人士、交易或財產的當地舉報點給予指示。

4.3.2 如分行及附屬公司位於並無實施或沒有充分實施財務行動特別組織的各項建議的司法管轄區，包括財務行動特別組織指定爲不合作國家及地區[5] 的司法管轄區，持牌法團及有聯繫實體便應格外留意該等分行及附屬公司的防止洗黑錢及恐怖分子籌資活動的合規水平。

4.3.3 倘若持牌法團或有聯繫實體獲悉某海外分行或附屬公司未能遵照集團標準，便應在切實可行範圍內盡快通知證監會。

第II部　　詳細指引

5. 客戶接納事宜

5.1 持牌法團及有聯繫實體應制定客戶接納政策和程序，以識別出洗黑錢及恐怖分子籌資活動風險較一般爲高的客戶類型。對於風險較高的客戶，應採用較全面的仔細查證客戶身分程序。此外，應有清晰的內部政策訂明與該類客戶的業務關係須經哪一級的管理層批准。

5.2 在釐定某名或某類客戶的風險概況時，持牌法團及有聯繫實體應考慮如以下的因素：

(a) 客戶的背景或概況，例如是否身爲政界人士，或與政界人士有關連；

(b) 客戶的業務性質，即特別是相當可能涉及洗黑錢風險的行業，例如貨幣兌換商或賭場等處理大量現金的行業；

[5] 對於出現嚴重缺失及在改善其情況方面進展不足的不合作國家及地區，財務行動特別組織可能會建議採取進一步的針對措施。證監會將繼續於適當時候，通知持牌法團及有聯繫實體由財務行動特別組織所建議的具體針對措施，包括其最新進展。這些措施一般強調更嚴謹地仔細查證客戶身分，以及更嚴格的監察和交易的舉報。持牌法團及有聯繫實體應按照證監會的通知，對該等不合作國家及地區採取針對措施。

(c) 客戶的國籍、公民身分及居民身分(如屬公司客戶，則註冊成立地)、客戶業務的成立地點、與客戶有業務往來的交易對手的所在地，例如財務行動特別組織指定爲不合作國家及地區，或據持牌法團及有聯繫實體所知在防止洗黑錢標準或仔細查證客戶身分程序方面缺乏適當標準的地區；

(d) 如屬公司客戶，其擁有權結構是否不合理地過度複雜；

(e) 付款方式及付款類別(例如以現金或第三方開立的支票付款，但付款人與準客戶之間看來並無關連，便可能有理由作出更詳盡的審查)；

(f) 涉及以非直接會面方式建立的業務關係的風險；及

(g) 反映客戶涉及較高風險的任何其他資料(例如客戶遭另一家財務機構拒絕與其建立業務關係的資料)。

5.3 對於洗黑錢及恐怖分子籌資活動風險較一般爲高的客戶，例如來自不合作國家及地區或與其有密切關連的客戶或來自其他未能符合財務行動特別組織的標準的司法管轄區的客戶，持牌法團及有聯繫實體應採納平衡及合乎常理的做法。雖然在處理該等個案時應格外審慎，但並無規定持牌法團及有聯繫實體應拒絕與該等客戶進行任何業務，或將他們自動歸類爲高風險並按照本指引第 6.2 分節論述的風險爲本的處理方法對其實施更嚴格的仔細查證客戶身分程序。相反，持牌法團及有聯繫實體應衡量每宗特定個案的所有情況，並評估是否存在高於正常水平的洗黑錢風險。

5.4 持牌法團或有聯繫實體在初次接納某客戶後，如發現該客戶的帳戶活動模式與持牌法團或有聯繫實體對該客戶的認識並不相符，便應考慮將該客戶重新歸類爲較高風險者，並應考慮舉報可疑交易。

6. 仔細查證客戶身分

6.1 一般事宜

6.1.1 持牌法團及(如適用)有聯繫實體應採取所有合理步驟，使其能夠確立每名客戶的全部及真正身分，以及

每名客戶的財政狀況和投資目標，直至其感到信納爲止。

6.1.2 仔細查證客戶身分程序應包括以下各項：

(a) 識別客戶的身分，即知道該個人或法律實體是誰；

(b) 利用從可靠來源獲得的文件、數據或資料來核實客戶身分；

(c) 識別及核實實益擁有權及控制權，即確定最終擁有或控制客戶的個人及／或代表其進行交易的人士；及

(d) 持續進行仔細查證及審察，即在業務關係維持有效的期間內持續審察交易及帳戶，以確保正在進行的交易與持牌法團或有聯繫實體對客戶、其業務及風險概況的認識相符，並在有需要時，同時考慮客戶的資金來源。

6.1.3 適用於不同類型客戶的特定客戶查證規定載於第 6.3 至 6.11 分節。就符合此等規定而言，指導原則是要求持牌法團及有聯繫實體應能夠列出理由證明他們已採取客觀地合理的步驟，使其信納客戶(包括實益擁有人)的真正身分。

6.1.4 除另有規定外，本指引中載列的客戶查證措施應同時適用於客戶本人及其實益擁有人。

6.1.5 持牌法團及有聯繫實體應利用從可靠來源發出的文件，以核實客戶的身分。如有懷疑或難以辨別身分證明文件的真僞，持牌法團及有聯繫實體應向獨立於該客戶以外的來源索取該文件。

6.1.6 視乎客戶、業務關係或交易類型而定，持牌法團及有聯繫實體需要在充分顧及風險的基礎上獲得有關業務關係的目的及擬定性質的適當資料，從而按照與該客戶的風險概況相符的水平，對該客戶進行持續的仔細查證。

6.1.7 持牌法團及有聯繫實體不應存置匿名帳戶或使用假名的帳戶。

6.1.8 在建立業務關係時，持牌法團及有聯繫實體應詢問客戶是代表其本人行事，抑或代表其他人士行事，藉以識別客戶所開立的帳戶的實益擁有人。

6.1.9 一般而言，持牌法團或有聯繫實體應在建立業務關係前核實客戶及實益擁有人的身分。如持牌法團或有聯繫實體無法在開戶階段進行使其信納的客戶查證程序，便不應開始業務關係或進行交易，並應考慮應否舉報可疑交易。

6.1.10 然而，若由於市況而需要迅速爲客戶執行交易，或在其他必須維持正常業務運作的情況下，在建立業務關係後才完成核實是可以允許的做法，但必須在合理的切實可行範圍內盡快作出核實。持牌法團或有聯繫實體需要採納清晰及適當的政策及程序，訂明允許客戶在未經核實身分前建立業務關係的條件及時限。該等程序應包括一系列措施，例如可以執行的交易次數、類型及／或交易金額限制，並監控對於該類業務關係而言屬預期之外的大額或複雜交易。例如，可能需要考慮不得允許(如可行的話)在客戶身分尚未以令人信納的方式核實前，把資金從該帳戶支付給第三方。在開展業務關係後，如持牌法團或有聯繫實體無法於合理的切實可行的時限內以使其信納的完成客戶查證程序，便應在可行情況下終止業務關係，並考慮應否舉報可疑交易。

6.1.11 持牌法團及有聯繫實體應採取合理步驟，確保現有客戶的紀錄載有最新及相關的資料。

6.1.12 爲此，持牌法團或有聯繫實體應考慮定期及／或特別審查現有客戶的紀錄，以考慮將某客戶重新歸類爲高或低風險。進行這些審查的頻常度可視乎持牌法團或有聯繫實體對該客戶的認識、與其關係和交易的類別。例如，當發生一宗根據持牌法團或有聯繫實體對該客戶的認識而言屬不尋常或與該客戶的正常交易模式不符的交易；或帳戶的運作方式出現重大變動；或持牌法團或有聯繫實體未能信納其擁有關於該客戶的

充分資料；或懷疑以往取得的身分識別資料並不真實或足夠，便可能是作出特別審查的適當時候。

6.1.13 即使並無出現上述第 6.1.12 分節所述的情況，持牌法團及有聯繫實體也應考慮是否需要向現有客戶索取額外資料，以符合現行標準。

6.2 風險爲本的處理方法

6.2.1 一般原則是應對客戶採取全面的客戶查證措施。然而，持牌法團及有聯繫實體應在充分顧及風險的基礎上，釐定每項客戶查證措施的應用程度。風險爲本的處理方法的基本原則是，持牌法團及有聯繫實體應對屬於較高風險類別的客戶、業務關係或交易，採取更嚴格的客戶查證程序。同樣，對屬於較低風險類別的客戶、業務關係或交易，則採取簡化客戶查證程序。有關更嚴格或簡化的客戶查證程序可能因應個別客戶的背景、交易種類及特定情況等而有所不同。持牌法團及有聯繫實體在對屬於特別高或特別低風險類別的客戶採取特定的更嚴格或簡化客戶查證措施時，應自行判斷及採取靈活的做法。

6.2.2 持牌法團及有聯繫實體應在其客戶接納政策內清晰地制定在確定將哪一類客戶或活動視作低或高風險時須考慮的風險因素，同時明白到沒有政策能夠巨細無遺地列出在每一個可能情況下應予考慮的全部風險因素。此外，他們必須使其信納在該等情況下採用簡化的仔細查證客戶身分程序是合理的，並已獲高級管理層批准。如開立須進行更嚴格客戶查證的高風險帳戶，應須由高級管理層批准。

6.2.3 如不存在洗黑錢或恐怖分子籌資活動的嫌疑及符合下列條件下，便可以採用簡化客戶查證程序來識別和核實客戶及實益擁有人的身分：

- 某類客戶涉及洗黑錢或恐怖分子籌資活動的固有風險被評估爲屬低風險類別；或
- 在全國性制度中已存在有關該等客戶的充分公開披露規定或其他制衡及監控措施。

下列爲一些屬於低風險類別客戶的例子：

(a) 受證監會、香港金融管理局、保險業監理處或受屬於財務行動特別組織成員的司法管轄區或其他同等標準的地區的同等機構認可及監督的財務機構；

(b) 須遵守監管披露規定的公眾上市公司，包括在屬財務行動特別組織成員的司法管轄區內的證券交易所或《證券及期貨條例》界定的指明證券交易所[6] 上市的公司及其附屬公司；

(c) 來自非不合作國家或地區的司法管轄區的政府或政府關連組織，而該等司法管轄區的洗黑錢風險被持牌法團或有聯繫實體評估爲屬低風險類別，及持牌法團或有聯繫實體對於該組織的擁有權並無懷疑；及

(d) 透過從薪金中扣減部分款項來供款的退休金、退職金或其他爲僱員提供退休福利的類似計劃，而該計劃的規則不容許轉讓該計劃之下的成員權益。

6.2.4 應注意的是，即使客戶的固有風險被評估爲屬低風險類別，仍可能有個別例子涉及惹人懷疑的情況。如有任何疑問，應採取全面的客戶查證措施。

6.2.5 持牌法團及有聯繫實體應留意，對於並無指定爲不合作國家及地區的司法管轄區，不一定代表可視爲同等標準的地區，即其採用的防止洗黑錢及恐怖分子籌資活動標準等同於財務行動特別組織的標準。

6.2.6 在評估某國家(並非財務行動特別組織的成員或本指引詞彙該節所列的同等標準的地區)有否充分應用財務行動特別組織的標準來打擊洗黑錢及恐怖分子籌資活動並符合作爲同等標準的地區的準則時，持牌法團及有聯繫實體應：

(a) 自行評估該國家在防止洗黑錢及恐怖分子籌資活動方面的標準。該項評估可以根據商號對有

[6] 持牌法團及有聯繫實體應特別留意財務行動特別組織的各項建議中的第 21 項建議，格外審慎地處理來自不合作國家及地區的客戶及業務關係，包括在不合作國家及地區的交易所上市的公司客戶。

關國家的認識及經驗或市場情報而進行。風險越高，在與來自有關國家的客戶進行業務時採用的仔細查證措施便應越嚴格；

(b) 特別留意財務行動特別組織等標準設定機構，以及國際貨幣基金組織等國際金融機構曾經作出的評估。除了財務行動特別組織及具備與財務行動特別組織類似性質的區內機構在評估多個國家及地區的財政穩健性時曾進行相互評核外，國際貨幣基金組織及世界銀行亦曾根據財務行動特別組織的各項建議，就遵從有關防止洗黑錢及恐怖分子籌資活動標準進行國家評估；及

(c) 對洗黑錢風險保持適當程度的持續警覺，並將他們可以合理地獲得、涉及在其任何客戶與之有聯繫的國家內運作的防止洗黑錢制度及監控措施的準則的資料列入考慮範圍內。

6.2.7 除第 5.2 分節所列舉在決定客戶的風險概況時應考慮的風險因素外，以下是一些高風險類別客戶的例子：

(a) 複雜的法律安排，例如未經註冊或不受規管的投資公司；

(b) 設有代名人股東或大部分股本爲以不記名股票形式持有的公司；

(c) 來自或所在地的國家並沒有採用或沒有充分採用財務行動特別組織的各項建議(例如財務行動特別組織指定爲不合作國家及地區，或據持牌法團及有聯繫實體所知在防止洗黑錢及恐怖分子籌資活動方面缺乏適當標準的司法管轄區)的人士(包括法團及其他財務機構)；及

(d) 政界人士及與其有明顯關連的人士或公司。

6.2.8 持牌法團及有聯繫實體應特別留意所有複雜而不尋常的大額交易，以及所有缺乏明顯的經濟目的或可見的合法目的的不尋常交易模式，尤其是來自沒有採用或沒有充分採用財務行動特別組織的各項建議的國家的客戶。在可行的情況下，應盡量審查該等交易的背景

及目的，並應以書面確立調查結果，以便向主管機關提供從而給予協助。

6.3 個人客戶

6.3.1 爲核實個人客戶的身分，一般都需要如下文所述的資料：

(a) 姓名，

(b) 如屬本地客戶（具有香港居留權的居民），其香港身分證號碼；及如屬非本地客戶，其護照或未過期的政府簽發以證明其國籍或居留權的身分證明文件，

(c) 出生日期，及

(d) 住址（及永久地址，如與住址不同）。

6.3.2 香港身分證或未過期的政府簽發身分證明文件（例如護照）爲應出示作身分證明的文件類別。身分證明文件的副本應保留存檔。

6.3.3 持牌法團及有聯繫實體應以最佳的可用途徑核實客戶的地址，例如查看客戶近期的公用服務帳單或銀行結單。持牌法團及有聯繫實體應採用按常理處理問題的方法，處理屬於可能不會支付公用服務帳單或沒有銀行帳戶的該類人士的客戶及／或實益擁有人（如學生及家庭主婦）的個案。

6.3.4 持牌法團及有聯繫實體也應取得有關客戶的職業／業務的資料，以利便他們進行持續的仔細查證及審察。然而，該項資料不屬於必須核實的客戶身分的一部分。

6.3.5 持牌法團及有聯繫實體必須明白，任何形式的身分證明文件都不能完全保證是真確的，或代表有關人士的正確身分。持牌法團及有聯繫實體如懷疑或難以辨別身分證明文件是否真確，可聯絡入境事務處，就如何識別真正身分證上的特徵尋求指引。

6.3.6 在可行的情況下，應親自接見所有準客戶。若該客戶所涉及的洗黑錢或恐怖分子籌資風險被評估爲屬高風險類別，則持牌法團及有聯繫實體宜要求與該客戶直接會面。

6.4 公司客戶

6.4.1 若某公司客戶並非在屬財務行動特別組織成員的司法管轄區內的證券交易所或《證券及期貨條例》所界定的指明證券交易所 [6] 上市的公司，或並非該等上市公司的附屬公司，或並不是非不合作國家及地區的政府關連企業，或並非第 6.6.7(a)(i)或 6.6.7(a)(ii)分節所述的財務機構，則就進行客戶查證而言，像下文所述的便屬於與此有關的文件及資料：

(a) 公司註冊證書及(如適用)商業登記證或可證明該法團的成立的任何其他文件或有關其法律地位的類似證據；

(b) 證明批准開戶及授權有關人士運作該帳戶的董事局決議案；

(c) 有關該公司客戶的業務性質及其擁有權及控制權結構的資料，以識別該名客戶最終由哪名（些）個人擁有或控制；

(d) 帳戶簽署人的簽名式樣；

(e) 代表該公司客戶行事的最少 2 名獲授權人的身分證明文件副本；

(f) 最少 2 名董事（包括董事總經理）的身分證明文件副本；及

(g) 大股東及（如適用的話）最終主要實益擁有人的身分證明文件副本。

有關文件或資料可來自公眾紀錄冊、客戶或其他可靠的來源，但持牌法團或有聯繫實體須信納所提供的資料是可靠的。

6.4.2 若公司客戶本身爲上市公司或投資公司，請參閱第 6.5 分節以便獲得進一步指引。

6.4.3 若該客戶並非上市公司，而其擁有權結構由多層公司組成，持牌法團或有聯繫實體一般需要依循擁有權結構識別哪些個人是該客戶的最終主要實益擁有人，並核實這些個人的身分。然而，持牌法團或有聯繫實體無需逐一查核擁有權結構內的每家中間公司（包括其董事）的詳細資料。若公司本身爲擁有權結構內其中一員，並且是在屬財務行動特別組織成員的司法管轄區內的證券交易所或《證券及期貨條例》所界定的指明交易所[6]上市的公司或該等上市公司的附屬公司，或獲證監會、香港金融管理局或保險業監理處或位於屬財務行動特別組織成員的司法管轄區或同等標準的地區內的同等監察機構認可及監管的財務機構或該財務機構的附屬公司，則持牌法團及有聯繫實體追查至此並按照下文第 6.5.2 分節所述的建議客戶查證措施核實該客戶的身分，一般應已足夠。

6.4.4 對於較高風險類別的客戶或如對於公司客戶的實益擁有人、股東、董事或帳戶簽署人的身分存疑，持牌法團及有聯繫實體宜在充分顧及風險的基礎上，採取額外的客戶查證措施。持牌法團及有聯繫實體可以採取的有關額外措施例子包括：

(a) 進行公司查冊或向信貸資料機構查詢該公司的紀錄；

(b) 取得公司的章程大綱及細則；及

(c) 核實所有獲授權運作該帳戶的人士的身分。

6.4.5 若某項由個人（即最終實益擁有人）擁用的離岸投資公司被用作爲與持牌法團或有聯繫實體訂立業務關係的立約方，而該投資公司的成立地點的司法管轄區並不能提供公司查冊服務或現任職位證明書（或同等證明），或不能提供有關該投資公司的董事及大股東的有用資料，持牌法團及有聯繫實體宜對該客戶進行更嚴格的客戶查證程序。持牌法團及有聯繫實體除了必須能夠使其信納：

- 自己已知悉該最終實益擁有人的身分；及
- 洗黑錢的嫌疑並不存在，

亦宜在充分顧及風險的基礎上，執行額外的客戶查證措施。有關的額外措施例子包括：

(a) 取得最終實益擁有人就董事及大股東的身分及彼此關係而自行作出的聲明；

(b) 取得全面的客戶概況資料，例如開戶目的及理由、業務或就業背景、資金來源或預計帳戶活動；

(c) 在接納該客戶前與其直接會面；

(d) 獲高級管理層批准接納該客戶；

(e) 委任指定職員服務該客戶，而該名職員應有責任進行客戶查證及持續監察，以便及時地識別任何異常或可疑交易；及

(f) 在雙方維持業務關係期間盡可能定期與客戶直接會面。

6.4.6 持牌法團及有聯繫實體與大部分股本爲以不記名股票形式持有的公司交易時亦應特別謹慎。持牌法團及有聯繫實體宜訂有程序，以監察所有大股東的身分。持牌法團及有聯繫實體可能因此需要考慮是否要使該等股票變爲非流動化，例如是以託管形式持有該等不記名股票。若將該等股票變爲非流動化是不切實可行的話，持牌法團或有聯繫實體可以採取措施，例如取得該公司客戶每名大股東就其持股百分比發出的聲明、要求這些大股東每年提供該等聲明及在售賣、轉讓或轉移股份時通知有關持牌法團或有聯繫實體。

6.4.7 持牌法團及有聯繫實體在與擁有代名人股東的公司開展業務交易時亦應特別謹慎，並應就這些公司的實益擁有人的身分取得令人信納的證據。

6.5 上市公司及投資公司

6.5.1 若某法團是在屬財務行動特別組織成員的司法管轄區內的證券交易所或《證券及期貨條例》所界定的指明證券交易所[6]上市的公司，或是該等上市公司的附屬公司，或是非不合作國家及地區[7]的政府關連企業，則該法團本身可視爲須予以核實身分的人士。

6.5.2 因此，對於上文第 6.5.1 分節所述的客戶，持牌法團或有聯繫實體若能取得有關證明文件的副本，例如公司註冊證書、商業登記證及董事局的開戶決議案，一般來說應已足夠，而毋須進一步查詢其大股東、個別董事或帳戶授權簽署人的身分，但卻應索取及保留任何人已取得所需授權以運作該帳戶的證據。

6.5.3 若上市法團實質上由一名個人或一組個人控制，則建議持牌法團或有聯繫實體考慮是否需要核實這些個人的身分。

6.5.4 若客戶爲受規管或註冊投資公司，例如受制於足夠監管披露規定的集體投資計劃或互惠基金，則毋須尋求識別及核實該實體各單位持有人的身分。

6.5.5 若客戶是不受規管或未經註冊的投資公司，持牌法團及有聯繫實體應按照第 6.5.6 分節的規限，遵從本指引第 6.4、6.7 或 6.8 分節(以適用者爲準)所載列的身分識別及核實規定。

6.5.6 如持牌法團或有聯繫實體能夠確定：

(i) 該不受規管或未經註冊的投資公司已設立防止洗黑錢及恐怖分子籌資活動的計劃；及

(ii) 負責對該投資公司的投資者進行客戶查證程序的人士(如管理人、經理等)已設立符合財務行動特別組織的標準的適當措施，

而負責客戶查證程序的人士是受證監會、香港金融管理局或保險業監理處或位於屬財務行動特別組織成員

[7] 持牌法團及有聯繫實體應使其信納，非不合作國家及地區的洗黑錢風險屬於低風險類別，同時有關企業的擁有權無可置疑。

的司法管轄區或同等標準的地區內的同等監察機構規管及監察的話，則持牌法團或有聯繫實體毋須識別及核實該等投資者的身分。

6.6 財務或專業中介人

6.6.1 若以財務或專業中介人的名義開立的帳戶爲綜合帳戶，以便該財務或專業中介人代表客戶進行證券、期貨或槓桿式外匯交易，持牌法團或有聯繫實體應根據以下條文對該綜合帳戶持有人，即作爲持牌法團或有聯繫實體客戶的財務或專業中介人，進行識別及核實工作，而毋須透過該財務或專業中介人來深入探究以識別及核實由該財務或專業中介人代爲執行金融交易的相關客戶。

6.6.2 然而，除非屬於下文第 6.6.7 及 6.6.8 分節所述的例外情況，否則便需要執行更嚴格的客戶查證程序。須採取的更嚴格程序包括收集有關該財務或專業中介人的足夠資料，以了解其業務性質及評估該財務或專業中介人所在地在客戶查證準則方面的規管及監督制度[8]。

6.6.3 持牌法團及有聯繫實體亦可參考公開資料，以評估財務或專業中介人的專業聲譽。

6.6.4 持牌法團及有聯繫實體在爲下列財務或專業中介人維持綜合帳戶時應加倍審慎：

(a) 該中介人在不合作國家及地區成立；

(b) 該中介人既不實際存在於任何司法管轄區，亦不聯屬於任何實際存在於某司法管轄區的受規管金融集團；或

(c) 未能確立該財務或專業中介人已設立可靠的客戶身分核實制度，

[8] 在評估財務或專業中介人的客戶查證準則時，持牌法團及有聯繫實體可考慮收集資料，例如該中介人的業務所在地、主要業務活動、管理層、認可狀況、聲譽（曾否成爲洗黑錢或恐怖分子籌資活動的調查或監管行動的對象）、監督質素（其所在地在客戶查證準則方面的規管及監督制度），以及其對防止洗黑錢或恐怖分子籌資活動的監控。我們不擬在此巨細無遺地列舉全部因素，持牌法團及有聯繫實體可考慮其他適當因素。

而在上述情況下，一般需要採取更嚴格的仔細查證程序，以偵察及防止洗黑錢及恐怖分子籌資活動。持牌法團及有聯繫實體應對透過綜合帳戶進行而構成關注原因的交易作出合理查詢，或在有懷疑時舉報這些交易。如有需要，持牌法團及有聯繫實體不應容許財務或專業中介人開立或維持綜合帳戶。

6.6.5 除非在採取上述更嚴格的程序後，持牌法團及有聯繫實體能使其信納某財務或專業中介人在其所在的司法管轄區的監管下，在客戶查證準則方面已受到足夠的規管監督，否則持牌法團及有聯繫實體尤其不應爲下列財務中介人開立或維持綜合帳戶：該中介人既不實際存在於其註冊成立的司法管轄區，亦不聯屬於任何實際存在於某司法管轄區的受規管金融集團。

6.6.6 在建立新的綜合帳戶關係前，應先取得高級管理層的批准。持牌法團及有聯繫實體最好以書面記錄[9] 各方各自承擔的責任。

6.6.7 若綜合帳戶由以下機構開立：

(a) 應用根據財務行動特別組織的各項建議的防止洗黑錢及恐怖分子籌資活動標準的財務中介人，並：

(i) 獲證監會、香港金融管理局或保險業監理處或屬財務行動特別組織成員的司法管轄區或同等標準的地區的同等監察機構認可和受其監督；或

(ii) 身爲獲香港金融管理局或屬財務行動特別組織成員的司法管轄區或同等標準的地區的同等監察機構認可和受其監督的銀行業機構的附屬公司的信託公司；或

(b) 受到規管及監察制度所規限的專業中介人，而該規管及監察制度能確保必要的防止洗黑錢及恐怖分子籌資活動措施已根據財務行動特別組織的標準有效地落實及受到監控，

[9] 持牌法團或有聯繫實體與財務或專業中介人並不一定需要將各自的責任以書面形式列出，但雙方需清楚所規定的措施是由哪方執行的。

則洗黑錢及恐怖分子籌資活動的風險被視爲較低，因此適宜就這些帳戶採用簡化的身分識別及核實程序。

6.6.8 就上文第 6.6.7 分節所述的各類財務或專業中介人而言，持牌法團或有聯繫實體若能核實該財務或專業中介人或（就信託公司而言）作爲其母公司的銀行業機構已列於有關司法管轄區的認可及受監督機構名單內，或向有關律師公會或會計團體查詢以確定該專業中介人是否已向有關專業組織註冊，並受確保實施有效的防止洗黑錢及恐怖分子籌資活動措施的監管制度所規限，一般已經足夠。此外，應索取及保留代表該中介人的任何人已具有所需授權的證據。

6.6.9 然而，就上文第 6.6.7 分節所述以外的各類財務或專業中介人而言，持牌法團及有聯繫實體應遵從本指引第 6.4 及 6.7 分節（以適用者爲準）所載的身分識別及核實規定。

6.6.10 如帳戶是由財務或專業中介人開立以供本身交易之用，持牌法團或有聯繫實體應進行與本指引第 6.6.8 及 6.6.9 分節（以適用者爲準）所述相符的身分識別及核實程序。

6.7 並非法團的業務機構

6.7.1 對於合夥及其他並非法團的業務機構，如持牌法團或有聯繫實體不認識該等合夥或並非法團的業務機構的合夥人，則爲了進行客戶查證，持牌法團及有聯繫實體須取得足夠的證據，例如最少 2 名合夥人的身分、最少 2 名獲授權簽署人的身分，以及如已訂立正式的合夥協議，則該合夥發出以授權開戶及授權有關人士操作該帳戶的授權書。

6.7.2 若該客戶被評估爲屬洗黑錢或恐怖分子籌資的高風險類別，便應進行更嚴格的客戶查證，例如核實所有合夥人及獲授權簽署人的身分。

6.8 信託及代名人帳戶

6.8.1 持牌法團及有聯繫實體處理信託或代名人帳戶時，應了解有關各方的關係。持牌法團及有聯繫實體應取得

受託人或代名人及代表受託人或代名人行事者的身分的令人信納的證據。

6.8.2 對於屬於信託帳戶的客戶，持牌法團及有聯繫實體應採取合理措施，以了解該信託的性質。就進行客戶查證而言，如下列的文件及資料將是相關的文件及資料：

(a) 受託人或可對該信託行使有效監控者、保護人[10]、財產授予人／資產提供者[11]的身分；

(b) 受益人的身分（在盡可能的情況下），但可以接受有關受益人的廣義說明，例如受益人爲某人的家庭成員或某退休金計劃所指的僱員（而該計劃的規則並不准許將該計劃下的成員權益轉讓）；

(c) 信託契約或證明有關法律安排存在及有效的法律文件的副本。

6.8.3 若受益人的身分從未經核實，持牌法團及有聯繫實體應在可行情況下並能充分顧及風險的基礎上，盡一切努力，於執行任何交易（例如從信託帳戶提款以支付予或代表受益人作出支付）前識別及核實該等受益人的身分。如不進行有關核實的決定，最好應獲得高級管理層的批准。

6.9 政界人士

6.9.1 持牌法團或有聯繫實體若與擔任重要公職的個人及明顯與該等個人有關連的人士或公司（即家人、有密切聯繫人士等）建立業務關係，會面對特別重大的聲譽或法律風險。持牌法團或有聯繫實體應對該等政界人士進行更嚴格的仔細查證。

---

10 持牌法團及有聯繫實體在決定是否需要核實保護人的身分時，可採用風險爲本的處理方法。保護人的身分屬須核實的有關資料，原因是這些人士可以在某些情況下行使權力，以取代現任的受託人。

11 若已充分履行有關財產授予人／資產提供者的客戶查證程序，持牌法團及有聯繫實體可以接受由受託人或其他合約方所發出，以確定財產授予人/資產提供者的連繫或關係的聲明。

6.9.2 需要關注的是（特別是在一些貪污普遍的國家），這些政界人士可能會濫用公職權力，透過收受賄賂等非法途徑斂財。

6.9.3 政界人士的定義並無意涵蓋上述類別內的中級或較初級的個人。然而，持牌法團及有聯繫實體必須能夠使其信納，用作將外國政客、政府官員、司法人員或軍官等分類爲政界人士的標準能夠充分顧及洗黑錢或恐怖分子籌資活動的風險。

6.9.4 持牌法團及有聯繫實體應設有適當的風險管理制度，以確定某客戶是否政界人士（包括參考公開資料或商業數據庫）。在識別政界人士及特別是來自一些一般被視爲就貪污罪行而言風險較高的國家的人士時，可採用風險爲本的處理方法。

6.9.5 持牌法團或有聯繫實體若正考慮與懷疑屬政界人士的人建立關係，便應充分識別出該名客戶以及明顯與其有關的人士及公司的身分。持牌法團及有聯繫實體在開立客戶帳戶前，應先確定被識別爲政界人士的客戶及實益擁有人的財富及資金來源。

6.9.6 應由高級管理層決定是否接受政界人士的開戶申請。若某人爲已獲接納的客戶而該客戶或其實益持有人其後被發現或成爲政界人士，持牌法團或有聯繫實體應取得高級管理層的批准，方可繼續彼此的業務關係。

6.9.7 持牌法團及有聯繫實體在處理與政界人士的業務關係（或可能建立的業務關係）時應考慮的風險因素包括：

(a) 政界人士所屬國家有否引起任何特別關注，並要考慮到該政界人士的職位；

(b) 任何無法解釋來源的財富或收入（即該政界人士所擁有的資產價值與其收入水平不相稱）；

(c) 未有預計而從政府機構或政府關連組織收到的大額款項；

(d) 被描述爲就政府合約所賺取的佣金的財富來源；

(e) 政界人士要求就某項交易作出任何形式的保密安排；及

(f) 以在政府的關連銀行開設的帳戶或政府帳戶作爲某項交易中的資金來源。

6.10 非直接會面的客戶

6.10.1 以非直接會面方式開戶是指持牌法團沒有與有關客戶會面，而其僱員既沒有目睹客戶簽署開戶文件，亦沒有查看客戶的身分證明文件，例如透過互聯網開戶。假如帳戶是以非直接會面的方式開立，有關的開戶程序應以令人信納的方式進行，從而確保該客戶的身分得以知悉。

6.10.2 持牌法團及有聯繫實體應參考《證券及期貨事務監察委員會持牌人或註冊人操守準則》（"該守則"）內有關以非直接會面方式開戶的條文。有關客戶協議書的簽署及查看客戶身分證明文件的程序應以該守則訂明的方式加以驗證（目前載於第 5.1（a）段）。此外，客戶（法團實體除外）的身分可根據該守則訂明的程序加以核實（目前載於第 5.1（b）段）。

6.10.3 如透過證明人以見證客戶協議書的簽署及查看有關身分證明文件，持牌法團或有聯繫實體應確保該證明人是受到屬財務行動特別組織成員的司法管轄區或同等標準的地區監管，及／或在該等地區成立或營運。

6.10.4 若有關客戶協議書的簽署及查看有關身分證明文件程序由並非財務行動特別組織成員的司法管轄區或並非同等標準的地區的證明人作見證，便需特別留心。在這些情況下，持牌法團及有聯繫實體應評估這些專業人士驗證的有關文件、數據或資料的可靠性，並考慮採取可以減輕該等非直接會面客戶構成的風險的額外措施，包括：

(a) 持牌法團或有聯繫實體獨立接觸該客戶；

(b) 要求提供較直接會面客戶所需爲多的額外文件；

(c) 更頻密地更新非直接會面客戶的資料；

(d) 要求需要廣泛而又可以獨立核實資料的開戶申請，須填妥網上調查問卷；或

(e) 在極端的情況下，拒絕與沒有直接會面的高風險客戶建立業務關係。

6.11 倚賴介紹人仔細查證客戶身分

6.11.1 本分節涉及向持牌法團或有聯繫實體介紹客戶的第三者。實際上，這情況往往來自同一金融服務集團的另一成員，或有時是來自另一財務機構的介紹。本分節並不適用於持牌法團或有聯繫實體與財務或專業中介人替其客戶安排的關係、帳戶或交易，即綜合帳戶。上述關係已於本指引第 6.6 分節加以解釋。

6.11.2 持牌法團或有聯繫實體可在符合下列標準的情況下，倚賴第三者執行第 6.1.2 分節的客戶查證措施的第（a）至（c）項。然而，持牌法團及有聯繫實體始終負有認識客戶的最終責任。

6.11.3 在倚賴任何介紹人前，持牌法團及有聯繫實體必須能夠信納，倚賴介紹人進行客戶查證程序是合理的，而該等客戶查證措施與持牌法團或有聯繫實體自行就客戶進行的措施須同樣嚴謹。就此而言，持牌法團及有聯繫實體宜訂立清晰的政策，以釐定有關介紹人是否具備可接受的可靠程度。

6.11.4 倚賴介紹人的持牌法團及有聯繫實體應：

(a) 在合理地切實可行範圍內盡快取得有關第 6.1.2 分節的客戶查證措施中第（a）至（c）項的必需資料，以及有關業務關係的目的和預期性質；

(b) 在合理地切實可行範圍內盡快取得如該守則第 6.2（a）段規定有關客戶身分的文件的副本（若（a）項已獲得遵行及介紹人會在接獲要求時沒有延誤地提供有關文件副本，持牌法團及有聯繫實體可選擇不索取其他有關文件的副本）；

(c) 採取足夠的程序，以便能夠信納介紹人會在接獲有關要求時，沒有延誤地提供與客戶查證要求有關的其他相關文件的副本，例如以書面確立各自的責任，包括與介紹人達成協議，表明介紹人將會應要求沒有延誤地提供與客戶查證要求有關的身分證明數據及其他相關文件的副本，以及持牌法團或有聯繫實體會獲准在任何階段核實第三者所進行的仔細查證；及

(d) 確保介紹人受到規管及監督，及已設立與財務行動特別組織的標準相符的有關遵守客戶查證程序及備存紀錄規定的措施。

6.11.5 爲了進一步確保這些準則獲得遵守，持牌法團或有聯繫實體宜在可能範圍內，倚賴在屬財務行動特別組織成員的司法管轄區或同等標準的地區註冊成立或運作的第三者，而該第三者：

(a) 是受證監會、香港金融管理局或保險業監理處或履行類似職能的機關監管的；或

(b) 若非受到這些機關監管，則能證明其已設有足夠程序，以防止清洗黑錢及恐怖份子籌資活動。

6.11.6 持牌法團及有聯繫實體應考慮進行定期檢討，以確保其倚賴的介紹人持續符合上文所列的準則，當中可包括檢討介紹人的有關政策與程序，以及抽樣查核其進行的仔細查證個案。

6.11.7 持牌法團及有聯繫實體一般不應倚賴以被視爲高風險的司法管轄區（例如不合作國家及地區或在客戶查證方面沒有受到足夠監管的司法管轄區）爲基地的介紹人，除非介紹人能夠證實他們已設有防止洗黑錢及恐怖份子籌資活動的充足程序。

7. 備存紀錄

7.1 持牌法團及有聯繫實體應確保遵守證監會及有關交易所的相關法例、規則或規例內載列的備存紀錄規定。

7.2 持牌法團及有聯繫實體應備存載有足夠資料的紀錄，以便日後能重組個別交易(包括所涉金額及貨幣種類，如有的話)，從而爲刑事行爲的檢控(如有需要的話)提供證據。

7.3 調查機關需要循令人信納的審計線索以調查及追蹤涉嫌與毒品有關或其他經清洗的黑錢或恐怖分子的財產，並需要能夠重組可疑帳戶的財政概況。就此等目的而言，持牌法團及有聯繫實體應爲其客戶的帳戶保留(如有需要的話)以下資料，以便爲調查機關提供犯罪活動的證據：

(a) 該帳戶的實益擁有人；

(b) 經該帳戶提存的資金的數額；及

(c) 個別交易的：

- 資金來源；
- 提存資金的方式，例如以現金、支票等；
- 進行該等交易的人士的身分；
- 資金調動去向；
- 指示及授權的方式。

7.4 持牌法團及有聯繫實體應確保所有客戶及交易紀錄及資料都能夠適時地提供予主管調查機關。在適當情況下，持牌法團及有聯繫實體應考慮在香港保留若干紀錄，例如客戶身分紀錄、帳戶檔案及業務往來通訊，而保留期間可較證監會或有關交易所的其他相關法例、規則及規例內所規定的爲長。

8. 保留紀錄

8.1 持牌法團及有聯繫實體應依循以下保留文件的年期：

(a) 所有關於本地及國際性交易所需備存的紀錄應保留至少7年。

(b) 客戶身分紀錄(例如正式的身分證明文件如護照、身分證、駕駛執照或類似文件的副本或紀錄)、帳戶檔案及

業務往來通訊，應在帳戶結束後保留(如切實可行的話)至少5年。

8.2 當有關紀錄涉及正在進行的調查或已被舉報的可疑交易，有關文件應予以保留，直至確定該宗調查個案已經完結爲止。

9. 識別可疑交易

9.1 爲遵守本指引，持牌法團或有聯繫實體應進行所需的持續監察，以識別可疑交易，從而履行有關需要向聯合財富情報組要求舉報其知悉或懷疑屬於犯罪收益或恐怖分子財產的資金或財產的法律義務。

9.2 視乎持牌法團或有聯繫實體的業務規模，有時單純依賴前線職員主動識別及舉報可疑交易是不足夠的。在此情況下，持牌法團或有聯繫實體可能需要設立若干系統或程序，例如編製交易報告，從而定期爲管理層及合規主任提供適時的資訊，讓他們偵察有否出現不尋常或可疑活動的模式，尤其是涉及較高風險帳戶的活動，例如政界人士的帳戶、在不合作國家及地區註冊成立的財務機構所開立的綜合帳戶等。

9.3 洗黑錢人士及恐怖分子可採用的交易類別幾乎是多不勝數的，而且很難具體詳列可能構成可疑交易的所有交易類別。然而，當交易進行的目的與有關客戶的已知商業或個人活動不相符，或與該類帳戶的正常業務運作不相符，便值得懷疑。因此，要識別可疑交易，首先要對客戶的業務及財政狀況有充分認識，以識別某項交易或連串交易屬不尋常的交易。

9.4 爲利便持牌法團及有聯繫實體識別出可疑活動，附錄C(i)載有由聯合財富情報組建議以助有效及有系統地識別可疑金融活動的方法。該等附錄僅以舉例方式提供識別可疑活動及查問客戶的方法。查問的時間性和範圍則視乎有關的整體情況而定。

9.5 附錄C(ii)亦列出可能屬於可疑或不尋常活動的清單，以說明哪些類別的交易可能需要進行詳細審查。該列表並非巨細無遺，亦不應取代有關法例所施加的任何舉報可疑或不尋常交

易的法律義務。持牌法團及有聯繫實體在考慮其他資料(包括可以在政府網站http://www.gld.gov.hk/chi/services_2.htm取覽的憲報刊登的任何指定爲恐怖分子的名單)，及查察有關交易的性質和所涉各方時，應連同上述的特徵清單加以考慮。如發現任何交易存在該清單所述的一項或多項因素，便可能需要加強對有關交易的審查。然而，出現其中一項因素未必表示有關交易是可疑或不尋常的。

9.6 財務行動特別組織在2002年4月發表了一份就財務機構有關偵察恐怖分子籌資活動的指引文件。 該指引文件描述恐怖分子籌資活動的一般特徵，並列出若干宗研究個案，說明執法機構曾如何藉著財務機構舉報的資料確立恐怖分子籌資活動的連繫。 該指引文件的附件1列出過往曾牽涉恐怖分子活動的財務交易的連串特徵。持牌法團或有聯繫實體應細閱該份由財務行動特別組織發出的指引文件[12]。

9.7 持牌法團及有聯繫實體應設立有效的程序，以迅速地識別出憲報公告或其已知的其他名單(例如載於美國財政部網站[13] 的根據美國總統的13224號行政命令發出的有關堵截恐怖分子財產的指定名單以及證監會發出的通函所提述的名單[14])內所指明的涉嫌恐怖分子。爲此，持牌法團及有聯繫實體應考慮將各名單綜合爲單一資料庫，以便其職員能取覽有關名單並識別出可疑交易。持牌法團及有聯繫實體應按照上述指明的涉嫌恐怖分子名單查核有否任何現有客戶及申請建立業務關係的新客戶的姓名／名稱。持牌法團及有聯繫實體應特別留意可疑的匯款，並應緊記非牟利機構在恐怖分子籌資活動中已知曾扮演的角色。若出現引起懷疑的情況，便應盡可能在處理交易前完成更嚴格的查核工作。

10. 舉報可疑交易

10.1 任何人如對其他人、交易或財產產生懷疑，他便有責任根據《販毒(追討得益)條例》、《有組織及嚴重罪行條例》或《聯合國反恐條例》作出舉報。根據《販毒(追討得益)條例》、《有組織及嚴重罪行條例》或《聯合國反恐條例》作出的可疑交易的披露，應向聯合財富情報組作出。聯合財富

12 財務行動特別組織的該份指引文件可從該組織的網站www.fatf-gafi.org/dataoecd/39/21/34033955.pdf 取覽。

13 根據美國總統行政命令發出的指定名單可在美國財政部網站www.ustreas.gov/offices/enforcement/ofac/sanctions/terrorism.html取覽。

14 有關的通函可在證監會網站www.sfc.hk/sfc/html/EN/intermediaries/supervision/supervision.html取覽。

情報組除負責接收機構或個人作出的披露外，亦是有關打擊洗黑錢的一般事宜的本地及國際顧問，並可以爲金融界就防止洗黑錢及恐怖分子籌資活動提供實際協助。

10.2 持牌法團及有聯繫實體內負責履行監察職能的負責人員(以下稱爲"合規主任")應獲委任爲機構內的中央聯絡點，從而負責向聯合財富情報組作出舉報。合規主任的職責不單是被動地接收有關可疑交易的特別舉報，而且亦需要積極參與識別及舉報可疑交易的工作，包括定期審查持牌法團或有聯繫實體的內部系統編製有關大額或不尋常交易的例外情況報告及前線職員提交的特別報告。視乎持牌法團或有聯繫實體的組織架構而定，審查有關報告的具體職責也可轉授予其他指定職員，但合規主任或有關監督管理人員應監察整個審查程序。

10.3 在若干情況下，如持牌法團或有聯繫實體的職員向合規主任舉報某宗交易，則由合規主任審查每宗個案的情況，以確定有關的懷疑是否有充分理由支持。若決定不向聯合財富情報組舉報看來是可疑的交易，合規主任應詳細記錄有關的理由。不論是否認爲可疑的交易亦涉及稅務事宜，合規主任亦應作出舉報。若出現新的可疑情況，過去曾就有關客戶過往的交易向聯合財富情報組作出舉報一事應不足以妨礙持牌法團或有聯繫實體向情報組作出新的舉報。如果可疑情況持續，便應沒有延誤地向該組舉報有關的交易。

10.4 當知道或懷疑聯合財富情報組已獲披露某項舉報，及因此有需要就有關客戶作進一步查訊時，便應格外審慎，以確保該客戶不會察覺執法機關已注意到其名稱。

10.5 證監會鼓勵按照劃一格式作出舉報(見附錄D)。如要作出緊急披露，可利用電話作出初步通知。聯合財富情報組的聯絡資料載於附錄 F。

10.6 持牌法團及有聯繫實體應備存紀錄冊，記錄所有曾向聯合財富情報組作出的，以及由僱員向管理層作出的舉報，包括管理層決定不需轉介聯合財富情報組的該等舉報。在向獲授權人(例如聯合財富情報組)舉報涉及客戶的資料的過程中，持牌法團及有聯繫實體，其董事、負責人員及僱員均不應向有關客戶作出提示，因此舉可能構成罪行。

10.7 聯合財富情報組將會認收接獲的披露。如果該組認爲無需即時採取行動(例如對某個帳戶發出限制令)，該組通常會同意

持牌法團或有聯繫實體根據《販毒(追討得益)條例》第25A(2)條或《有組織及嚴重罪行條例》第25A(2)條或《聯合國反恐條例》第12(2)條(視屬何情況而定)繼續操作該帳戶。附錄E載有該函件的樣本。

10.8 當聯合財富情報組收到及考慮過披露事項後，已披露的資料將會提供予香港警務處及香港海關內經過訓練的財富事務調查員，以便作進一步調查。

10.9 已披露的資料只限於香港警務處及香港海關內負責財富事務的調查員使用。如提出檢控，控方將會向法院申請出示令，要求將有關資料呈堂。《販毒(追討得益)條例》第26條及《有組織及嚴重罪行條例》第26條對公開根據第25A條作出披露者的身分有嚴格限制。

10.10 香港警務處、香港海關及聯合財富情報組並沒有責任必須向作出披露的持牌法團或有聯繫實體提供有關披露的最新情況報告。然而，有關的報告可應要求予以提供。

10.11 證監會認爲，加強和維持執法機構與持牌法團／有聯繫實體之間所建立的良好關係是十分重要的。

11. 職員的甄選、教育及培訓

11.1 爲遵守本指引，持牌法團及有聯繫實體應考慮到涉及洗黑錢及恐怖分子籌資活動的風險以及其本身的業務規模，採取適當的措施以甄選及培訓僱員。

11.2 持牌法團及有聯繫實體應就打擊洗黑錢及恐怖分子籌資活動而識別出其組織架構內的主要職位，並確保擔任該等主要職位的所有僱員都是履行有關職責的適合及勝任人選。

11.3 持牌法團及有聯繫實體必須向其本地及海外職員提供有關打擊洗黑錢及恐怖分子籌資活動的適當培訓。

11.4 持牌法團及有聯繫實體的職員應認識其根據《販毒(追討得益)條例》、《有組織及嚴重罪行條例》及《聯合國反恐條例》須履行的個人責任，並且認識到如果未有根據規定舉報有關資料，他們可能會因此而負上個人責任。他們應該詳細閱讀上述三條條例的有關條文。持牌法團及有聯繫實體應鼓勵其職員與聯合財富情報組通力合作，即時披露可疑的交易。如果有任何疑問，應聯絡該組。

11.5 持牌法團及有聯繫實體應推行教育計劃，以培訓所有新入職的僱員。

11.6 持牌法團及有聯繫實體須定期安排職員參與溫習培訓，確保職員(尤其是與公眾直接接觸及協助客戶開戶的職員，以及負責監督或管理這些職員的人員)不會遺忘其需履行的責任。

附錄 A：洗黑錢及恐怖分子籌資活動法例撮要

1. 《販毒(追討得益)條例》

1.1 《販毒(追討得益)條例》載有關於調查涉嫌從販毒活動所得的資產、在逮捕涉嫌罪犯後將資產凍結，以及在定罪後沒收販毒收益的條文。

1.2 《販毒(追討得益)條例》第25(1)條規定，如有人知道或有合理理由相信任何財產代表任何人的販毒收益而仍處理該財產，即屬犯罪。就“販毒”一詞的定義中所提述的財產、關乎根據第10條發出的限制令或第25條所指的罪行而言，“處理”一詞包括：-

(a) 收受或取得該財產；

(b) 隱藏或掩飾該財產(不論是隱藏或掩飾該財產的性質、來源、所在位置、處置、調動或擁有權或與其有關的任何權利或其他方面的事宜)；

(c) 處置或轉換該財產；

(d) 把該財產運入香港或調離香港；

(e) 以該財產借款或作保證(不論是藉押記、按揭或質押或其他方式)。

該項罪行經定罪後的最高刑罰爲監禁14年及罰款500萬元。根據第25(1)條，任何人如能證明他曾意圖根據第25A條作出披露，以及對未能作出披露有合理解釋，則可以此作爲免責辯護。

1.3 根據《販毒(追討得益)條例》第25A條，凡任何人知道或懷疑任何財產

(a) 是直接或間接代表任何人的販毒收益，

(b) 曾在與販毒有關的情況下使用，或

(c) 擬在與販毒有關的情況下使用，

該人須在合理範圍內盡快把該知悉或懷疑向獲授權人披露。“獲授權人”包括警務人員、香港海關的人員，以及聯合財富情報組。聯合財富情報組於1989年成立，並由香港警務處及香港海關聯合運作。《販毒(追討得益)條例》第25A(4)條規定，任何人如在有關時間內是受僱的，則該人可按其僱主爲作出披露所定下的程序，向適當人士作出披露(請參閱本指引第10節)。對該僱員而言，作出上述披露等同於根據第25A(1)條向獲授權人披露有關的知悉或懷疑。如未能根據第25A條的規定作出披露，即屬犯罪。該罪行經定罪後的最高刑罰爲罰款5萬元及監禁3個月。

1.4 《販毒(追討得益)條例》第25A(2)條規定，已作出第25A(1)條所指作出披露的人，如在作出該項披露之前或之後作出任何違反第25(1)條的作爲，而該項披露與該作爲有關，則只要符合以下條件，該人並沒有觸犯第25(1)條所訂的罪行：-

(a) 該項披露是在他作出該作爲之前作出的，而且他作出該作爲是得到獲授權人的同意的；或

(b) 該項披露是在他作出該作爲之後作出的；是由他主動作出的；及是他在合理範圍內盡快作出的。

1.5 根據《販毒(追討得益)條例》第25A(5)條，任何人如知道或懷疑已有任何披露根據第25A(1)或(4)條作出，而仍向其他人披露任何相當可能會損害或者會爲跟進第25A(1)或(4)條下的披露而進行的調查的事宜，即屬犯罪。該罪行經定罪後的最高刑罰爲罰款50萬元及監禁3年。

1.6 《販毒(追討得益)條例》第25A(3)(a)條規定，根據該條例作出的披露，不得視爲違反合約或任何成文法則、操守規則或其他條文對披露資料所施加的任何規限。第25A(3)(b)條則規定，作出披露的人，毋須就該

項披露或該項披露所引致的就有關財產所作出的任何作爲或不作爲而引致的任何損失，負上支付損害賠償的法律責任。

1.7 持牌法團及有聯繫實體可能會就被控販毒的某被告人的財產而接獲限制令及押記令。這些命令是依據《販毒(追討得益)條例》第10及11條的規定發出的。經送達這些命令，獲授權人可要求任何人交付可能有助釐定有關財產的價值的文件或資料。根據《販毒(追討得益)條例》第10及11條，任何人未有在切實可行的範圍內盡快提供有關文件或資料，即屬犯罪。此外，根據《販毒(追討得益)條例》，任何人違反限制令或押記令而處理有關的財產，即屬犯罪。

1.8 《販毒(追討得益)條例》第26條規定，除非所檢控的是該條例第25、25A或26條所指的罪行，或法庭認爲必須公開該項披露或披露人的身分，方能在各當事人之間秉行公正，否則在任何民事或刑事法律程序中，不得迫使任何證人公開有人曾經作出披露，或公開披露人的身分。

2. 《有組織及嚴重罪行條例》

2.1 《有組織及嚴重罪行條例》(除其他事項外)：

(a) 賦予香港警務處及香港海關調查有組織罪行及三合會活動的權力；

(b) 賦予法院司法權，沒收來自有組織及嚴重罪行的收益，以及就被控觸犯《有組織及嚴重罪行條例》所指罪行的被告人的財產發出限制令及押記令；

(c) 增訂一項有關來自可公訴罪行的收益的洗黑錢罪行；及

(d) 容許法院在適當的情況下接收有關違法者及有關罪行的資料，以決定當有關罪行構成有組織

／有關三合會的罪行或其他嚴重罪行時，是否適宜作出更嚴厲的判決。

“有組織罪行”一詞在《有組織及嚴重罪行條例》中具有廣泛的定義。簡單來說，有組織罪行指《有組織及嚴重罪行條例》附表1所列明的罪行，而這些罪行與某三合會的活動相關，或由2名或以上的人所犯並涉及相當程度的策劃及組織。附表1所列明的罪行包括謀殺、綁架、販毒、襲擊、強姦、盜竊、打劫、以欺騙手段取得財產、僞造帳目、軍火罪行、誤殺、貪污及走私等。

2.2 《有組織及嚴重罪行條例》第3至5條規定，獲授權人(包括香港警務處)可以爲偵查有組織罪行，向原訟法庭申請頒令，命令某人提供資料或提交物料，而有關的資料及物料是合理地看來關乎該項偵查的。此外，法庭亦可命令某人向獲授權人提供有關的物料，而獲授權人亦可根據《有組織及嚴重罪行條例》申請搜查令。任何人不得以提供資料或提交物料會使該人被入罪或會違反法規或其他規則或規例所施加的保密責任或對披露資料或物料的其他限制爲理由，而拒絕根據《有組織及嚴重罪行條例》第3及4條的規定提供資料或提交物料。

2.3 《有組織及嚴重罪行條例》第25、25A及26條是參照《販毒(追討得益)條例》第25、25A及26條而制訂的。扼要來說，根據《有組織及嚴重罪行條例》第25(1)條，如有人知道或有合理理由相信任何財產代表任何人從可公訴罪行獲得的收益而仍處理該財產，即屬犯罪。就該條所指的財產而言，“處理”一詞包括：-

(a) 收受或取得該財產；

(b) 隱藏或掩飾該財產(不論是隱藏或掩飾該財產的性質、來源、所在位置、處置、調動或擁有權或與其有關的任何權利或其他方面的事宜)；

(c) 處置或轉換該財產；

(d) 把該財產運入香港或調離香港；

(e) 以該財產借款或作保證(不論是藉押記、按揭或質押或其他方式)。

第25條所指的罪行經定罪後的最高刑罰爲罰款500萬元及監禁14年。根據第25(1)條，任何人如能證明他曾意圖根據第25A條作出披露，以及對未能作出披露有合理解釋，則可以此作爲免責辯護。

2.4 根據《有組織及嚴重罪行條例》第25A條，凡任何人知道或懷疑任何財產

(a) 是直接或間接代表任何人從可公訴罪行的收益，

(b) 曾在與可公訴罪行有關的情況下使用，或

(c) 擬在與可公訴罪行有關的情況下使用，

該人須在合理範圍內盡快把該知悉或懷疑向獲授權人披露。如未能根據規定作出披露，即屬犯罪。如任何人在有關時間內是受僱的，則該人可按其僱主爲作出披露所定下的程序，向適當的人士作出披露。該項罪行經定罪後的最高刑罰爲罰款5萬元及監禁3個月。

2.5 《有組織及嚴重罪行條例》第25A(2)條規定，已作出第25A(1)條所指披露的人，如在作出該項披露之前或之後作出任何違反第25(1)條的作爲，而該項披露與該作爲有關，則只要符合以下條件，該人並沒有觸犯第25(1)條所訂的罪行：-

(a) 該項披露是在他作出該作爲之前作出的，而且他作出該作爲是得到獲授權人的同意的；或

(b) 該項披露是在他作出該作爲之後作出的；是由他主動作出的；及是他在合理範圍內盡快作出的。

2.6 根據《有組織及嚴重罪行條例》第25A(5)條，任何人如知道或懷疑已有任何披露根據第25A(1)或(4)條作出，而仍向其他人披露任何相當可能會損害或者會爲跟進第25A(1)或(4)條下的披露而進行的調查的事宜，即屬犯罪。該項罪行經定罪後的最高刑罰爲罰款50萬元及監禁3年。

2.7 《有組織及嚴重罪行條例》第25A(3)(a)條規定，根據該條例作出的披露，不得視爲違反合約或任何成文法則、操守規則或其他條文對披露資料所施加的任何限制。第25A(3)(b)條則規定，作出披露的人，毋須就該項披露或該項披露所引致的就有關財產所作出的任何作爲或不作爲而引致的任何損失，負上支付損害賠償的法律責任。

2.8 持牌法團及有聯繫實體可能會就被控犯有《有組織及嚴重罪行條例》的某被告人的財產而接獲限制令及押記令。這些命令是依據《有組織及嚴重罪行條例》第15及16條的規定發出的。經送達這些命令，獲授權人可要求任何人交付可能有助釐定有關財產的價值的文件或資料。根據《有組織及嚴重罪行條例》第15及16條，任何人未有在切實可行的範圍內盡快提供有關資料，即屬犯罪。此外，根據《有組織及嚴重罪行條例》，任何人違反限制令或押記令而處理有關的財產，即屬犯罪。

2.9 《有組織及嚴重罪行條例》第26條規定，除非所檢控的是該條例第25、25A或26條所訂的罪行，或法庭認爲必須公開該項披露或披露人的身分，方能在各當事人之間秉行公正，否則在任何民事或刑事法律程序中，不得迫使任何證人公開有人曾作出披露，或公開披露人的身分。

3. 《聯合國(反恐怖主義措施)條例》("《聯合國反恐條例》")

3.1 《聯合國反恐條例》在2002年7月制定，當中大部分條文自2002年8月23日起實施。該條例主要旨在實施聯合國安全理事會2001年9月28日第1373號決議中關於防止

恐怖主義行爲的籌資活動的決定。聯合國安全理事會過往曾通過多項其他決議，從而對若干指定的恐怖分子及恐怖組織施加制裁。根據《聯合國制裁條例》(第537章)頒布的規例，使這些由聯合國安全理事會作出的決議得以實施。《聯合國制裁(阿富汗)規例》及《聯合國制裁(阿富汗) (修訂)規例》(除其他事項外)特別禁止向指定的恐怖分子提供資金。《聯合國反恐條例》則針對所有恐怖分子。

3.2 《聯合國(反恐怖主義措施)(修訂)草案》在2004年6月獲得通過，而《2004年聯合國(反恐怖主義措施)(修訂)條例》的大部分條文亦自2005年1月起實施。

3.3 除了聯合國安全理事第1373號決議中的強制措施外，根據《2004年聯合國(反恐怖主義措施)(修訂)條例》("《修訂條例》")作出修改的《聯合國反恐條例》亦實施財務行動特別組織頒布有關恐怖分子籌資活動的特別建議中某些更重要的建議。《修訂條例》(除其他事項外)訂明，向恐怖分子或與恐怖分子有聯繫者供應或收集資金及向他們提供資金或金融(或有關的)服務，均屬違法。該條例容許將恐怖分子財產凍結及充公。《修訂條例》第12(1)條亦規定，任何人如知悉或懷疑任何財產是恐怖分子財產，該人須向獲授權人(包括《修訂條例》所指明的警務人員、香港海關／入境事務處成員及廉政公署人員)作出披露。如未能根據規定作出披露，即屬犯罪。該項罪行經定罪後的最高刑罰爲罰款5萬元及監禁3個月。

3.4 在《修訂條例》中，"資金"一詞包括《修訂條例》附表1所述的各類資金。該詞涵蓋現金、支票、存於財務機構或其他實體的存款、帳戶結餘、證券及債務票據(包括股額及股份、代表證券的證明書、債券、票據、權證、債權證、債權股證及衍生工具合約)、利息、股息，或財產上的其他收入或自財產累算或產生的價值、資金或財務資源的權益的證明文件等。

3.5 "恐怖分子"指作出或企圖作出恐怖主義行爲或參與或協助作出恐怖主義行爲的人。"與恐怖分子有聯繫者"

則指由恐怖分子直接或間接擁有或控制的實體。“恐怖主義行爲”指作出或恐嚇作出行動，而該行動是懷有達致以下結果的意圖而進行的，或該恐嚇的意圖是採取行動以達致出現以下結果的效果：

(a) 導致針對人的嚴重暴力；

(b) 導致對財產的嚴重損害；

(c) 危害作出該行動以外的人的生命；

(d) 對公眾人士或部分公眾人士的健康或安全造成嚴重危險；

(e) 嚴重干擾或嚴重擾亂電子系統；或

(f) 嚴重干擾或嚴重擾亂基要服務、設施或系統(不論是公共或私人的)；及

該行動的作出或該恐嚇：

(i) 的意圖是強迫特區政府或威嚇公眾人士或部分公眾人士的；及
(ii) 是爲推展政治、宗教或思想上的主張而進行的。

如屬以上(d)、(e)及(f)段的情況，“恐怖主義行爲”不包括在任何宣揚、抗議、持異見或工業行動的過程中作出或恐嚇作出行動。

3.6 特區政府不時根據《聯合國制裁(阿富汗)規例》第10條及《修訂條例》第4條的規定，在憲報刊登被指定的恐怖分子、與恐怖分子有聯繫者及恐怖分子財產的名單。已刊登的名單列出了根據聯合國安全理事會第1267號決議案成立的聯合國委員會所指定的人士或實體。《修訂條例》規定，在沒有相反證據的情況下，則假定該名單列名的人士或實體爲恐怖分子或與恐怖分子有聯繫者(視屬何情況而定)。

3.7 就《修訂條例》第12(1)條所訂有關在知悉或懷疑任何財產是恐怖分子財產後作出披露的責任而言，應注意若任何已作出該項披露的人，在作出該項披露之前或之後作出任何違反第7或8條(即有關向恐怖分子或其有聯繫者供應或收集資金或提供資金或金融(或有關的)服務的條文)的作爲，而該項披露與該作爲有關，則只要符合以下條件，該人並沒有觸犯罪行：

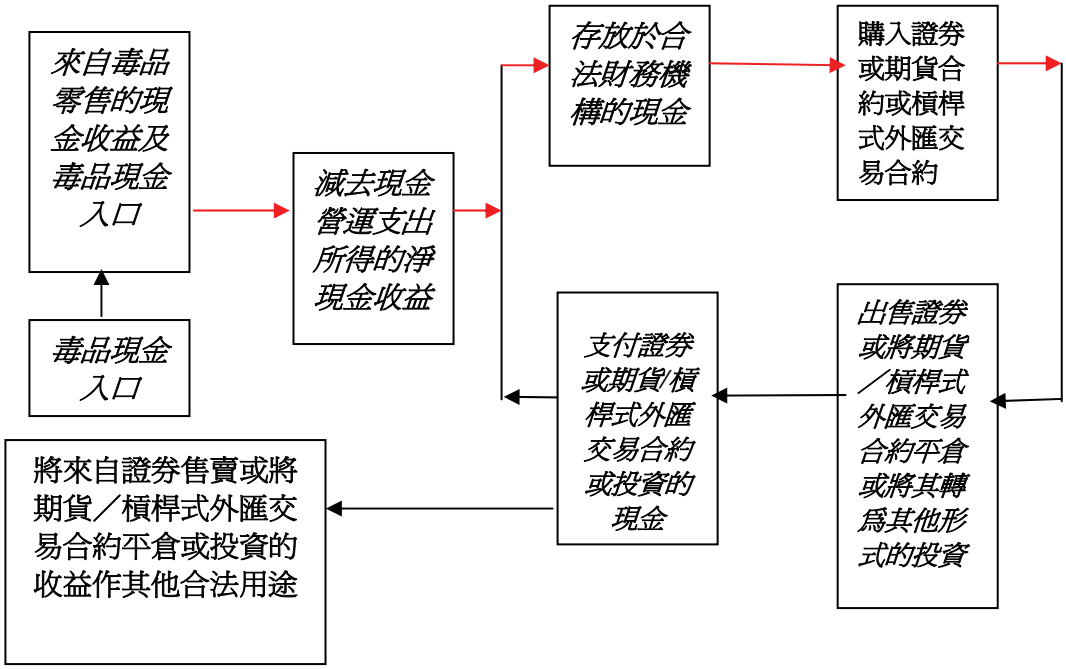
(a) 該項披露是在他作出該作爲之前作出的，而且他作出該作爲是得到獲授權人的同意的；或

(b) 該項披露是在他作出該作爲之後作出的；是由他主動作出的；及是他在合理範圍內盡快作出的。

3.8 《修訂條例》第12(3)條規定，根據該條例作出的披露，不得視爲違反合約或任何成文法則、操守規則或其他條文對披露資料所施加的任何限制。作出披露的人，亦毋須就該項披露或該項披露所引致的就有關財產所作出的任何作爲或不作爲而引致的任何損失，負上支付損害賠償的法律責任。

3.9 《修訂條例》第12(6)條允許獲授權人向負責調查或防止及遏止資助恐怖主義行爲的若干主管當局(即律政司、香港警務處等)及海外主管當局披露其根據第12(1)條取得的資料。

附錄B：洗黑錢的過程



聯合財富情報組網站(www.jfiu.gov.hk) 及財務行動特別組織網站(www.fatf-gafi.org)載有洗黑錢方法的其他例子及顯示與恐怖分子籌資活動有關的財務交易特徵的詳情。

附錄C(i)：聯合財富情報組建議的識別可疑交易的有系統方法

以下爲設立一個能有效地識別可疑金融活動的有系統方法所需的四個步驟。

(a) **第一步**： 識別一項或多項有關可疑金融活動的指標。

(b) **第二步**： 向客戶作出恰當的提問。

(c) **第三步**： 審查有關客戶的已知資料，以判斷客戶是否如預期一樣會從事該宗看來是可疑的活動。

(d) **第四步**： 綜合上述(a)、(b)、(c)的結果，然後就客戶的金融活動是否真正可疑作出決定。

聯合財富情報組在研究以往接獲的可疑交易舉報中，發現許多舉報機構都沒有採取如上述建議的步驟，而僅在識別到可疑活動的某項指標後便即時舉報；換言之，他們只採取該套有系統方法的步驟(a)，而忽略其餘(b)、(c)和(d)等步驟，導致可疑交易舉報的素質未如理想。

識別可疑活動的有系統方法的四個步驟將會逐一在下文詳細討論。若干該等建議措施或程序未必適用於所有情況。各持牌法團或有聯繫實體在設計本身的制度以落實有關步驟時，應仔細考慮其業務性質、組織結構、客戶及交易種類等因素。

第一步： 識別一項或多項有關可疑金融活動的指標

識別一項(或以上則更佳)有關可疑金融活動的指標是建立可疑活動識別系統的第一步。本港證券業常見可疑活動的指標載於附錄C(ii)。

我們亦須利用其他監察客戶活動的方法，以找出可疑活動的指標。

以下概述的措施，都公認爲有效地識別可疑活動的整體方法：

(a) 提供訓練、維持各級職員識別可疑活動的警覺性。

在某些情況下，倘若一名客戶從事出現可疑活動指標的交易時，職員跟該名客戶有直接會面，則這項方法最爲有效。然而，當職員與客戶並無直接會面，又或客戶進行連串交易，且每宗交易均選擇不同的職員辦理，令個別交易

看來並無可疑，則這項方法所帶來的效果卻可能會大打折扣。

(b) 找出職員與客戶無須透過直接會面而接觸的交易類別(例如網上交易)，並採用額外方法，以識別這類可疑活動。

(c) 以電腦程式鑑認哪些帳戶的活動與電腦內所預設常見洗黑錢的方法資料相同。

(d) 監察帳戶的交易趨勢。以電腦程式監察某帳戶的成交額，並以其最近數月平均每月所累積的成交額，與當前月份的成交額作一比較；若當前月份的成交額較過往的平均成交額大幅提高，則當前月份的活動應視爲可疑。

(e) 商號內部的視察制度應包括查核職員向當局舉報可疑活動的情況。

(f) 識別"高風險"帳戶，即通常會被人用作洗黑錢的帳戶，例如匯款公司、貨幣兌換商和賭場的帳戶，以及以秘書服務公司的職員爲獲授權簽署人的帳戶、空殼公司的帳戶和律師行爲客戶而設的帳戶等。職員要更密切留意這些帳戶的活動，以防範可疑的交易。

(g) 在商號的電腦上替一些特別令人關注的帳戶標上記號。職員日後處理客戶的交易，當在電腦屏幕上發現這些記號時，便會格外留意有關帳戶所進行的交易。一些曾被舉報有可疑交易和/或涉及高風險業務的帳戶(見上文(f)段的詮釋)，都須標上記號。

然而，在帳戶標上記號會出現另一問題，就是當職員看見一個標有記號的帳戶涉及一宗大額交易時，無論可疑與否，他們會傾向馬上向合規主任舉報，以致合規主任接獲許多並無實質價值的報告，令工作倍添繁重。此外，標上記號的方法也會導致職員以爲沒有標上記號的帳戶便無可疑。因此，要使這個方法行之有效，商號方面便須教導職員如何正確使用有關記號。

(h) 利用"例外情況報告"、"不尋常情況報告"或"頻密交易活動報告"識別出進行頻密交易活動的帳戶，並從而考慮有關活動是否可疑。雖然，這些報告對於職員識別可疑活動也有幫助，但商號在設計這些報告時，其真正目的並非如此，因此，所得的效果亦可能會未如想象中的理想。例

如：商號主管爲了讓每天審閱這些報告的數量維持在可處理的水平之內，會把職員每天須呈報可疑交易的金額訂得比洗黑錢人士一般會清洗的數目還高，結果這些報告便不能有效地識別到可疑活動。

(i) 對一些可能會進行大額款項交易的客戶，採取更爲嚴謹的措施。例如：商號替一些公司客戶開立帳戶時，應要求他們提供日後交易的性質及其款項來源等資料。

第二步： 向客戶作出恰當的提問

持牌法團或有聯繫實體的職員若接獲執行一宗或多宗交易的指示，當中又出現一項或多項可疑活動的指標時，便應向該名客戶查詢進行該等交易的原因，以及交易中那些款項的來源和最終受益人的身分；職員應就其對有關金融活動的觀察所得，考慮客戶所作的解釋是否合情合理，如否，便應將該客戶的活動視爲可疑，並須向聯合財富情報組舉報有關可疑交易。

曾有財務機構的職員表示，不大願意向客戶查詢上述的問題，理由是客戶可能覺得他/她被人懷疑進行非法活動，或者認爲職員的提問與其工作無關；在這些情況下，客戶可能感到不快，產生戒心並採取不合作的態度，甚至將其交易活動轉往別處辦理。誠然，這種情況確實值得關注，但這些問題卻不是無法解決的。財務機構的職員只要向客戶提出一些問題，而這些問題看來都是爲了向客戶推介服務或滿足其需要而提出的，都可以使他們放下戒心，並取得如上文所述問題的答案。

當發現顯示可疑活動指標的交易時，爲了取得客戶從事該宗可疑交易的原因，我們必須視乎每宗金融活動的實際情況而向客戶作出恰當的提問。例如，客戶如欲進行一筆大額的現金交易，財務機構的職員便可藉著爲客戶提供更安全的交易方法的理由，而向其提問以現金交易的原因。

一般來說，從事正當生意的客戶都不會拒絕，或毫不猶疑地回答問題。反之，從事不法活動的客戶很有可能不願作答，或者以三言兩語予以敷衍，甚至給予令人難以置信的解釋。

客戶如不願或拒絕回答問題，又或給予令有關職員懷疑是不盡不實的答覆，都進一步顯示有關金融活動的性質可疑。

第三步：　審查有關客戶的已知資料，以判斷客戶是否如預期一樣會從事該宗看來是可疑的活動。

識別可疑活動的有系統方法的第三個步驟是，審查持牌法團或有聯繫實體對有關客戶的已知資料及其過往的金融活動，再經綜合考慮後，決定客戶是否如所預期一樣會從事該宗看來可疑的活動。這步驟一般稱之爲“認識客戶的原則”。

持牌法團及有聯繫實體(如適用的話)如擁有客戶各項資料，在考慮客戶的金融活動是否如預期一樣，還是屬於不尋常時便很有幫助。這些資料的部分例子及從中所得的結論現列舉如下：

(a) 客戶的職業：某些職業意味著客戶可能屬低收入人士，例如司機、小販、侍應生、學生等。因此，這些人士的帳戶都不應有涉及巨額的交易。

(b) 客戶的住址：若客戶報稱的住址是位於租金低廉的屋邨，例如公共屋邨，這顯示該客戶可能屬低收入人士。

(c) 客戶的年齡：無論年少還是年邁者通常都不會涉及經常性的巨額交易。這些人士的帳戶都不應出現這類活動。

(d) 帳戶在一段期間內出現的平均結餘、交易次數及類別，都可顯示客戶在正常情況下可能從事的金融活動。因此，交易顯著增加或交易形式異常，均可視爲不尋常的活動。

第四步： 客戶的金融活動是否可疑？

識別可疑活動的有系統方法的最後一個步驟是決定應否舉報有關的可疑交易。一宗交易是否可疑實在難以作出實質界定，因此我們不可能就應在何種情況下舉報或不應舉報給予明確的指引。然而，決策者若已掌握並考慮過一切有關情況，也就是說，他們已採取並考慮過前文所述識別可疑交易系統的首三個步驟，其最終決定應是最佳的決定。因此，職員若考慮過所有的情況後，發現有關活動真正可疑，便應向當局舉報。

附錄C(ii)：可疑交易的例子

<u>透過與投資有關的交易進行的洗黑錢活動</u>

(a) 以現金或不記名方式交收的大額或不尋常的交易。

(b) 並無明顯目的或在看來是不尋常的情況下進行的證券／期貨買賣。

(c) 與同一個對手方進行的多宗涉及相同證券的小額交易，而每次均用現金購買，然後再一次過將其售賣，但售賣所得款項則存入另一個帳戶。

(d) 任何與身分不明的對手方進行的交易，或其交易性質、規模或頻密程度看來不尋常。

(e) 由海外銀行、聯屬公司或其他投資者介紹的投資者，而該投資者及介紹人所在的國家，均有著嚴重的毒品生產和販毒問題。

(f) 客戶利用持牌法團或有聯繫實體代其持有資金，但有關資金卻並非用來買賣證券，期貨合約或槓桿式外匯交易合約。

(g) 客戶與持牌法團或有聯繫實體交易時，只使用現金或等同於現金的金融工具，而非透過銀行體系進行交易。

(h) 就某些證券或期貨或槓桿式外匯交易合約進行數量相同的買賣("清洗交易"或"虛假售賣")，從而營造曾進行交易的假像。這種清洗交易並非真正的市場交易，而可能只是爲洗黑錢的人士提供"掩飾"。

(i) 透過不同帳戶進行的清洗交易，將可用作抵銷不同帳戶之間的盈虧，從而在不同帳戶之間調動資金。此外，在並非屬同一人控制的帳戶之間進行轉倉，亦可能是涉及洗黑錢的警告信號。(應注意的是清洗交易亦顯示出現操縱市場活動，持牌法團或註冊人應採取適當步驟，以確保有妥善的預防措施，防止導致它作出構成《證券及期貨條例》第279條所指的市場失當行爲的方式行事。)

(j) 與未經核證或難以核證的第三者有頻繁的資金調撥或支票付款活動。

(k) 涉及透過離岸公司的帳戶進行多次調撥，尤其是有關的資金是調撥至避稅天堂，或是轉帳至某些根據海外法例註冊成立的公司名下的帳戶，而有關客戶可能是該等公司的股東。

(l) 透過非居民帳戶進行大額提存，並繼而將資金調撥至離岸金融中心。

<u>涉及持牌法團及有聯繫實體的僱員的洗黑錢活動</u>

(a) 僱員的作風有變，例如生活奢華或不願休假。

(b) 僱員或代理人的業績有變，例如藉售賣投資產品以收取現金的營業員的業績，出現顯著或預期以外的增幅。

(c) 沒有依照有關業務的正常程序，披露代理人所進行的交易的最終實益擁有人或對手方的身分。

(d) 客戶所使用的地址並非其永久地址，例如使用其代表的公司地址或住址，以供送遞客戶文件之用。

(e) 客戶要求公司提供投資管理服務(例如外幣、證券或期貨)，而有關資金來源不明或與客戶表面的地位不相符。

附錄D：向聯合財富情報組作出的舉報

根據《販毒(追討得益)條例》 或《有組織及嚴重罪行條例》第25A條 或《聯合國(反恐怖主義措施)條例》第12條 向聯合財富情報組作出的舉報		
持牌法團或有聯繫實體的名稱及地址		
可疑帳戶的名稱 (全名)		
開戶日期		出生日期／註冊成立日期 (如屬公司客戶)
職業及僱主／業務性質 (如屬公司客戶)		
國籍／註冊成立地(如屬公司客戶)		香港身分證號碼／護照號碼／商業登記證號碼 (如屬公司客戶)
帳戶持有人的地址		
引起懷疑的交易／財產的詳情及其他有關資料。請提供交易文件及帳戶結單的副本作參考。帳戶持有人或進行交易者的詳細資料，請以另紙說明		
作出舉報的職員／電話號碼	簽署／日期	已輸入的紀錄

附錄E：聯合財富情報組的認收函件樣本

貴方檔號：

〔　　〕先生
ABC 證券有限公司
〔地址〕

敬啓者：

《販毒(追討得益)條例》
《有組織及嚴重罪行條例》
《聯合國(反恐怖主義措施)條例》

你在XX年X月X日向聯合財富情報組作出的上述檔號的披露收悉。

我確認收到你根據《販毒(追討得益)條例》(第405章)第25A條及《有組織及嚴重罪行條例》(第455章)第25A條／《聯合國(反恐怖主義措施)條例》(第575章)第12條所提供的資料。

按照目前所得的資料，本組現同意你根據上述條例的規定，依照正常的證券／期貨／槓桿式外匯交易手法，繼續操作上述帳戶。

對於你給予的合作，謹此致謝。

聯合財富情報組
〔日期〕

附錄F：聯合財富情報組的聯絡資料

請將書面報告送往聯合財富情報組的以下地址、傳真號碼、電郵地址或郵政信箱：

香港軍器廠街警察總部警政大樓西翼16樓聯合財富情報組

或　　香港郵政總局信箱 6555 號

傳真　：2529-4013

電郵　：jfiu@police.gov.hk

緊急舉報請以傳真或電郵方式提交，或致電 2860-3413 或 2866-3366。

STATUTORY INSTRUMENTS

2007 No. 2157

FINANCIAL SERVICES

The Money Laundering Regulations 2007

Made - - - -	*24th July 2007*
Laid before Parliament	*25th July 2007*
Coming into force - -	*15th December 2007*

The Treasury are a government department designated(**a**) for the purposes of section 2(2) of the European Communities Act 1972(**b**) in relation to measures relating to preventing the use of the financial system for the purpose of money laundering;

The Treasury, in exercise of the powers conferred on them by section 2(2) of the European Communities Act 1972 and by sections 168(4)(b), 402(1)(b), 417(1)(**c**) and 428(3) of the Financial Services and Markets Act 2000(**d**), make the following Regulations:

PART 1

GENERAL

Citation, commencement etc.

1.—(1) These Regulations may be cited as the Money Laundering Regulations 2007 and come into force on 15th December 2007.

(2) These Regulations are prescribed for the purposes of sections 168(4)(b) (appointment of persons to carry out investigations in particular cases) and 402(1)(b) (power of the Authority to institute proceedings for certain other offences) of the 2000 Act.

(a) S.I. 1992/1711.

(b) 1972 c. 68; section 2(2) was amended by section 27 of the Legislative and Regulatory Reform Act 2006 (c.51). By virtue of the amendment of section 1(2) made by section 1 of the European Economic Area Act 1993 (c.51) regulations may be made under section 2(2) to implement obligations of the United Kingdom created by or arising under the Agreement on the European Economic Area signed at Oporto on 2nd May 1992 (Cm 2073, OJ No L 1, 3.11.1994, p. 3) and the Protocol adjusting that Agreement signed at Brussels on 17th March 1993 (Cm 2183, OJ No L 1, 3.1.1994, p.572). For the decision of the EEA Joint Committee in relation to Directive 2005/60/EC, see Decision No 87/2006 of 7th July 2006 amending Annex IX (Financial Services) to the EEA Agreement (OJ No L 289 19.10.2006, p. 23).

(c) See the definition of "prescribed".

(d) 2000 c. 8.

(3) The Money Laundering Regulations 2003(**e**) are revoked.

Interpretation

2.—(1) In these Regulations—

"the 2000 Act" means the Financial Services and Markets Act 2000;

"Annex I financial institution" has the meaning given by regulation 22(1);

"auditor", except in regulation 17(2)(c) and (d), has the meaning given by regulation 3(4) and (5);

"authorised person" means a person who is authorised for the purposes of the 2000 Act(**f**);

"the Authority" means the Financial Services Authority;

"the banking consolidation directive" means Directive 2006/48/EC of the European Parliament and of the Council of 14th June 2006 relating to the taking up and pursuit of the business of credit institutions(**g**);

"beneficial owner" has the meaning given by regulation 6;

"business relationship" means a business, professional or commercial relationship between a relevant person and a customer, which is expected by the relevant person, at the time when contact is established, to have an element of duration;

"cash" means notes, coins or travellers' cheques in any currency;

"casino" has the meaning given by regulation 3(13);

"the Commissioners" means the Commissioners for Her Majesty's Revenue and Customs;

"consumer credit financial institution" has the meaning given by regulation 22(1);

"credit institution" has the meaning given by regulation 3(2);

"customer due diligence measures" has the meaning given by regulation 5;

"DETI" means the Department of Enterprise, Trade and Investment in Northern Ireland;

"the electronic money directive" means Directive 2000/46/EC of the European Parliament and of the Council of 18th September 2000 on the taking up, pursuit and prudential supervision of the business of electronic money institutions(**h**);

"estate agent" has the meaning given by regulation 3(11);

"external accountant" has the meaning given by regulation 3(7);

"financial institution" has the meaning given by regulation 3(3);

"firm" means any entity, whether or not a legal person, that is not an individual and includes a body corporate and a partnership or other unincorporated association;

"high value dealer" has the meaning given by regulation 3(12);

"the implementing measures directive" means Commission Directive 2006/70/EC of 1st August 2006 laying down implementing measures for the money laundering directive(**i**);

"independent legal professional" has the meaning given by regulation 3(9);

"insolvency practitioner", except in regulation 17(2)(c) and (d), has the meaning given by regulation 3(6);

"the life assurance consolidation directive" means Directive 2002/83/EC of the European Parliament and of the Council of 5th November 2002 concerning life assurance(**j**);

(e) S.I. 2003/3075.

"local weights and measures authority" has the meaning given by section 69 of the Weights and Measures Act 1985(**k**) (local weights and measures authorities);

"the markets in financial instruments directive" means Directive 2004/39/EC of the European Parliament and of the Council of 12th April 2004(**l**) on markets in financial instruments;

"money laundering" means an act which falls within section 340(11) of the Proceeds of Crime Act 2002(**m**);

"the money laundering directive" means Directive 2005/60/EC of the European Parliament and of the Council of 26th October 2005(**n**) on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing;

"money service business" means an undertaking which by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or cashes cheques which are made payable to customers;

"nominated officer" means a person who is nominated to receive disclosures under Part 7 of the Proceeds of Crime Act 2002(**o**) (money laundering) or Part 3 of the Terrorism Act 2000(**p**) (terrorist property);

"non-EEA state" means a state that is not an EEA state;

"notice" means a notice in writing;

"occasional transaction" means a transaction (carried out other than as part of a business relationship) amounting to 15,000 euro or more, whether the transaction is carried out in a single operation or several operations which appear to be linked;

"the OFT" means the Office of Fair Trading;

"ongoing monitoring" has the meaning given by regulation 8(2);

"regulated market"—

(a) within the EEA, has the meaning given by point 14 of Article 4(1) of the markets in financial instruments directive; and

(b) outside the EEA, means a regulated financial market which subjects companies whose securities are admitted to trading to disclosure obligations which are contained in international standards and are equivalent to the specified disclosure obligations;

"relevant person" means a person to whom, in accordance with regulations 3 and 4, these Regulations apply;

"the specified disclosure obligations" means disclosure requirements consistent with—

(a) Article 6(1) to (4) of Directive 2003/6/EC of the European Parliament and of the Council of 28th January 2003(**q**) on insider dealing and market manipulation;

(b) Articles 3, 5, 7, 8, 10, 14 and 16 of Directive 2003/71/EC of the European Parliament and of the Council of 4th November 2003(**r**) on the prospectuses to be published when securities are offered to the public or admitted to trading;

(c) Articles 4 to 6, 14, 16 to 19 and 30 of Directive 2004/109/EC of the European Parliament and of the Council of 15th December 2004(**s**) relating to the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market; or

(d) Community legislation made under the provisions mentioned in sub-paragraphs (a) to (c);

"supervisory authority" in relation to any relevant person means the supervisory authority specified for such a person by regulation 23;

"tax adviser" (except in regulation 11(3)) has the meaning given by regulation 3(8);

"terrorist financing" means an offence under—

(a) section 15 (fund-raising), 16 (use and possession), 17 (funding arrangements), 18 (money laundering) or 63 (terrorist finance: jurisdiction) of the Terrorism Act 2000;

(b) paragraph 7(2) or (3) of Schedule 3 to the Anti-Terrorism, Crime and Security Act 2001(**t**) (freezing orders);

(c) article 7, 8 or 10 of the Terrorism (United Nations Measures) Order 2006(**u**); or

(d) article 7, 8 or 10 of the Al-Qaida and Taliban (United Nations Measures) Order 2006(**v**);

"trust or company service provider" has the meaning given by regulation 3(10).

(2) In these Regulations, references to amounts in euro include references to equivalent amounts in another currency.

(3) Unless otherwise defined, expressions used in these Regulations and the money laundering directive have the same meaning as in the money laundering directive and expressions used in these Regulations and in the implementing measures directive have the same meaning as in the implementing measures directive.

Application of the Regulations

3.—(1) Subject to regulation 4, these Regulations apply to the following persons acting in the course of business carried on by them in the United Kingdom ("relevant persons")—

(a) credit institutions;

(b) financial institutions;

(c) auditors, insolvency practitioners, external accountants and tax advisers;

(d) independent legal professionals;

(e) trust or company service providers;

(f) estate agents;

(g) high value dealers;

(h) casinos.

(2) "Credit institution" means—

(a) a credit institution as defined in Article 4(1)(a) of the banking consolidation directive; or

(b) a branch (within the meaning of Article 4(3) of that directive) located in an EEA state of an institution falling within sub-paragraph (a) (or an equivalent institution whose head office is located in a non-EEA state) wherever its head office is located,

when it accepts deposits or other repayable funds from the public or grants credits for its own account (within the meaning of the banking consolidation directive).

(3) "Financial institution" means—

(a) an undertaking, including a money service business, when it carries out one or more of the activities listed in points 2 to 12 and 14 of Annex 1 to the banking consolidation directive (the relevant text of which is set out in Schedule 1 to these Regulations), other than—

(i) a credit institution;

(ii) an undertaking whose only listed activity is trading for own account in one or more of the products listed in point 7 of Annex 1 to the banking consolidation directive where the undertaking does not have a customer,

and, for this purpose, "customer" means a third party which is not a member of the same group as the undertaking;

(b) an insurance company duly authorised in accordance with the life assurance consolidation directive, when it carries out activities covered by that directive;

(c) a person whose regular occupation or business is the provision to other persons of an investment service or the performance of an investment activity on a professional basis, when providing or performing investment services or activities (within the meaning of the markets in financial instruments directive(**w**)), other than a person falling within Article 2 of that directive;

(d) a collective investment undertaking, when marketing or otherwise offering its units or shares;

(e) an insurance intermediary as defined in Article 2(5) of Directive 2002/92/EC of the European Parliament and of the Council of 9th December 2002(**x**) on insurance mediation, with the exception of a tied insurance intermediary as mentioned in Article 2(7) of that Directive, when it acts in respect of contracts of long-term insurance within the meaning given by article 3(1) of, and Part II of Schedule 1 to, the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001(**y**);

(f) a branch located in an EEA state of a person referred to in sub-paragraphs (a) to (e) (or an equivalent person whose head office is located in a non-EEA state), wherever its head office is located, when carrying out any activity mentioned in sub-paragraphs (a) to (e);

(g) the National Savings Bank;

(h) the Director of Savings, when money is raised under the auspices of the Director under the National Loans Act 1968(**z**).

(4) "Auditor" means any firm or individual who is a statutory auditor within the meaning of Part 42 of the Companies Act 2006(**aa**) (statutory auditors), when carrying out statutory audit work within the meaning of section 1210 of that Act.

(5) Before the entry into force of Part 42 of the Companies Act 2006 the reference in paragraph (4) to—

(a) a person who is a statutory auditor shall be treated as a reference to a person who is eligible for appointment as a company auditor under section 25 of the Companies Act 1989(**ab**) (eligibility for appointment) or article 28 of the Companies (Northern Ireland) Order 1990(**ac**); and

(b) the carrying out of statutory audit work shall be treated as a reference to the provision of audit services.

(6) "Insolvency practitioner" means any person who acts as an insolvency practitioner within the meaning of section 388 of the Insolvency Act 1986(**ad**) (meaning of "act as insolvency practitioner") or article 3 of the Insolvency (Northern Ireland) Order 1989(**ae**).

(7) "External accountant" means a firm or sole practitioner who by way of business provides accountancy services to other persons, when providing such services.

(8) "Tax adviser" means a firm or sole practitioner who by way of business provides advice about the tax affairs of other persons, when providing such services.

(9) "Independent legal professional" means a firm or sole practitioner who by way of business provides legal or notarial services to other persons, when participating in financial or real property transactions concerning—

(a) the buying and selling of real property or business entities;

(aa) 2006 c. 46.

(ad) 1986 c. 45; s388 was amended by section 4 of the Insolvency Act 2000 (c.45), section 11 of the Bankruptcy (Scotland) Act 1993 (c.6), and S.I. 1994/2421, 2002/1240 and 2002/2708.

(ae) 1989 No. 2405 (NI 19); article 3 was amended by the Insolvency (Northern Ireland) Order 2002 No. 3152 (N.I. 6) and S.R. 1995/225, 2002/334, 2003/550, 2004/307.

(b) the managing of client money, securities or other assets;

(c) the opening or management of bank, savings or securities accounts;

(d) the organisation of contributions necessary for the creation, operation or management of companies; or

(e) the creation, operation or management of trusts, companies or similar structures,

and, for this purpose, a person participates in a transaction by assisting in the planning or execution of the transaction or otherwise acting for or on behalf of a client in the transaction.

(10) "Trust or company service provider" means a firm or sole practitioner who by way of business provides any of the following services to other persons—

(a) forming companies or other legal persons;

(b) acting, or arranging for another person to act—

(i) as a director or secretary of a company;

(ii) as a partner of a partnership; or

(iii) in a similar position in relation to other legal persons;

(c) providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or arrangement;

(d) acting, or arranging for another person to act, as—

(i) a trustee of an express trust or similar legal arrangement; or

(ii) a nominee shareholder for a person other than a company whose securities are listed on a regulated market,

when providing such services.

(11) "Estate agent" means—

(a) a firm; or

(b) sole practitioner,

who, or whose employees, carry out estate agency work (within the meaning given by section 1 of the Estate Agents Act 1979(**af**) (estate agency work)), when in the course of carrying out such work.

(12) "High value dealer" means a firm or sole trader who by way of business trades in goods (including an auctioneer dealing in goods), when he receives, in respect of any transaction, a payment or payments in cash of at least 15,000 euros in total, whether the transaction is executed in a single operation or in several operations which appear to be linked.

(13) "Casino" means the holder of a casino operating licence and, for this purpose, a "casino operating licence" has the meaning given by section 65(2) of the Gambling Act 2005(**ag**) (nature of licence).

(14) In the application of this regulation to Scotland, for "real property" in paragraph (9) substitute "heritable property".

Exclusions

4.—(1) These Regulations do not apply to the following persons when carrying out any of the following activities—

(af) 1979 c. 38. Section 1 was amended by the Law Reform (Miscellaneous Provisions) (Scotland) Act 1985 (c.73), section.56, Schedule 1, Part I, paragraph 40, the Planning (Consequential Provisions) Act 1990 (c.11), section 4, Schedule 2, paragraph 42, the Planning (Consequential Provisions) (Scotland) Act 1997 (c.11), sections 4 and 6(2), Schedule 2, paragraph 28 and by S.I. 2001/1283.

(ag) See also section 7 on the meaning of "casino" and Part 5 of the Act generally on operating licences

(a) a society registered under the Industrial and Provident Societies Act 1965(**ah**), when it—

(i) issues withdrawable share capital within the limit set by section 6 of that Act (maximum shareholding in society); or

(ii) accepts deposits from the public within the limit set by section 7(3) of that Act (carrying on of banking by societies);

(b) a society registered under the Industrial and Provident Societies Act (Northern Ireland) 1969(**ai**), when it—

(i) issues withdrawable share capital within the limit set by section 6 of that Act (maximum shareholding in society); or

(ii) accepts deposits from the public within the limit set by section 7(3) of that Act (carrying on of banking by societies);

(c) a person who is (or falls within a class of persons) specified in any of paragraphs 2 to 23, 25 to 38 or 40 to 49 of the Schedule to the Financial Services and Markets Act 2000 (Exemption) Order 2001(**aj**), when carrying out any activity in respect of which he is exempt;

(d) a person who was an exempted person for the purposes of section 45 of the Financial Services Act 1986(**ak**) (miscellaneous exemptions) immediately before its repeal, when exercising the functions specified in that section;

(e) a person whose main activity is that of a high value dealer, when he engages in financial activity on an occasional or very limited basis as set out in paragraph 1 of Schedule 2 to these Regulations; or

(f) a person, when he prepares a home information pack or a document or information for inclusion in a home information pack.

(2) These Regulations do not apply to a person who falls within regulation 3 solely as a result of his engaging in financial activity on an occasional or very limited basis as set out in paragraph 1 of Schedule 2 to these Regulations.

(3) Parts 2 to 5 of these Regulations do not apply to—

(a) the Auditor General for Scotland;

(b) the Auditor General for Wales;

(c) the Bank of England;

(d) the Comptroller and Auditor General;

(e) the Comptroller and Auditor General for Northern Ireland;

(f) the Official Solicitor to the Supreme Court, when acting as trustee in his official capacity;

(g) the Treasury Solicitor.

(4) In paragraph (1)(f), "home information pack" has the same meaning as in Part 5 of the Housing Act 2004(**al**) (home information packs).

PART 2

CUSTOMER DUE DILIGENCE

Meaning of customer due diligence measures

5. "Customer due diligence measures" means—

(al) 2004 c. 34.

(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

(b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and

(c) obtaining information on the purpose and intended nature of the business relationship.

Meaning of beneficial owner

6.—(1) In the case of a body corporate, "beneficial owner" means any individual who—

(a) as respects any body other than a company whose securities are listed on a regulated market, ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25% of the shares or voting rights in the body; or

(b) as respects any body corporate, otherwise exercises control over the management of the body.

(2) In the case of a partnership (other than a limited liability partnership), "beneficial owner" means any individual who—

(a) ultimately is entitled to or controls (whether the entitlement or control is direct or indirect) more than a 25% share of the capital or profits of the partnership or more than 25% of the voting rights in the partnership; or

(b) otherwise exercises control over the management of the partnership.

(3) In the case of a trust, "beneficial owner" means—

(a) any individual who is entitled to a specified interest in at least 25% of the capital of the trust property;

(b) as respects any trust other than one which is set up or operates entirely for the benefit of individuals falling within sub-paragraph (a), the class of persons in whose main interest the trust is set up or operates;

(c) any individual who has control over the trust.

(4) In paragraph (3)—

"specified interest" means a vested interest which is—

(a) in possession or in remainder or reversion (or, in Scotland, in fee); and

(b) defeasible or indefeasible;

"control" means a power (whether exercisable alone, jointly with another person or with the consent of another person) under the trust instrument or by law to—

(a) dispose of, advance, lend, invest, pay or apply trust property;

(b) vary the trust;

(c) add or remove a person as a beneficiary or to or from a class of beneficiaries;

(d) appoint or remove trustees;

(e) direct, withhold consent to or veto the exercise of a power such as is mentioned in sub-paragraph (a), (b), (c) or (d).

(5) For the purposes of paragraph (3)—

(a) where an individual is the beneficial owner of a body corporate which is entitled to a specified interest in the capital of the trust property or which has control over the trust, the individual is to be regarded as entitled to the interest or having control over the trust; and

(b) an individual does not have control solely as a result of—

(i) his consent being required in accordance with section 32(1)(c) of the Trustee Act 1925(**am**) (power of advancement);

(ii) any discretion delegated to him under section 34 of the Pensions Act 1995(**an**) (power of investment and delegation);

(iii) the power to give a direction conferred on him by section 19(2) of the Trusts of Land and Appointment of Trustees Act 1996(**ao**) (appointment and retirement of trustee at instance of beneficiaries); or

(iv) the power exercisable collectively at common law to vary or extinguish a trust where the beneficiaries under the trust are of full age and capacity and (taken together) absolutely entitled to the property subject to the trust (or, in Scotland, have a full and unqualified right to the fee).

(6) In the case of a legal entity or legal arrangement which does not fall within paragraph (1), (2) or (3), "beneficial owner" means—

(a) where the individuals who benefit from the entity or arrangement have been determined, any individual who benefits from at least 25% of the property of the entity or arrangement;

(b) where the individuals who benefit from the entity or arrangement have yet to be determined, the class of persons in whose main interest the entity or arrangement is set up or operates;

(c) any individual who exercises control over at least 25% of the property of the entity or arrangement.

(7) For the purposes of paragraph (6), where an individual is the beneficial owner of a body corporate which benefits from or exercises control over the property of the entity or arrangement, the individual is to be regarded as benefiting from or exercising control over the property of the entity or arrangement.

(8) In the case of an estate of a deceased person in the course of administration, "beneficial owner" means—

(a) in England and Wales and Northern Ireland, the executor, original or by representation, or administrator for the time being of a deceased person;

(b) in Scotland, the executor for the purposes of the Executors (Scotland) Act 1900(**ap**).

(9) In any other case, "beneficial owner" means the individual who ultimately owns or controls the customer or on whose behalf a transaction is being conducted.

(10) In this regulation—

"arrangement", "entity" and "trust" means an arrangement, entity or trust which administers and distributes funds;

"limited liability partnership" has the meaning given by the Limited Liability Partnerships Act 2000(**aq**).

Application of customer due diligence measures

7.—(1) Subject to regulations 9, 10, 12, 13, 14, 16(4) and 17, a relevant person must apply customer due diligence measures when he—

(a) establishes a business relationship;

(b) carries out an occasional transaction;

(c) suspects money laundering or terrorist financing;

(d) doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

(2) Subject to regulation 16(4), a relevant person must also apply customer due diligence measures at other appropriate times to existing customers on a risk-sensitive basis.

(3) A relevant person must—

(a) determine the extent of customer due diligence measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction; and

(b) be able to demonstrate to his supervisory authority that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

(4) Where—

(a) a relevant person is required to apply customer due diligence measures in the case of a trust, legal entity (other than a body corporate) or a legal arrangement (other than a trust); and

(b) the class of persons in whose main interest the trust, entity or arrangement is set up or operates is identified as a beneficial owner,

the relevant person is not required to identify all the members of the class.

(5) Paragraph (3)(b) does not apply to the National Savings Bank or the Director of Savings.

Ongoing monitoring

8.—(1) A relevant person must conduct ongoing monitoring of a business relationship.

(2) "Ongoing monitoring" of a business relationship means—

(a) scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile; and

(b) keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date.

(3) Regulation 7(3) applies to the duty to conduct ongoing monitoring under paragraph (1) as it applies to customer due diligence measures.

Timing of verification

9.—(1) This regulation applies in respect of the duty under regulation 7(1)(a) and (b) to apply the customer due diligence measures referred to in regulation 5(a) and (b).

(2) Subject to paragraphs (3) to (5) and regulation 10, a relevant person must verify the identity of the customer (and any beneficial owner) before the establishment of a business relationship or the carrying out of an occasional transaction.

(3) Such verification may be completed during the establishment of a business relationship if—

(a) this is necessary not to interrupt the normal conduct of business; and

(b) there is little risk of money laundering or terrorist financing occurring,

provided that the verification is completed as soon as practicable after contact is first established.

(4) The verification of the identity of the beneficiary under a life insurance policy may take place after the business relationship has been established provided that it takes place at or before the time of payout or at or before the time the beneficiary exercises a right vested under the policy.

(5) The verification of the identity of a bank account holder may take place after the bank account has been opened provided that there are adequate safeguards in place to ensure that—

(a) the account is not closed; and

(b) transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder),

before verification has been completed.

Casinos

10.—(1) A casino must establish and verify the identity of—

(a) all customers to whom the casino makes facilities for gaming available—

(i) before entry to any premises where such facilities are provided; or

(ii) where the facilities are for remote gaming, before access is given to such facilities; or

(b) if the specified conditions are met, all customers who, in the course of any period of 24 hours—

(i) purchase from, or exchange with, the casino chips with a total value of 2,000 euro or more;

(ii) pay the casino 2,000 or more for the use of gaming machines; or

(iii) pay to, or stake with, the casino 2,000 euro or more in connection with facilities for remote gaming.

(2) The specified conditions are—

(a) the casino verifies the identity of each customer before or immediately after such purchase, exchange, payment or stake takes place, and

(b) the Gambling Commission is satisfied that the casino has appropriate procedures in place to monitor and record—

(i) the total value of chips purchased from or exchanged with the casino;

(ii) the total money paid for the use of gaming machines; or

(iii) the total money paid or staked in connection with facilities for remote gaming,

by each customer.

(3) In this regulation—

"gaming", "gaming machine", "remote operating licence" and "stake" have the meanings given by, respectively, sections 6(1) (gaming & game of chance), 235 (gaming machine), 67 (remote gambling) and 353(1) (interpretation) of the Gambling Act 2005(**ar**);

"premises" means premises subject to—

(a) a casino premises licence within the meaning of section 150(1)(a) of the Gambling Act 2005 (nature of licence); or

(b) a converted casino premises licence within the meaning of paragraph 65 of Part 7 of Schedule 4 to the Gambling Act 2005 (Commencement No. 6 and Transitional Provisions) Order 2006(**as**);

"remote gaming" means gaming provided pursuant to a remote operating licence.

Requirement to cease transactions etc.

11.—(1) Where, in relation to any customer, a relevant person is unable to apply customer due diligence measures in accordance with the provisions of this Part, he—

(a) must not carry out a transaction with or for the customer through a bank account;

(b) must not establish a business relationship or carry out an occasional transaction with the customer;

(c) must terminate any existing business relationship with the customer;

(d) must consider whether he is required to make a disclosure by Part 7 of the Proceeds of Crime Act 2002 or Part 3 of the Terrorism Act 2000.

(2) Paragraph (1) does not apply where a lawyer or other professional adviser is in the course of ascertaining the legal position for his client or performing his task of defending or representing that client in, or concerning, legal proceedings, including advice on the institution or avoidance of proceedings.

(3) In paragraph (2), "other professional adviser" means an auditor, accountant or tax adviser who is a member of a professional body which is established for any such persons and which makes provision for—

(a) testing the competence of those seeking admission to membership of such a body as a condition for such admission; and

(b) imposing and maintaining professional and ethical standards for its members, as well as imposing sanctions for non-compliance with those standards.

Exception for trustees of debt issues

12.—(1) A relevant person—

(a) who is appointed by the issuer of instruments or securities specified in paragraph (2) as trustee of an issue of such instruments or securities; or

(b) whose customer is a trustee of an issue of such instruments or securities,

is not required to apply the customer due diligence measure referred to in regulation 5(b) in respect of the holders of such instruments or securities.

(2) The specified instruments and securities are—

(a) instruments which fall within article 77 of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001(**at**); and

(b) securities which fall within article 78 of that Order.

Simplified due diligence

13.—(1) A relevant person is not required to apply customer due diligence measures in the circumstances mentioned in regulation 7(1)(a), (b) or (d) where he has reasonable grounds for believing that the customer, transaction or product related to such transaction, falls within any of the following paragraphs.

(2) The customer is—

(a) a credit or financial institution which is subject to the requirements of the money laundering directive; or

(b) a credit or financial institution (or equivalent institution) which—

(i) is situated in a non-EEA state which imposes requirements equivalent to those laid down in the money laundering directive; and

(ii) is supervised for compliance with those requirements.

(3) The customer is a company whose securities are listed on a regulated market subject to specified disclosure obligations.

(4) The customer is an independent legal professional and the product is an account into which monies are pooled, provided that—

(a) where the pooled account is held in a non-EEA state—

(i) that state imposes requirements to combat money laundering and terrorist financing which are consistent with international standards; and

(ii) the independent legal professional is supervised in that state for compliance with those requirements; and

(b) information on the identity of the persons on whose behalf monies are held in the pooled account is available, on request, to the institution which acts as a depository institution for the account.

(5) The customer is a public authority in the United Kingdom.

(6) The customer is a public authority which fulfils all the conditions set out in paragraph 2 of Schedule 2 to these Regulations.

(7) The product is—

(a) a life insurance contract where the annual premium is no more than 1,000 euro or where a single premium of no more than 2,500 euro is paid;

(b) an insurance contract for the purposes of a pension scheme where the contract contains no surrender clause and cannot be used as collateral;

(c) a pension, superannuation or similar scheme which provides retirement benefits to employees, where contributions are made by an employer or by way of deduction from an employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme (other than an assignment permitted by section 44 of the Welfare Reform and Pensions Act 1999(**au**) (disapplication of restrictions on alienation) or section 91(5)(a) of the Pensions Act 1995(**av**) (inalienability of occupational pension)); or

(d) electronic money, within the meaning of Article 1(3)(b) of the electronic money directive, where—

(i) if the device cannot be recharged, the maximum amount stored in the device is no more than 150 euro; or

(ii) if the device can be recharged, a limit of 2,500 euro is imposed on the total amount transacted in a calendar year, except when an amount of 1,000 euro or more is redeemed in the same calendar year by the bearer (within the meaning of Article 3 of the electronic money directive).

(8) The product and any transaction related to such product fulfils all the conditions set out in paragraph 3 of Schedule 2 to these Regulations.

(9) The product is a child trust fund within the meaning given by section 1(2) of the Child Trust Funds Act 2004(**aw**).

Enhanced customer due diligence and ongoing monitoring

14.—(1) A relevant person must apply on a risk-sensitive basis enhanced customer due diligence measures and enhanced ongoing monitoring—

(a) in accordance with paragraphs (2) to (4);

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

(aw) 2004 c. 6.

(2) Where the customer has not been physically present for identification purposes, a relevant person must take specific and adequate measures to compensate for the higher risk, for example, by applying one or more of the following measures—

(a) ensuring that the customer's identity is established by additional documents, data or information;

(b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the money laundering directive;

(c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution.

(3) A credit institution ("the correspondent") which has or proposes to have a correspondent banking relationship with a respondent institution ("the respondent") from a non-EEA state must—

(a) gather sufficient information about the respondent to understand fully the nature of its business;

(b) determine from publicly-available information the reputation of the respondent and the quality of its supervision;

(c) assess the respondent's anti-money laundering and anti-terrorist financing controls;

(d) obtain approval from senior management before establishing a new correspondent banking relationship;

(e) document the respective responsibilities of the respondent and correspondent; and

(f) be satisfied that, in respect of those of the respondent's customers who have direct access to accounts of the correspondent, the respondent—

(i) has verified the identity of, and conducts ongoing monitoring in respect of, such customers; and

(ii) is able to provide to the correspondent, upon request, the documents, data or information obtained when applying customer due diligence measures and ongoing monitoring.

(4) A relevant person who proposes to have a business relationship or carry out an occasional transaction with a politically exposed person must—

(a) have approval from senior management for establishing the business relationship with that person;

(b) take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or occasional transaction; and

(c) where the business relationship is entered into, conduct enhanced ongoing monitoring of the relationship.

(5) In paragraph (4), "a politically exposed person" means a person who is—

(a) an individual who is or has, at any time in the preceding year, been entrusted with a prominent public function by—

(i) a state other than the United Kingdom;

(ii) a Community institution; or

(iii) an international body,

including a person who falls in any of the categories listed in paragraph 4(1)(a) of Schedule 2;

(b) an immediate family member of a person referred to in sub-paragraph (a), including a person who falls in any of the categories listed in paragraph 4(1)(c) of Schedule 2; or

(c) a known close associate of a person referred to in sub-paragraph (a), including a person who falls in either of the categories listed in paragraph 4(1)(d) of Schedule 2.

(6) For the purpose of deciding whether a person is a known close associate of a person referred to in paragraph (5)(a), a relevant person need only have regard to information which is in his possession or is publicly known.

Branches and subsidiaries

15.—(1) A credit or financial institution must require its branches and subsidiary undertakings which are located in a non-EEA state to apply, to the extent permitted by the law of that state, measures at least equivalent to those set out in these Regulations with regard to customer due diligence measures, ongoing monitoring and record-keeping.

(2) Where the law of a non-EEA state does not permit the application of such equivalent measures by the branch or subsidiary undertaking located in that state, the credit or financial institution must—

(a) inform its supervisory authority accordingly; and

(b) take additional measures to handle effectively the risk of money laundering and terrorist financing.

(3) In this regulation "subsidiary undertaking"—

(a) except in relation to an incorporated friendly society, has the meaning given by section 1162 of the Companies Act 2006(**ax**) (parent and subsidiary undertakings) and, in relation to a body corporate in or formed under the law of an EEA state other than the United Kingdom, includes an undertaking which is a subsidiary undertaking within the meaning of any rule of law in force in that state for purposes connected with implementation of the European Council Seventh Company Law Directive 83/349/EEC of 13th June 1983(**ay**) on consolidated accounts;

(b) in relation to an incorporated friendly society, means a body corporate of which the society has control within the meaning of section 13(9)(a) or (aa) of the Friendly Societies Act 1992(**az**) (control of subsidiaries and other bodies corporate).

(4) Before the entry into force of section 1162 of the Companies Act 2006 the reference to that section in paragraph (3)(a) shall be treated as a reference to section 258 of the Companies Act 1985(**ba**) (parent and subsidiary undertakings).

Shell banks, anonymous accounts etc.

16.—(1) A credit institution must not enter into, or continue, a correspondent banking relationship with a shell bank.

(2) A credit institution must take appropriate measures to ensure that it does not enter into, or continue, a corresponding banking relationship with a bank which is known to permit its accounts to be used by a shell bank.

(3) A credit or financial institution carrying on business in the United Kingdom must not set up an anonymous account or an anonymous passbook for any new or existing customer.

(4) As soon as reasonably practicable on or after 15th December 2007 all credit and financial institutions carrying on business in the United Kingdom must apply customer due diligence measures to, and conduct ongoing monitoring of, all anonymous accounts and passbooks in existence on that date and in any event before such accounts or passbooks are used.

(5) A "shell bank" means a credit institution, or an institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence involving meaningful decision-

(ba) 1985 c. 6.

making and management, and which is not part of a financial conglomerate or third-country financial conglomerate.

(6) In this regulation, "financial conglomerate" and "third-country financial conglomerate" have the meanings given by regulations 1(2) and 7(1) respectively of the Financial Conglomerates and Other Financial Groups Regulations 2004(**bb**).

Reliance

17.—(1) A relevant person may rely on a person who falls within paragraph (2) (or who the relevant person has reasonable grounds to believe falls within paragraph (2)) to apply any customer due diligence measures provided that—

(a) the other person consents to being relied on; and

(b) notwithstanding the relevant person's reliance on the other person, the relevant person remains liable for any failure to apply such measures.

(2) The persons are—

(a) a credit or financial institution which is an authorised person;

(b) a relevant person who is—

(i) an auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional; and

(ii) supervised for the purposes of these Regulations by one of the bodies listed in Part 1 of Schedule 3;

(c) a person who carries on business in another EEA state who is—

(i) a credit or financial institution, auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional;

(ii) subject to mandatory professional registration recognised by law; and

(iii) supervised for compliance with the requirements laid down in the money laundering directive in accordance with section 2 of Chapter V of that directive; or

(d) a person who carries on business in a non-EEA state who is—

(i) a credit or financial institution (or equivalent institution), auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional;

(ii) subject to mandatory professional registration recognised by law;

(iii) subject to requirements equivalent to those laid down in the money laundering directive; and

(iv) supervised for compliance with those requirements in a manner equivalent to section 2 of Chapter V of the money laundering directive.

(3) In paragraph (2)(c)(i) and (d)(i), "auditor" and "insolvency practitioner" includes a person situated in another EEA state or a non-EEA state who provides services equivalent to the services provided by an auditor or insolvency practitioner.

(4) Nothing in this regulation prevents a relevant person applying customer due diligence measures by means of an outsourcing service provider or agent provided that the relevant person remains liable for any failure to apply such measures.

(5) In this regulation, "financial institution" excludes money service businesses.

(bb) S.I. 2004/1862.

Directions where Financial Action Task Force applies counter-measures

18. The Treasury may direct any relevant person—

(a) not to enter into a business relationship;

(b) not to carry out an occasional transaction; or

(c) not to proceed any further with a business relationship or occasional transaction,

with a person who is situated or incorporated in a non-EEA state to which the Financial Action Task Force has decided to apply counter-measures.

PART 3

RECORD-KEEPING, PROCEDURES AND TRAINING

Record-keeping

19.—(1) Subject to paragraph (4), a relevant person must keep the records specified in paragraph (2) for at least the period specified in paragraph (3).

(2) The records are—

(a) a copy of, or the references to, the evidence of the customer's identity obtained pursuant to regulation 7, 8, 10, 14 or 16(4);

(b) the supporting records (consisting of the original documents or copies) in respect of a business relationship or occasional transaction which is the subject of customer due diligence measures or ongoing monitoring.

(3) The period is five years beginning on—

(a) in the case of the records specified in paragraph (2)(a), the date on which—

(i) the occasional transaction is completed; or

(ii) the business relationship ends; or

(b) in the case of the records specified in paragraph (2)(b)—

(i) where the records relate to a particular transaction, the date on which the transaction is completed;

(ii) for all other records, the date on which the business relationship ends.

(4) A relevant person who is relied on by another person must keep the records specified in paragraph (2)(a) for five years beginning on the date on which he is relied on for the purposes of regulation 7, 10, 14 or 16(4) in relation to any business relationship or occasional transaction.

(5) A person referred to in regulation 17(2)(a) or (b) who is relied on by a relevant person must, if requested by the person relying on him within the period referred to in paragraph (4)—

(a) as soon as reasonably practicable make available to the person who is relying on him any information about the customer (and any beneficial owner) which he obtained when applying customer due diligence measures; and

(b) as soon as reasonably practicable forward to the person who is relying on him copies of any identification and verification data and other relevant documents on the identity of the customer (and any beneficial owner) which he obtained when applying those measures.

(6) A relevant person who relies on a person referred to in regulation 17(2)(c) or (d) (a "third party") to apply customer due diligence measures must take steps to ensure that the third party will, if requested by the relevant person within the period referred to in paragraph (4)—

(a) as soon as reasonably practicable make available to him any information about the customer (and any beneficial owner) which the third party obtained when applying customer due diligence measures; and

(b) as soon as reasonably practicable forward to him copies of any identification and verification data and other relevant documents on the identity of the customer (and any beneficial owner) which the third party obtained when applying those measures.

(7) Paragraphs (5) and (6) do not apply where a relevant person applies customer due diligence measures by means of an outsourcing service provider or agent.

(8) For the purposes of this regulation, a person relies on another person where he does so in accordance with regulation 17(1).

Policies and procedures

20.—(1) A relevant person must establish and maintain appropriate and risk-sensitive policies and procedures relating to—

(a) customer due diligence measures and ongoing monitoring;

(b) reporting;

(c) record-keeping;

(d) internal control;

(e) risk assessment and management;

(f) the monitoring and management of compliance with, and the internal communication of, such policies and procedures,

in order to prevent activities related to money laundering and terrorist financing.

(2) The policies and procedures referred to in paragraph (1) include policies and procedures—

(a) which provide for the identification and scrutiny of—

(i) complex or unusually large transactions;

(ii) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and

(iii) any other activity which the relevant person regards as particularly likely by its nature to be related to money laundering or terrorist financing;

(b) which specify the taking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products and transactions which might favour anonymity;

(c) to determine whether a customer is a politically exposed person;

(d) under which—

(i) an individual in the relevant person's organisation is a nominated officer under Part 7 of the Proceeds of Crime Act 2002(**bc**) and Part 3 of the Terrorism Act 2000(**bd**);

(ii) anyone in the organisation to whom information or other matter comes in the course of the business as a result of which he knows or suspects or has reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing is required to comply with Part 7 of the Proceeds of Crime Act 2002 or, as the case may be, Part 3 of the Terrorism Act 2000; and

(iii) where a disclosure is made to the nominated officer, he must consider it in the light of any relevant information which is available to the relevant person and determine whether it gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion that a person is engaged in money laundering or terrorist financing.

(3) Paragraph (2)(d) does not apply where the relevant person is an individual who neither employs nor acts in association with any other person.

(4) A credit or financial institution must establish and maintain systems which enable it to respond fully and rapidly to enquiries from financial investigators accredited under section 3 of the Proceeds of Crime Act 2002 (accreditation and training), persons acting on behalf of the Scottish Ministers in their capacity as an enforcement authority under that Act, officers of Revenue and Customs or constables as to—

(a) whether it maintains, or has maintained during the previous five years, a business relationship with any person; and

(b) the nature of that relationship.

(5) A credit or financial institution must communicate where relevant the policies and procedures which it establishes and maintains in accordance with this regulation to its branches and subsidiary undertakings which are located outside the United Kingdom.

(6) In this regulation—

"politically exposed person" has the same meaning as in regulation 14(4);

"subsidiary undertaking" has the same meaning as in regulation 15.

Training

21. A relevant person must take appropriate measures so that all relevant employees of his are—

(a) made aware of the law relating to money laundering and terrorist financing; and

(b) regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.

PART 4

SUPERVISION AND REGISTRATION

Interpretation

Interpretation

22.—(1) In this Part—

"Annex I financial institution" means any undertaking which falls within regulation 3(3)(a) other than—

(a) a consumer credit financial institution;

(b) a money service business; or

(c) an authorised person;

"consumer credit financial institution" means any undertaking which falls within regulation 3(3)(a) and which requires, under section 21 of the Consumer Credit Act 1974(**be**) (businesses needing a licence), a licence to carry on a consumer credit business, other than—

(a) a person covered by a group licence issued by the OFT under section 22 of that Act (standard and group licences);

(b) a money service business; or

(c) an authorised person.

(2) In paragraph (1), "consumer credit business" has the meaning given by section 189(1) of the Consumer Credit Act 1974 (definitions) and, on the entry into force of section 23(a) of the Consumer Credit Act 2006(**bf**) (definitions of "consumer credit business" and "consumer hire business"), has the meaning given by section 189(1) of the Consumer Credit Act 1974 as amended by section 23(a) of the Consumer Credit Act 2006.

Supervision

Supervisory authorities

23.—(1) Subject to paragraph (2), the following bodies are supervisory authorities—

(a) the Authority is the supervisory authority for—

(i) credit and financial institutions which are authorised persons;

(ii) trust or company service providers which are authorised persons;

(iii) Annex I financial institutions;

(b) the OFT is the supervisory authority for—

(i) consumer credit financial institutions;

(ii) estate agents;

(c) each of the professional bodies listed in Schedule 3 is the supervisory authority for relevant persons who are regulated by it;

(d) the Commissioners are the supervisory authority for—

(i) high value dealers;

(ii) money service businesses which are not supervised by the Authority;

(iii) trust or company service providers which are not supervised by the Authority or one of the bodies listed in Schedule 3;

(iv) auditors, external accountants and tax advisers who are not supervised by one of the bodies listed in Schedule 3.

(e) the Gambling Commission is the supervisory authority for casinos;

(f) DETI is the supervisory authority for—

(i) credit unions in Northern Ireland;

(ii) insolvency practitioners authorised by it under article 351 of the Insolvency (Northern Ireland) Order 1989;

(g) the Secretary of State is the supervisory authority for insolvency practitioners authorised by him under section 393 of the Insolvency Act 1986(**bg**) (grant, refusal and withdrawal of authorisation).

(2) Where under paragraph (1) there is more than one supervisory authority for a relevant person, the supervisory authorities may agree that one of them will act as the supervisory authority for that person.

(3) Where an agreement has been made under paragraph (2), the authority which has agreed to act as the supervisory authority must notify the relevant person or publish the agreement in such manner as it considers appropriate.

(4) Where no agreement has been made under paragraph (2), the supervisory authorities for a relevant person must cooperate in the performance of their functions under these Regulations.

(bf) 2006 c. 14.

Duties of supervisory authorities

24.—(1) A supervisory authority must effectively monitor the relevant persons for whom it is the supervisory authority and take necessary measures for the purpose of securing compliance by such persons with the requirements of these Regulations.

(2) A supervisory authority which, in the course of carrying out any of its functions under these Regulations, knows or suspects that a person is or has engaged in money laundering or terrorist financing must promptly inform the Serious Organised Crime Agency.

(3) A disclosure made under paragraph (2) is not to be taken to breach any restriction, however imposed, on the disclosure of information.

(4) The functions of the Authority under these Regulations shall be treated for the purposes of Parts 1, 2 and 4 of Schedule 1 to the 2000 Act (the Financial Services Authority) as functions conferred on the Authority under that Act.

Registration of high value dealers, money service businesses and trust or company service providers

Duty to maintain registers

25.—(1) The Commissioners must maintain registers of—

(a) high value dealers;

(b) money service businesses for which they are the supervisory authority; and

(c) trust or company service providers for which they are the supervisory authority.

(2) The Commissioners may keep the registers in any form they think fit.

(3) The Commissioners may publish or make available for public inspection all or part of a register maintained under this regulation.

Requirement to be registered

26.—(1) A person in respect of whom the Commissioners are required to maintain a register under regulation 25 must not act as a—

(a) high value dealer;

(b) money service business; or

(c) trust or company service provider,

unless he is included in the register.

(2) Paragraph (1) and regulation 29 are subject to the transitional provisions set out in regulation 50.

Applications for registration in a register maintained under regulation 25

27.—(1) An applicant for registration in a register maintained under regulation 25 must make an application in such manner and provide such information as the Commissioners may specify.

(2) The information which the Commissioners may specify includes—

(a) the applicant's name and (if different) the name of the business;

(b) the nature of the business;

(c) the name of the nominated officer (if any);

(d) in relation to a money service business or trust or company service provider—

(i) the name of any person who effectively directs or will direct the business and any beneficial owner of the business; and

(ii) information needed by the Commissioners to decide whether they must refuse the application pursuant to regulation 28.

(3) At any time after receiving an application and before determining it, the Commissioners may require the applicant to provide, within 21 days beginning with the date of being requested to do so, such further information as they reasonably consider necessary to enable them to determine the application.

(4) If at any time after the applicant has provided the Commissioners with any information under paragraph (1) or (3)—

(a) there is a material change affecting any matter contained in that information; or

(b) it becomes apparent to that person that the information contains a significant inaccuracy,

he must provide the Commissioners with details of the change or, as the case may be, a correction of the inaccuracy within 30 days beginning with the date of the occurrence of the change (or the discovery of the inaccuracy) or within such later time as may be agreed with the Commissioners.

(5) The obligation in paragraph (4) applies also to material changes or significant inaccuracies affecting any matter contained in any supplementary information provided pursuant to that paragraph.

(6) Any information to be provided to the Commissioners under this regulation must be in such form or verified in such manner as they may specify.

Fit and proper test

28.—(1) The Commissioners must refuse to register an applicant as a money service business or trust or company service provider if they are satisfied that—

(a) the applicant;

(b) a person who effectively directs, or will effectively direct, the business or service provider;

(c) a beneficial owner of the business or service provider; or

(d) the nominated officer of the business or service provider,

is not a fit and proper person.

(2) For the purposes of paragraph (1), a person is not a fit and proper person if he—

(a) has been convicted of—

(i) an offence under the Terrorism Act 2000(**bh**);

(ii) an offence under paragraph 7(2) or (3) of Schedule 3 to the Anti-Terrorism, Crime and Security Act 2001(**bi**) (offences);

(iii) an offence under the Terrorism Act 2006(**bj**);

(iv) an offence under Part 7 (money laundering) of, or listed in Schedule 2 (lifestyle offences: England and Wales), 4 (lifestyle offences: Scotland) or 5 (lifestyle offences: Northern Ireland) to, the Proceeds of Crime Act 2002(**bk**);

(v) an offence under the Fraud Act 2006(**bl**) or, in Scotland, the common law offence of fraud;

(vi) an offence under section 72(1), (3) or (8) of the Value Added Tax Act 1994(**bm**) (offences); or

(vii) the common law offence of cheating the public revenue;

(b) has been adjudged bankrupt or sequestration of his estate has been awarded and (in either case) he has not been discharged;

(c) is subject to a disqualification order under the Company Directors Disqualification Act 1986(**bn**);

(d) is or has been subject to a confiscation order under the Proceeds of Crime Act 2002;

(e) has consistently failed to comply with the requirements of these Regulations, the Money Laundering Regulations 2003(**bo**) or the Money Laundering Regulations 2001(**bp**);

(f) has consistently failed to comply with the requirements of regulation 2006/1781/EC of the European Parliament and of the Council of 15th November 2006 on information on the payer accompanying the transfer of funds(**bq**);

(g) has effectively directed a business which falls within sub-paragraph (e) or (f);

(h) is otherwise not a fit and proper person with regard to the risk of money laundering or terrorist financing.

(3) For the purposes of this regulation, a conviction for an offence listed in paragraph (2)(a) is to be disregarded if it is spent for the purposes of the Rehabilitation of Offenders Act 1974(**br**).

Determination of applications under regulation 27

29.—(1) Subject to regulation 28, the Commissioners may refuse to register an applicant for registration in a register maintained under regulation 25 only if—

(a) any requirement of, or imposed under, regulation 27 has not been complied with;

(b) it appears to the Commissioners that any information provided pursuant to regulation 27 is false or misleading in a material particular; or

(c) the applicant has failed to pay a charge imposed by them under regulation 35(1).

(2) The Commissioners must within 45 days beginning either with the date on which they receive the application or, where applicable, with the date on which they receive any further information required under regulation 27(3), give the applicant notice of—

(a) their decision to register the applicant; or

(b) the following matters—

(i) their decision not to register the applicant;

(ii) the reasons for their decision;

(iii) the right to require a review under regulation 43; and

(iv) the right to appeal under regulation 44(1)(a).

(3) The Commissioners must, as soon as practicable after deciding to register a person, include him in the relevant register.

Cancellation of registration in a register maintained under regulation 25

30.—(1) The Commissioners must cancel the registration of a money service business or trust or company service provider in a register maintained under regulation 25(1) if, at any time after registration, they are satisfied that he or any person mentioned in regulation 28(1)(b), (c) or (d) is not a fit and proper person within the meaning of regulation 28(2).

(2) The Commissioners may cancel a person's registration in a register maintained by them under regulation 25 if, at any time after registration, it appears to them that they would have had grounds to refuse registration under regulation 29(1).

(br) 1974 c. 53.

(3) Where the Commissioners decide to cancel a person's registration they must give him notice of—

(a) their decision and, subject to paragraph (4), the date from which the cancellation takes effect;

(b) the reasons for their decision;

(c) the right to require a review under regulation 43; and

(d) the right to appeal under regulation 44(1)(a).

(4) If the Commissioners—

(a) consider that the interests of the public require the cancellation of a person's registration to have immediate effect; and

(b) include a statement to that effect and the reasons for it in the notice given under paragraph (3),

the cancellation takes effect when the notice is given to the person.

Requirement to inform the Authority

Requirement on authorised person to inform the Authority

31.—(1) An authorised person whose supervisory authority is the Authority must, before acting as a money service business or a trust or company service provider or within 28 days of so doing, inform the Authority that he intends, or has begun, to act as such.

(2) Paragraph (1) does not apply to an authorised person who—

(a) immediately before 15th December 2007 was acting as a money service business or a trust or company service provider and continues to act as such after that date; and

(b) before 15th January 2008 informs the Authority that he is or was acting as such.

(3) Where an authorised person whose supervisory authority is the Authority ceases to act as a money service business or a trust or company service provider, he must immediately inform the Authority.

(4) Any requirement imposed by this regulation is to be treated as if it were a requirement imposed by or under the 2000 Act.

(5) Any information to be provided to the Authority under this regulation must be in such form or verified in such manner as it may specify.

Registration of Annex I financial institutions, estate agents etc.

Power to maintain registers

32.—(1) The supervisory authorities mentioned in paragraph (2), (3) or (4) may, in order to fulfil their duties under regulation 24, maintain a register under this regulation.

(2) The Authority may maintain a register of Annex I financial institutions.

(3) The OFT may maintain registers of—

(a) consumer credit financial institutions; and

(b) estate agents.

(4) The Commissioners may maintain registers of—

(a) auditors;

(b) external accountants; and

(c) tax advisers,

who are not supervised by the Secretary of State, DETI or any of the professional bodies listed in Schedule 3.

(5) Where a supervisory authority decides to maintain a register under this regulation, it must take reasonable steps to bring its decision to the attention of those relevant persons in respect of whom the register is to be established.

(6) A supervisory authority may keep a register under this regulation in any form it thinks fit.

(7) A supervisory authority may publish or make available to public inspection all or part of a register maintained by it under this regulation.

Requirement to be registered

33. Where a supervisory authority decides to maintain a register under regulation 32 in respect of any description of relevant persons and establishes a register for that purpose, a relevant person of that description may not carry on the business or profession in question for a period of more than six months beginning on the date on which the supervisory authority establishes the register unless he is included in the register.

Applications for and cancellation of registration in a register maintained under regulation 32

34.—(1) Regulations 27, 29 (with the omission of the words "Subject to regulation 28" in regulation 29(1)) and 30(2), (3) and (4) apply to registration in a register maintained by the Commissioners under regulation 32 as they apply to registration in a register maintained under regulation 25.

(2) Regulation 27 applies to registration in a register maintained by the Authority or the OFT under regulation 32 as it applies to registration in a register maintained under regulation 25 and, for this purpose, references to the Commissioners are to be treated as references to the Authority or the OFT, as the case may be.

(3) The Authority and the OFT may refuse to register an applicant for registration in a register maintained under regulation 32 only if—

(a) any requirement of, or imposed under, regulation 27 has not been complied with;

(b) it appears to the Authority or the OFT, as the case may be, that any information provided pursuant to regulation 27 is false or misleading in a material particular; or

(c) the applicant has failed to pay a charge imposed by the Authority or the OFT, as the case may be, under regulation 35(1).

(4) The Authority or the OFT, as the case may be, must, within 45 days beginning either with the date on which it receives an application or, where applicable, with the date on which it receives any further information required under regulation 27(3), give the applicant notice of—

(a) its decision to register the applicant; or

(b) the following matters—

(i) that it is minded not to register the applicant;

(ii) the reasons for being minded not to register him; and

(iii) the right to make representations to it within a specified period (which may not be less than 28 days).

(5) The Authority or the OFT, as the case may be, must then decide, within a reasonable period, whether to register the applicant and it must give the applicant notice of—

(a) its decision to register the applicant; or

(b) the following matters—

(i) its decision not to register the applicant;

(ii) the reasons for its decision; and

(iii) the right to appeal under regulation 44(1)(b).

(6) The Authority or the OFT, as the case may be, must, as soon as reasonably practicable after deciding to register a person, include him in the relevant register.

(7) The Authority or the OFT may cancel a person's registration in a register maintained by them under regulation 32 if, at any time after registration, it appears to them that they would have had grounds to refuse registration under paragraph (3).

(8) Where the Authority or the OFT proposes to cancel a person's registration, it must give him notice of—

(a) its proposal to cancel his registration;

(b) the reasons for the proposed cancellation; and

(c) the right to make representations to it within a specified period (which may not be less than 28 days).

(9) The Authority or the OFT, as the case may be, must then decide, within a reasonable period, whether to cancel the person's registration and it must give him notice of—

(a) its decision not to cancel his registration; or

(b) the following matters—

(i) its decision to cancel his registration and, subject to paragraph (10), the date from which cancellation takes effect;

(ii) the reasons for its decision; and

(iii) the right to appeal under regulation 44(1)(b).

(10) If the Authority or the OFT, as the case may be—

(a) considers that the interests of the public require the cancellation of a person's registration to have immediate effect; and

(b) includes a statement to that effect and the reasons for it in the notice given under paragraph (9)(b),

the cancellation takes effect when the notice is given to the person.

(11) In paragraphs (3) and (4), references to regulation 27 are to be treated as references to that paragraph as applied by paragraph (2) of this regulation.

Financial provisions

Costs of supervision

35.—(1) The Authority, the OFT and the Commissioners may impose charges—

(a) on applicants for registration;

(b) on relevant persons supervised by them.

(2) Charges levied under paragraph (1) must not exceed such amount as the Authority, the OFT or the Commissioners (as the case may be) consider will enable them to meet any expenses

reasonably incurred by them in carrying out their functions under these Regulations or for any incidental purpose.

(3) Without prejudice to the generality of paragraph (2), a charge may be levied in respect of each of the premises at which a person carries on (or proposes to carry on) business.

(4) The Authority must apply amounts paid to it by way of penalties imposed under regulation 42 towards expenses incurred in carrying out its functions under these Regulations or for any incidental purpose.

(5) In paragraph (2), "expenses" in relation to the OFT includes expenses incurred by a local weights and measures authority or DETI pursuant to arrangements made for the purposes of these Regulations with the OFT—

(a) by or on behalf of the authority; or

(b) by DETI.

PART 5

ENFORCEMENT

Powers of designated authorities

Interpretation

36. In this Part—

"designated authority" means—

(a) the Authority;

(b) the Commissioners;

(c) the OFT; and

(d) in relation to credit unions in Northern Ireland, DETI;

"officer", except in regulations 40(3), 41 and 47 means—

(a) an officer of the Authority, including a member of the Authority's staff or an agent of the Authority;

(b) an officer of Revenue and Customs;

(c) an officer of the OFT;

(d) a relevant officer; or

(e) an officer of DETI acting for the purposes of its functions under these Regulations in relation to credit unions in Northern Ireland;

"recorded information" includes information recorded in any form and any document of any nature;

"relevant officer" means—

(a) in Great Britain, an officer of a local weights and measures authority;

(b) in Northern Ireland, an officer of DETI acting pursuant to arrangements made with the OFT for the purposes of these Regulations.

Power to require information from, and attendance of, relevant and connected persons

37.—(1) An officer may, by notice to a relevant person or to a person connected with a relevant person, require the relevant person or the connected person, as the case may be—

(a) to provide such information as may be specified in the notice;

(b) to produce such recorded information as may be so specified; or

(c) to attend before an officer at a time and place specified in the notice and answer questions.

(2) For the purposes of paragraph (1), a person is connected with a relevant person if he is, or has at any time been, in relation to the relevant person, a person listed in Schedule 4 to these Regulations.

(3) An officer may exercise powers under this regulation only if the information sought to be obtained as a result is reasonably required in connection with the exercise by the designated authority for whom he acts of its functions under these Regulations.

(4) Where an officer requires information to be provided or produced pursuant to paragraph (1)(a) or (b)—

(a) the notice must set out the reasons why the officer requires the information to be provided or produced; and

(b) such information must be provided or produced—

(i) before the end of such reasonable period as may be specified in the notice; and

(ii) at such place as may be so specified.

(5) In relation to information recorded otherwise than in legible form, the power to require production of it includes a power to require the production of a copy of it in legible form or in a form from which it can readily be produced in visible and legible form.

(6) The production of a document does not affect any lien which a person has on the document.

(7) A person may not be required under this regulation to provide or produce information or to answer questions which he would be entitled to refuse to provide, produce or answer on grounds of legal professional privilege in proceedings in the High Court, except that a lawyer may be required to provide the name and address of his client.

(8) Subject to paragraphs (9) and (10), a statement made by a person in compliance with a requirement imposed on him under paragraph (1)(c) is admissible in evidence in any proceedings, so long as it also complies with any requirements governing the admissibility of evidence in the circumstances in question.

(9) In criminal proceedings in which a person is charged with an offence to which this paragraph applies—

(a) no evidence relating to the statement may be adduced; and

(b) no question relating to it may be asked,

by or on behalf of the prosecution unless evidence relating to it is adduced, or a question relating to it is asked, in the proceedings by or on behalf of that person.

(10) Paragraph (9) applies to any offence other than one under—

(a) section 5 of the Perjury Act 1911(**bs**) (false statements without oath);

(b) section 44(2) of the Criminal Law (Consolidation)(Scotland) Act 1995(**bt**) (false statements and declarations); or

(c) Article 10 of the Perjury (Northern Ireland) Order 1979(**bu**) (false unsworn statements).

(11) In the application of this regulation to Scotland, the reference in paragraph (7) to—

(a) proceedings in the High Court is to be read as a reference to legal proceedings generally; and

(b) an entitlement on grounds of legal professional privilege is to be read as a reference to an entitlement on the grounds of confidentiality of communications.

Entry, inspection without a warrant etc.

38.—(1) Where an officer has reasonable cause to believe that any premises are being used by a relevant person in connection with his business or professional activities, he may on producing evidence of his authority at any reasonable time—

(a) enter the premises;

(b) inspect the premises;

(c) observe the carrying on of business or professional activities by the relevant person;

(d) inspect any recorded information found on the premises;

(e) require any person on the premises to provide an explanation of any recorded information or to state where it may be found;

(f) in the case of a money service business or a high value dealer, inspect any cash found on the premises.

(2) An officer may take copies of, or make extracts from, any recorded information found under paragraph (1).

(3) Paragraphs (1)(d) and (e) and (2) do not apply to recorded information which the relevant person would be entitled to refuse to disclose on grounds of legal professional privilege in proceedings in the High Court, except that a lawyer may be required to provide the name and address of his client and, for this purpose, regulation 37(11) applies to this paragraph as it applies to regulation 37(7).

(4) An officer may exercise powers under this regulation only if the information sought to be obtained as a result is reasonably required in connection with the exercise by the designated authority for whom he acts of its functions under these Regulations.

(5) In this regulation, "premises" means any premises other than premises used only as a dwelling.

Entry to premises under warrant

39.—(1) A justice may issue a warrant under this paragraph if satisfied on information on oath given by an officer that there are reasonable grounds for believing that the first, second or third set of conditions is satisfied.

(2) The first set of conditions is—

(a) that there is on the premises specified in the warrant recorded information in relation to which a requirement could be imposed under regulation 37(1)(b); and

(b) that if such a requirement were to be imposed—

(i) it would not be complied with; or

(ii) the recorded information to which it relates would be removed, tampered with or destroyed.

(3) The second set of conditions is—

(a) that a person on whom a requirement has been imposed under regulation 37(1)(b) has failed (wholly or in part) to comply with it; and

(b) that there is on the premises specified in the warrant recorded information which has been required to be produced.

(4) The third set of conditions is—

(a) that an officer has been obstructed in the exercise of a power under regulation 38; and

(b) that there is on the premises specified in the warrant recorded information or cash which could be inspected under regulation 38(1)(d) or (f).

(5) A justice may issue a warrant under this paragraph if satisfied on information on oath given by an officer that there are reasonable grounds for suspecting that—

(a) an offence under these Regulations has been, is being or is about to be committed by a relevant person; and

(b) there is on the premises specified in the warrant recorded information relevant to whether that offence has been, or is being or is about to be committed.

(6) A warrant issued under this regulation shall authorise an officer—

(a) to enter the premises specified in the warrant;

(b) to search the premises and take possession of any recorded information or anything appearing to be recorded information specified in the warrant or to take, in relation to any such recorded information, any other steps which may appear to be necessary for preserving it or preventing interference with it;

(c) to take copies of, or extracts from, any recorded information specified in the warrant;

(d) to require any person on the premises to provide an explanation of any recorded information appearing to be of the kind specified in the warrant or to state where it may be found;

(e) to use such force as may reasonably be necessary.

(7) Where a warrant is issued by a justice under paragraph (1) or (5) on the basis of information given by an officer of the Authority, for "an officer" in paragraph (6) substitute "a constable".

(8) In paragraphs (1), (5) and (7), "justice" means—

(a) in relation to England and Wales, a justice of the peace;

(b) in relation to Scotland, a justice within the meaning of section 307 of the Criminal Procedure (Scotland) Act 1995(**bv**) (interpretation);

(c) in relation to Northern Ireland, a lay magistrate.

(9) In the application of this regulation to Scotland, the references in paragraphs (1) and (5) to information on oath are to be read as references to evidence on oath.

Failure to comply with information requirement

40.—(1) If, on an application made by—

(a) a designated authority; or

(b) a local weights and measures authority or DETI pursuant to arrangements made with the OFT—

(i) by or on behalf of the authority; or

(ii) by DETI,

it appears to the court that a person (the "information defaulter") has failed to do something that he was required to do under regulation 37(1), the court may make an order under this regulation.

(2) An order under this regulation may require the information defaulter—

(a) to do the thing that he failed to do within such period as may be specified in the order;

(b) otherwise to take such steps to remedy the consequences of the failure as may be so specified.

(3) If the information defaulter is a body corporate, a partnership or an unincorporated body of persons which is not a partnership, the order may require any officer of the body corporate, partnership or body, who is (wholly or partly) responsible for the failure to meet such costs of the application as are specified in the order.

(4) In this regulation, "court" means—

(a) in England and Wales and Northern Ireland, the High Court or the county court;

(b) in Scotland, the Court of Session or the sheriff.

Powers of relevant officers

41.—(1) A relevant officer may only exercise powers under regulations 37 to 39 pursuant to arrangements made with the OFT—

(a) by or on behalf of the local weights and measures authority of which he is an officer ("his authority"); or

(b) by DETI.

(2) Anything done or omitted to be done by, or in relation to, a relevant officer in the exercise or purported exercise of a power in this Part shall be treated for all purposes as having been done or omitted to be done by, or in relation to, an officer of the OFT.

(3) Paragraph (2) does not apply for the purposes of any criminal proceedings brought against the relevant officer, his authority, DETI or the OFT, in respect of anything done or omitted to be done by the officer.

(4) A relevant officer shall not disclose to any person other than the OFT and his authority or, as the case may be, DETI information obtained by him in the exercise of such powers unless—

(a) he has the approval of the OFT to do so; or

(b) he is under a duty to make the disclosure.

Civil penalties, review and appeals

Power to impose civil penalties

42.—(1) A designated authority may impose a penalty of such amount as it considers appropriate on a relevant person who fails to comply with any requirement in regulation 7(1), (2) or (3), 8(1) or (3), 9(2), 10(1), 11(1), 14(1), 15(1) or (2), 16(1), (2), (3) or (4), 19(1), (4), (5) or (6), 20(1), (4) or (5), 21, 26, 27(4) or 33 or a direction made under regulation 18 and, for this purpose, "appropriate" means effective, proportionate and dissuasive.

(2) The designated authority must not impose a penalty on a person under paragraph (1) where there are reasonable grounds for it to be satisfied that the person took all reasonable steps and exercised all due diligence to ensure that the requirement would be complied with.

(3) In deciding whether a person has failed to comply with a requirement of these Regulations, the designated authority must consider whether he followed any relevant guidance which was at the time—

(a) issued by a supervisory authority or any other appropriate body;

(b) approved by the Treasury; and

(c) published in a manner approved by the Treasury as suitable in their opinion to bring the guidance to the attention of persons likely to be affected by it.

(4) In paragraph (3), an "appropriate body" means any body which regulates or is representative of any trade, profession, business or employment carried on by the alleged offender.

(5) Where the Commissioners decide to impose a penalty under this regulation, they must give the person notice of—

(a) their decision to impose the penalty and its amount;

(b) the reasons for imposing the penalty;

(c) the right to a review under regulation 43; and

(d) the right to appeal under regulation 44(1)(a).

(6) Where the Authority, the OFT or DETI proposes to impose a penalty under this regulation, it must give the person notice of—

(a) its proposal to impose the penalty and the proposed amount;

(b) the reasons for imposing the penalty; and

(c) the right to make representations to it within a specified period (which may not be less than 28 days).

(7) The Authority, the OFT or DETI, as the case may be, must then decide, within a reasonable period, whether to impose a penalty under this regulation and it must give the person notice of—

(a) its decision not to impose a penalty; or

(b) the following matters—

(i) its decision to impose a penalty and the amount;

(ii) the reasons for its decision; and

(iii) the right to appeal under regulation 44(1)(b).

(8) A penalty imposed under this regulation is payable to the designated authority which imposes it.

Review procedure

43.—(1) This regulation applies to decisions of the Commissioners made under—

(a) regulation 29, to refuse to register an applicant;

(b) regulation 30, to cancel the registration of a registered person; and

(c) regulation 42, to impose a penalty.

(2) Any person who is the subject of a decision to which this regulation applies may by notice to the Commissioners require them to review that decision.

(3) The Commissioners need not review any decision unless the notice requiring the review is given within 45 days beginning with the date on which they first gave notice of the decision to the person requiring the review.

(4) Where the Commissioners are required under this regulation to review any decision they must either—

(a) confirm the decision; or

(b) withdraw or vary the decision and take such further steps (if any) in consequence of the withdrawal or variation as they consider appropriate.

(5) Where the Commissioners do not, within 45 days beginning with the date on which the review was required by a person, give notice to that person of their determination of the review, they are to be taken for the purposes of these Regulations to have confirmed the decision.

Appeals

44.—(1) A person may appeal from a decision by—

(a) the Commissioners on a review under regulation 43; and

(b) the Authority, the OFT or DETI under regulation 34 or 42.

(2) An appeal from a decision by—

(a) the Commissioners is to a VAT and duties tribunal(**bw**);

(b) the Authority is to the Financial Services and Markets Tribunal(**bx**);

(c) the OFT is to the Consumer Credit Appeals Tribunal(**by**); and

(d) DETI is to the High Court.

(3) The provisions of Part 5 of the Value Added Tax Act 1994(**bz**) (appeals), subject to the modifications set out in paragraph 1 of Schedule 5, apply in respect of appeals to a VAT and duties tribunal made under this regulation as they apply in respect of appeals made to such a tribunal under section 83 (appeals) of that Act.

(4) The provisions of Part 9 of the 2000 Act (hearings and appeals), subject to the modifications set out in paragraph 2 of Schedule 5, apply in respect of appeals to the Financial Services and Markets Tribunal made under this regulation as they apply in respect of references made to that Tribunal under that Act.

(5) Sections 40A (the Consumer Credit Appeals Tribunal), 41 (appeals to the Secretary of State under Part 3) and 41A (appeals from the Consumer Credit Appeals Tribunal) of the Consumer Credit Act 1974(**ca**) apply in respect of appeals to the Consumer Credit Appeal Tribunal made under this regulation as they apply in respect of appeals made to that Tribunal under section 41 of that Act.

(6) A VAT and duties tribunal hearing an appeal under paragraph (2) has the power to—

(a) quash or vary any decision of the supervisory authority, including the power to reduce any penalty to such amount (including nil) as they think proper; and

(b) substitute their own decision for any decision quashed on appeal.

(7) Notwithstanding paragraph (2)(c), until the coming into force of section 55 of the Consumer Credit Act 2006(**cb**) (the Consumer Credit Appeals Tribunal), an appeal from a decision by the OFT is to the Financial Services and Markets Tribunal and, for these purposes, the coming into force of that section shall not affect—

(a) the hearing and determination by the Financial Service and Markets Tribunal of an appeal commenced before the coming into force of that section ("the original appeal"); or

(b) any appeal against the decision of the Financial Services and Markets Tribunal with respect to the original appeal.

(8) The modifications in Schedule 5 have effect for the purposes of appeals made under this regulation.

Criminal offences

Offences

45.—(1) A person who fails to comply with any requirement in regulation 7(1), (2) or (3), 8(1) or (3), 9(2), 10(1), 11(1)(a), (b) or (c), 14(1), 15(1) or (2), 16(1), (2), (3) or (4), 19(1), (4), (5) or (6), 20(1), (4) or (5), 21, 26, 27(4) or 33, or a direction made under regulation 18, is guilty of an offence and liable—

(a) on summary conviction, to a fine not exceeding the statutory maximum;

(bz) 1994 c. 23.

(ca) Sections 40A and 41A were inserted by respectively sections 55 and 57 of the Consumer Credit Act 2006 and section 41 was amended by section 56 of that Act.

(cb) 2006 c. 14.

(b) on conviction on indictment, to imprisonment for a term not exceeding two years, to a fine or to both.

(2) In deciding whether a person has committed an offence under paragraph (1), the court must consider whether he followed any relevant guidance which was at the time—

(a) issued by a supervisory authority or any other appropriate body;

(b) approved by the Treasury; and

(c) published in a manner approved by the Treasury as suitable in their opinion to bring the guidance to the attention of persons likely to be affected by it.

(3) In paragraph (2), an "appropriate body" means any body which regulates or is representative of any trade, profession, business or employment carried on by the alleged offender.

(4) A person is not guilty of an offence under this regulation if he took all reasonable steps and exercised all due diligence to avoid committing the offence.

(5) Where a person is convicted of an offence under this regulation, he shall not also be liable to a penalty under regulation 42.

Prosecution of offences

46.—(1) Proceedings for an offence under regulation 45 may be instituted by—

(a) the Director of Revenue and Customs Prosecutions or by order of the Commissioners;

(b) the OFT;

(c) a local weights and measures authority;

(d) DETI;

(e) the Director of Public Prosecutions; or

(f) the Director of Public Prosecutions for Northern Ireland.

(2) Proceedings for an offence under regulation 45 may be instituted only against a relevant person or, where such a person is a body corporate, a partnership or an unincorporated association, against any person who is liable to be proceeded against under regulation 47.

(3) Where proceedings under paragraph (1) are instituted by order of the Commissioners, the proceedings must be brought in the name of an officer of Revenue and Customs.

(4) Where a local weights and measures authority in England or Wales proposes to institute proceedings for an offence under regulation 45 it must give the OFT notice of the intended proceedings, together with a summary of the facts on which the charges are to be founded.

(5) A local weights and measures authority must also notify the OFT of the outcome of the proceedings after they are finally determined.

(6) A local weights and measures authority must, whenever the OFT requires, report in such form and with such particulars as the OFT requires on the exercise of its functions under these Regulations.

(7) Where the Commissioners investigate, or propose to investigate, any matter with a view to determining—

(a) whether there are grounds for believing that an offence under regulation 45 has been committed by any person; or

(b) whether such a person should be prosecuted for such an offence,

that matter is to be treated as an assigned matter within the meaning of section 1(1) of the Customs and Excise Management Act 1979(**cc**).

(cc) 1979 c. 2. There are amendments to section 1 not relevant to these Regulations.

(8) Paragraphs (1) and (3) to (6) do not extend to Scotland.

Offences by bodies corporate etc.

47.—(1) If an offence under regulation 45 committed by a body corporate is shown—

(a) to have been committed with the consent or the connivance of an officer of the body corporate; or

(b) to be attributable to any neglect on his part,

the officer as well as the body corporate is guilty of an offence and liable to be proceeded against and punished accordingly.

(2) If an offence under regulation 45 committed by a partnership is shown—

(a) to have been committed with the consent or the connivance of a partner; or

(b) to be attributable to any neglect on his part,

the partner as well as the partnership is guilty of an offence and liable to be proceeded against and punished accordingly.

(3) If an offence under regulation 45 committed by an unincorporated association (other than a partnership) is shown—

(a) to have been committed with the consent or the connivance of an officer of the association; or

(b) to be attributable to any neglect on his part,

that officer as well as the association is guilty of an offence and liable to be proceeded against and punished accordingly.

(4) If the affairs of a body corporate are managed by its members, paragraph (1) applies in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body.

(5) Proceedings for an offence alleged to have been committed by a partnership or an unincorporated association must be brought in the name of the partnership or association (and not in that of its members).

(6) A fine imposed on the partnership or association on its conviction of an offence is to be paid out of the funds of the partnership or association.

(7) Rules of court relating to the service of documents are to have effect as if the partnership or association were a body corporate.

(8) In proceedings for an offence brought against the partnership or association—

(a) section 33 of the Criminal Justice Act 1925(**cd**) (procedure on charge of offence against corporation) and Schedule 3 to the Magistrates' Courts Act 1980(**ce**) (corporations) apply as they do in relation to a body corporate;

(b) section 70 (proceedings against bodies corporate) of the Criminal Procedure (Scotland) Act 1995(**cf**) applies as it does in relation to a body corporate;

(c) section 18 of the Criminal Justice (Northern Ireland) Act 1945(**cg**) (procedure on charge) and Schedule 4 to the Magistrates' Courts (Northern Ireland) Order 1981(**ch**) (corporations) apply as they do in relation to a body corporate.

(9) In this regulation—

"officer"—

(a) in relation to a body corporate, means a director, manager, secretary, chief executive, member of the committee of management, or a person purporting to act in such a capacity; and

(b) in relation to an unincorporated association, means any officer of the association or any member of its governing body, or a person purporting to act in such capacity; and

"partner" includes a person purporting to act as a partner.

PART 6

MISCELLANEOUS

Recovery of charges and penalties through the court

48. Any charge or penalty imposed on a person by a supervisory authority under regulation 35(1) or 42(1) is a debt due from that person to the authority, and is recoverable accordingly.

Obligations on public authorities

49.—(1) The following bodies and persons must, if they know or suspect or have reasonable grounds for knowing or suspecting that a person is or has engaged in money laundering or terrorist financing, as soon as reasonably practicable inform the Serious Organised Crime Agency—

(a) the Auditor General for Scotland;

(b) the Auditor General for Wales;

(c) the Authority;

(d) the Bank of England;

(e) the Comptroller and Auditor General;

(f) the Comptroller and Auditor General for Northern Ireland;

(g) the Gambling Commission;

(h) the OFT;

(i) the Official Solicitor to the Supreme Court;

(j) the Pensions Regulator;

(k) the Public Trustee;

(l) the Secretary of State, in the exercise of his functions under enactments relating to companies and insolvency;

(m) the Treasury, in the exercise of their functions under the 2000 Act;

(n) the Treasury Solicitor;

(o) a designated professional body for the purposes of Part 20 of the 2000 Act (provision of financial services by members of the professions);

(p) a person or inspector appointed under section 65 (investigations on behalf of Authority) or 66 (inspections and special meetings) of the Friendly Societies Act 1992(**ci**);

(q) an inspector appointed under section 49 of the Industrial and Provident Societies Act 1965(**cj**) (appointment of inspectors) or section 18 of the Credit Unions Act 1979(**ck**) (power to appoint inspector);

(r) an inspector appointed under section 431 (investigation of a company on its own application), 432 (other company investigations), 442 (power to investigate company ownership) or 446 (investigation of share dealing) of the Companies Act 1985(**cl**) or under Article 424, 425, 435 or 439 of the Companies (Northern Ireland) Order 1986(**cm**);

(s) a person or inspector appointed under section 55 (investigations on behalf of Authority) or 56 (inspections and special meetings) of the Building Societies Act 1986(**cn**);

(t) a person appointed under section 167 (appointment of persons to carry out investigations), 168(3) or (5) (appointment of persons to carry out investigations in particular cases), 169(1)(b) (investigations to support overseas regulator) or 284 (power to investigate affairs of a scheme) of the 2000 Act, or under regulations made under section 262(2)(k) (open-ended investment companies) of that Act, to conduct an investigation; and

(u) a person authorised to require the production of documents under section 447 of the Companies Act 1985 (Secretary of State's power to require production of documents), Article 440 of the Companies (Northern Ireland) Order 1986 or section 84 of the Companies Act 1989(**co**) (exercise of powers by officer).

(2) A disclosure made under paragraph (1) is not to be taken to breach any restriction on the disclosure of information however imposed.

Transitional provisions: requirement to be registered

50.—(1) Regulation 26 does not apply to an existing money service business, an existing trust or company service provider or an existing high value dealer until—

(a) where it has applied in accordance with regulation 27 before the specified date for registration in a register maintained under regulation 25(1) (a "new register")—

(i) the date it is included in a new register following the determination of its application by the Commissioners; or

(ii) where the Commissioners give it notice under regulation 29(2)(b) of their decision not to register it, the date on which the Commissioners state that the decision takes effect or, where a statement is included in accordance with paragraph (3)(b), the time at which the Commissioners give it such notice;

(b) in any other case, the specified date.

(2) The specified date is—

(a) in the case of an existing money service business, 1st February 2008;

(b) in the case of an existing trust or company service provider, 1st April 2008;

(c) in the case of an existing high value dealer, the first anniversary which falls on or after 1st January 2008 of the date of its registration in a register maintained under regulation 10 of the Money Laundering Regulations 2003.

(3) In the case of an application for registration in a new register made before the specified date by an existing money service business, an existing trust or company service provider or an existing high value dealer, the Commissioners must include in a notice given to it under regulation 29(2)(b)—

(a) the date on which their decision is to take effect; or

(b) if the Commissioners consider that the interests of the public require their decision to have immediate effect, a statement to that effect and the reasons for it.

(4) In the case of an application for registration in a new register made before the specified date by an existing money services business or an existing trust or company service provider, the Commissioners must give it a notice under regulation 29(2) by—

(a) in the case of an existing money service business, 1st June 2008;

(b) in the case of an existing trust or company service provider, 1st July 2008; or

(c) where applicable, 45 days beginning with the date on which they receive any further information required under regulation 27(3).

(5) In this regulation—

"existing money service business" and an "existing high value dealer" mean a money service business or a high value dealer which, immediately before 15th December 2007, was included in a register maintained under regulation 10 of the Money Laundering Regulations 2003;

"existing trust or company service provider" means a trust or company service provider carrying on business in the United Kingdom immediately before 15th December 2007.

Minor and consequential amendments

51. Schedule 6, which contains minor and consequential amendments to primary and secondary legislation, has effect.

Signatory text

Alan Campbell
Frank Roy
Two Lords Commissioners of
Her Majesty's Treasury

24th July 2007

SCHEDULE 1

Regulation 3(3)(a)

ACTIVITIES LISTED IN POINTS 2 TO 12 AND 14 OF ANNEX I TO THE BANKING CONSOLIDATION DIRECTIVE

2. Lending including, inter alia: consumer credit, mortgage credit, factoring, with or without recourse, financing of commercial transactions (including forfeiting).

3. Financial leasing.

4. Money transmission services.

5. Issuing and administering means of payment (e.g. credit cards, travellers' cheques and bankers' drafts).

6. Guarantees and commitments.

7. Trading for own account or for account of customers in:

(a) money market instruments (cheques, bills, certificates of deposit, etc.);

(b) foreign exchange;

(c) financial futures and options;

(d) exchange and interest-rate instruments; or

(e) transferable securities.

8. Participation in securities issues and the provision of services related to such issues.

9. Advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertakings.

10. Money broking.

11. Portfolio management and advice.

12. Safekeeping and administration of securities.

14. Safe custody services

SCHEDULE 2

Regulations 4(1)(e) and (2), 13(6) and (8) and 14(5).

FINANCIAL ACTIVITY, SIMPLIFIED DUE DILIGENCE AND POLITICALLY EXPOSED PERSONS

Financial activity on an occasional or very limited basis

1. For the purposes of regulation 4(1)(e) and (2), a person is to be considered as engaging in financial activity on an occasional or very limited basis if all the following conditions are fulfilled—

(a) the person's total annual turnover in respect of the financial activity does not exceed £64,000;

(b) the financial activity is limited in relation to any customer to no more than one transaction exceeding 1,000 euro, whether the transaction is carried out in a single operation, or a series of operations which appear to be linked;

(c) the financial activity does not exceed 5% of the person's total annual turnover;

(d) the financial activity is ancillary and directly related to the person's main activity;

(e) the financial activity is not the transmission or remittance of money (or any representation of monetary value) by any means;

(f) the person's main activity is not that of a person falling within regulation 3(1)(a) to (f) or (h);

(g) the financial activity is provided only to customers of the person's main activity and is not offered to the public.

Simplified due diligence

2. For the purposes of regulation 13(6), the conditions are—

(a) the authority has been entrusted with public functions pursuant to the Treaty on the European Union(**cp**), the Treaties on the European Communities or Community secondary legislation;

(b) the authority's identity is publicly available, transparent and certain;

(c) the activities of the authority and its accounting practices are transparent;

(d) either the authority is accountable to a Community institution or to the authorities of an EEA state, or otherwise appropriate check and balance procedures exist ensuring control of the authority's activity.

3. For the purposes of regulation 13(8), the conditions are—

(a) the product has a written contractual base;

(b) any related transaction is carried out through an account of the customer with a credit institution which is subject to the money laundering directive or with a credit institution situated in a non-EEA state which imposes requirements equivalent to those laid down in that directive;

(c) the product or related transaction is not anonymous and its nature is such that it allows for the timely application of customer due diligence measures where there is a suspicion of money laundering or terrorist financing;

(d) the product is within the following maximum threshold—

(i) in the case of insurance policies or savings products of a similar nature, the annual premium is no more than 1,000 euro or there is a single premium of no more than 2,500 euro;

(ii) in the case of products which are related to the financing of physical assets where the legal and beneficial title of the assets is not transferred to the customer until the termination of the contractual relationship (whether the transaction is carried out in a single operation or in several operations which appear to be linked), the annual payments do not exceed 15,000 euro;

(iii) in all other cases, the maximum threshold is 15,000 euro;

(e) the benefits of the product or related transaction cannot be realised for the benefit of third parties, except in the case of death, disablement, survival to a predetermined advanced age, or similar events;

(f) in the case of products or related transactions allowing for the investment of funds in financial assets or claims, including insurance or other kinds of contingent claims—

(i) the benefits of the product or related transaction are only realisable in the long term;

(ii) the product or related transaction cannot be used as collateral; and

(iii) during the contractual relationship, no accelerated payments are made, surrender clauses used or early termination takes place.

Politically exposed persons

4.—(1) For the purposes of regulation 14(5)—

(a) individuals who are or have been entrusted with prominent public functions include the following—

(i) heads of state, heads of government, ministers and deputy or assistant ministers;

(ii) members of parliaments;

(iii) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not generally subject to further appeal, other than in exceptional circumstances;

(iv) members of courts of auditors or of the boards of central banks;

(v) ambassadors, chargés d'affaires and high-ranking officers in the armed forces; and

(vi) members of the administrative, management or supervisory bodies of state-owned enterprises;

(b) the categories set out in paragraphs (i) to (vi) of sub-paragraph (a) do not include middle-ranking or more junior officials;

(c) immediate family members include the following—

(i) a spouse;

(ii) a partner;

(iii) children and their spouses or partners; and

(iv) parents;

(d) persons known to be close associates include the following—

(i) any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a person referred to in regulation 14(5)(a); and

(ii) any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person referred to in regulation 14(5)(a).

(2) In paragraph (1)(c), "partner" means a person who is considered by his national law as equivalent to a spouse.

SCHEDULE 3 Regulations 17(2)(b), 23(1)(c) and 32(4)

PROFESSIONAL BODIES

PART 1

1. Association of Chartered Certified Accountants

2. Council for Licensed Conveyancers

3. Faculty of Advocates

4. General Council of the Bar

5. General Council of the Bar of Northern Ireland

6. Institute of Chartered Accountants in England and Wales

7. Institute of Chartered Accountants in Ireland

8. Institute of Chartered Accountants of Scotland

9. Law Society

10. Law Society of Scotland

11. Law Society of Northern Ireland

PART 2

12. Association of Accounting Technicians

13. Association of International Accountants

14. Association of Taxation Technicians

15. Chartered Institute of Management Accountants

16. Chartered Institute of Public Finance and Accountancy

17. Chartered Institute of Taxation

18. Faculty Office of the Archbishop of Canterbury

19. Insolvency Practitioners Association

20. Institute of Certified Bookkeepers

21. Institute of Financial Accountants

SCHEDULE 4

Regulation 37(2)

CONNECTED PERSONS

Corporate bodies

1. If the relevant person is a body corporate ("BC"), a person who is or has been—

(a) an officer or manager of BC or of a parent undertaking of BC;

(b) an employee of BC;

(c) an agent of BC or of a parent undertaking of BC.

Partnerships

2. If the relevant person is a partnership, a person who is or has been a member, manager, employee or agent of the partnership.

Unincorporated associations

3. If the relevant person is an unincorporated association of persons which is not a partnership, a person who is or has been an officer, manager, employee or agent of the association.

Individuals

4. If the relevant person is an individual, a person who is or has been an employee or agent of that individual.

SCHEDULE 5 Regulation 44(8)

MODIFICATIONS IN RELATION TO APPEALS

PART 1

Primary legislation

The Value Added Tax Act 1994 (c. 23)

1. Part 5 of the Value Added Tax Act 1994 (appeals) is modified as follows—

(a) omit section 84; and

(b) in paragraphs (1)(a), (2)(a) and (3)(a) of section 87, omit ", or is recoverable as, VAT".

The Financial Services and Markets Act 2000 (c. 8)

2. Part 9 of the 2000 Act (hearings and appeals) is modified as follows—

(a) in the application of section 133 and Schedule 13 to any appeal commenced before the coming into force of section 55 of the Consumer Credit Act 2006, for all the references to "the Authority", substitute "the Authority or the OFT (as the case may be)";

(b) in section 133(1)(a) for "decision notice or supervisory notice in question" substitute "notice under regulation 34(5) or (9) or 42(7) of the Money Laundering Regulations 2007";

(c) in section 133 omit subsections (6), (7), (8) and (12); and

(d) in section 133(9) for "decision notice" in both places where it occurs substitute "notice under regulation 34(5) or (9) or 42(7) of the Money Laundering Regulations 2007".

PART 2

Secondary legislation

The Financial Services and Markets Tribunal Rules 2001

3. In the application of the Financial Services and Markets Tribunal Rules 2001(**cq**) to any appeal commenced before the coming into force of section 55 of the Consumer Credit Act 2006, for all the references to "the Authority" substitute "the Authority or the OFT (as the case may be)".

(cq) S.I.2001/2476.

SCHEDULE 6 Regulation 51

MINOR AND CONSEQUENTIAL AMENDMENTS

PART 1

Primary legislation

The Value Added Tax Act 1994 (c. 23)

1. In section 83 of the Value Added Tax Act 1994(**cr**) (appeals), omit paragraph (zz).

The Northern Ireland Act 1998 (c. 47)

2. In paragraph 25 of Schedule 3 to the Northern Ireland Act 1998(**cs**) (reserved matters), for "2003" substitute "2007".

The Criminal Justice and Police Act 2001 (c. 16)

3. In Part 1 of Schedule 1 to the Criminal Justice and Police Act 2001(**ct**) (powers of seizure to which section 50 of the 2001 Act applies), after paragraph 73I insert—

"**The Money Laundering Regulations 2007**

73J. The power of seizure conferred by regulation 39(6) of the Money Laundering Regulations 2007 (entry to premises under warrant)."

PART 2

Secondary legislation

The Independent Qualified Conveyancers (Scotland) Regulations 1997

4. Regulation 28 of the Independent Qualified Conveyancers (Scotland) Regulations 1997(**cu**) is revoked.

The Executry Practitioners (Scotland) Regulations 1997

5. Regulation 26 of the Executry Practitioners (Scotland) Regulations 1997(**cv**) is revoked.

The Cross-Border Credit Transfers Regulations 1999

6. In regulation 12(2) of the Cross-Border Credit Transfers Regulations 1999(**cw**), for "2003" substitute "2007".

(cr) 1994 c. 23. Section 83(zz) was inserted by S.I. 2001/3541 and amended by S.I. 2003/3075.
(cs) 1998 c. 47. Paragraph 25 of Schedule 3 was amended by S.I. 2003/3075.
(ct) 2001 c. 16. Section 73I was inserted by the Animal Welfare Act 2006, section 64, Schedule 3, paragraph 14(3).
(cu) S.S.I. 1997/316.
(cv) S.S.I. 1997/317.
(cw) S.I. 1999/1876, amended by S.I. 2003/3075.

The Terrorism Act 2000 (Crown Servants and Regulators) Regulations 2001

7. In regulation 2 of the Terrorism Act 2000 (Crown Servants and Regulators) Regulations 2001(**cx**), in the definition of "relevant business", for "has the meaning given by regulation 2(2) of the Money Laundering Regulations 2003" substitute "means an activity carried on in the course of business by any of the persons listed in regulation 3(1)(a) to (h) of the Money Laundering Regulations 2007".

The Representation of the People (England and Wales) Regulations 2001

8. In regulation 114(3)(b) of the Representation of the People (England and Wales) Regulations 2001(**cy**), for "2003" substitute "2007".

The Representation of the People (Scotland) Regulations 2001

9. In regulation 113(3)(b) of the Representation of the People (Scotland) Regulations 2001(**cz**), for "2003" substitute "2007".

The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001

10. In article 72E(9) of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001(**da**), for "2003" substitute "2007".

The Proceeds of Crime Act 2002 (Failure to Disclose Money Laundering: Specified Training) Order 2003

11. In article 2 of the Proceeds of Crime Act 2002 (Failure to Disclose Money Laundering: Specified Training) Order 2003(**db**), for "regulation 3(1)(c)(ii) of the Money Laundering Regulations 2003" substitute "regulation 21 of the Money Laundering Regulations 2007".

The Public Contracts (Scotland) Regulations 2006

12. In regulation 23(1)(f) of the Public Contracts (Scotland) Regulations 2006(**dc**), for "2003" substitute "2007".

The Utilities Contracts (Scotland) Regulations 2006

13. In regulation 26(1)(f) of the Utilities Contracts (Scotland) Regulations 2006(**dd**), for "2003" substitute "2007".

The Public Contracts Regulations 2006

14. In regulation 23(1)(e) of the Public Contracts Regulations 2006(**de**), for "2003" substitute "2007".

(cx) S.I. 2001/192, amended by S.I. 2003/3075.
(cy) S.I. 2001/341, amended by S.I. 2002/1871, 2003/3075.
(cz) S.S.I. 2001/497, amended by S.I. 2002/1871, 2003/3075.
(da) S.I. 2001/544, amended by S.I. 2005/1518.
(db) S.I. 2003/171, amended by S.I. 2003/3075.
(dc) S.S.I. 2006/1.
(dd) S.S.I. 2006/2.
(de) S.I. 2006/5.

The Utilities Contracts Regulations 2006

15. In regulation 26(1)(e) of the Utilities Contracts Regulations 2006(**df**), for "2003" substitute "2007".

EXPLANATORY NOTE

(This note is not part of the Regulations)

These Regulations replace the Money Laundering Regulations 2003 (S.I. 2003/3075) with updated provisions which implement in part Directive 2005/60/EC (OJ No L 309, 25.11.2005, p.15) of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. A Transposition Note setting out how the main elements of this directive will be transposed into UK law is available from the Financial Services Team, HM Treasury, 1 Horse Guards Road, London SW1A 2HQ. An impact assessment has also been prepared. Copies of both documents have been placed in the library of each House of Parliament and are available on HM Treasury's website (www.hm-treasury.gov.uk).

The Regulations provide for various steps to be taken by the financial services sector and other persons to detect and prevent money laundering and terrorist financing. Obligations are imposed on "relevant persons" (defined in regulation 3 and subject to the exclusions in regulation 4), who are credit and financial institutions, auditors, accountants, tax advisers and insolvency practitioners, independent legal professionals, trust or company service providers, estate agents, high value dealers and casinos.

Relevant persons are required, when undertaking certain activities in the course of business, to apply customer due diligence measures where they establish a business relationship, carry out an occasional transaction, suspect money laundering or terrorist finance or doubt the accuracy of customer identification information (regulation 7). Customer due diligence measures (defined in regulation 5) consist of identifying and verifying the identity of the customer and any beneficial owner (defined in regulation 6) of the customer, and obtaining information on the purpose and intended nature of the business relationship. Relevant persons also have to undertake ongoing monitoring of their business relationships (regulation 8).

Regulation 9 sets out the general rule on the timing of the verification of the customer's identity and certain exceptions. Regulation 10 sets out when casinos must identify and verify their customers. Failure to apply such measures means that a person cannot establish or continue a business relationship with the customer concerned or undertake an occasional transaction (regulation 11). Regulation 12 provides an exception from the requirement to identify the beneficial owner for debt issues held in trust.

Relevant persons may apply simplified customer due diligence measures for the products, customers or transactions listed in regulation 13 and must apply enhanced measures in the four situations set out in regulation 14. Regulation 15 sets out the obligations on relevant persons in respect of their overseas branches and subsidiaries. Regulation 16 imposes obligations in respect of shell banks and anonymous accounts. Regulation 17 lists the persons on whom relevant persons can rely to perform customer due diligence measures. Regulation 18 provides for the Treasury to make directions where the Financial Action Task Force applies counter-measures to a non-EEA state.

(df) S.I. 2006/6.

Part 3 imposes obligations in respect of record-keeping (regulation 19), policies and procedures (regulation 20) and staff training (regulation 21).

Part 4 deals with supervision and registration. Regulation 23 allocates supervisory authorities for different relevant persons. Regulation 24 sets out the duties of supervisors. Money service businesses, high value dealers and trust or company service providers which are not otherwise registered are subject to a system of mandatory registration set out in regulations 25 to 30. Money service businesses and trust or company service providers must not be registered unless the business, its owners, its nominated officer and senior managers are fit and proper persons: regulation 28. Other sectors will only be required to register if the supervisor decides to maintain a register (regulations 33 and 34). Regulation 35 enables supervisors to impose charges on persons they supervise.

Part 5 provides enforcement powers for certain supervisors, including powers to obtain information and enter and inspect premises (regulations 37 to 41). Civil penalties may be imposed by these supervisors under regulation 42 on persons who fail to comply with the requirements of Parts 2, 3 and 4. Provision is made for reviews of and appeals against such penalties (regulations 43 and 44). Relevant persons who fail to comply with the requirements of Parts 2, 3 and 4 will also be guilty of a criminal offence: regulations 45 to 47. Persons convicted of a criminal offence may not also be liable to a civil penalty.

Part 6 contains provision for the recovery of penalties and charges through the court (regulation 48), imposes an obligation on certain public authorities to report suspicions of money laundering or terrorist financing (regulation 49) and makes transitional provision (regulation 50). Regulation 51 makes minor and consequential amendments to primary and secondary legislation.

附件 F

草擬《打擊洗錢及恐怖分子資金籌集(金融機構)條例草案》時所參考資料一覽表

條次	標題	參考資料
第 1 部	導言	
第 4 條	豁免承擔法律責任	● 《保險公司條例》(第 41 章)第 55A 條 ● 《電子交易條例》(第 553 章)第 51(3)條
第 2 部	關於就客戶作盡職審查及備存紀錄的規定	
第 7 條	有關當局可公布指引	● 《證券及期貨條例》(第 571 章)第 193(3)、399(5)、399(6)及 399(8)條
第 3 部	監管及調查	● 《證券及期貨條例》第 VIII 部
第 8 條	第 3 部的釋義	● 《證券及期貨條例》第 178 條
第 9 條	進入業務處所等作例行視察的權力	● 《證券及期貨條例》第 180(1)至 180(13)條
第 10 條	不遵從根據第 9 條施加的要求的罪行	● 《證券及期貨條例》第 180(14)至 180(16)條
第 11 條	有關當局可委任調查員	● 《證券及期貨條例》第 182 條
第 12 條	調查員要求交出紀錄或文件等的權力	● 《證券及期貨條例》第 183 條
第 13 條	不遵從根據第 12 條施加的要求的罪行	● 《證券及期貨條例》第 184 條
第 14 條	就根據第 9 或 12 條施加的要求不獲遵從而向原訟法庭提出申請	● 《證券及期貨條例》第 185 條
第 15 條	導致入罪的證據在法律程序中的使用	● 《證券及期貨條例》第 187 條
第 16 條	對紀錄或文件的聲稱留置權	● 《證券及期貨條例》第 188 條
第 17 條	裁判官手令	● 《證券及期貨條例》第 191 條

條次	標題	參考資料
第 18 條	交出在資訊系統等內的資料	● 《證券及期貨條例》第 189 條
第 19 條	查閱被檢取的紀錄或文件等	● 《證券及期貨條例》第 190 條
第 20 條	文件的銷毀等	● 《證券及期貨條例》第 192 條
第 4 部	有關當局採取的紀律行動	
第 21 條	有關當局可採取紀律行動	● 《證券及期貨條例》第 194 條
第 22 條	根據第 21 條行使權力的程序規定	● 《證券及期貨條例》第 198(1)及 198(2)條
第 23 條	有關當局如何行使施加罰款的權力的指引	● 《證券及期貨條例》第 199 條
第 5 部	對經營金錢服務的規管	
第 28 條	登記冊或登記冊內記項的核證複本獲接納為證據	● 《旅行代理商規例》(第 218A 章)第 5 條
第 39 條	持牌人有責任向關長具報詳情改變	● 《有組織及嚴重罪行條例》(第 455 章)第 24B(6)條
第 40 條	持牌人有責任向關長具報停業	● 《有組織及嚴重罪行條例》(第 455 章)第 24B(6)條
第 42 條	關長可採取紀律行動	● 反映第 21 條的規定
第 43 條	根據第 42 條行使權力的程序規定	● 反映第 22 條的規定
第 44 條	關長如何行使施加罰款的權力的指引	● 反映第 23 條的規定
第 46 條	進入和搜查處所的手令	● 《商品說明條例》(第 362 章)第 15、16 及 17(1)(a)條
第 47 條	獲授權人員拘捕及搜查等的權力	● 《商品說明條例》(第 362 章)第 16B 條及《警隊條例》(第 232 章)第 50(1)(b)條
第 48 條	保密	● 《證券及期貨條例》第 378 條
第 51 條	就牌照申請等提供虛假資料屬罪行	● 《證券及期貨條例》第 383 條

條次	標題	參考資料
第 52 條	檢控時限	● 《強制性公積金計劃條例》(第 485 章)第 43B 條
第 6 部	打擊洗錢及恐怖分子資金籌集(金融機構)覆核審裁處	● 《證券及期貨條例》第 VI 部
第 53 條	第 6 部的釋義	● 《證券及期貨條例》第 215 條
第 54 條	審裁處的設立	● 《證券及期貨條例》第 216(1)及 216(5)條
第 55 條	審裁處的組成	● 《證券及期貨條例》第 216(2)及 216(3)條
第 56 條	審裁處的主席及其他成員可獲酬金	● 《證券及期貨條例》第 216(6)條
第 57 條	附表 4 具有效力	● 《證券及期貨條例》第 216(4)條
第 58 條	要求覆核指明決定的申請	● 《證券及期貨條例》第 217(1)、217(3)、217(4)、217(5)及 217(6)條
第 59 條	審裁處作出的覆核裁定	● 《證券及期貨條例》第 218(2)、218(3)、218(5)及 218(7) 條
第 60 條	審裁處的權力	● 《證券及期貨條例》第 219 條
第 61 條	強迫提供的會導致入罪的證據的使用	● 《證券及期貨條例》第 220 條
第 62 條	審裁處處理的藐視罪	● 《證券及期貨條例》第 221 條
第 63 條	受保密權涵蓋的資料	● 《證券及期貨條例》第 222 條
第 64 條	訟費	● 《證券及期貨條例》第 223 條
第 65 條	審裁處的裁定的通知	● 《證券及期貨條例》第 224 條
第 66 條	審裁處命令的格式及證明	● 《證券及期貨條例》第 225 條
第 67 條	審裁處命令可在原訟法庭登記	● 《證券及期貨條例》第 226 條

條次	標題	參考資料
第 68 條	申請暫緩執行指明決定	● 《證券及期貨條例》第 227 條
第 69 條	申請暫緩執行審裁處的裁定	● 《證券及期貨條例》第 228 條
第 70 條	獲許可向上訴法庭提出上訴	● 《證券及期貨條例》第 229(1)條 ● 《高等法院條例》(第 4 章)第 14AA(1)、14AA(3)及 14AA(4)條
第 71 條	上訴法庭的權力	● 《證券及期貨條例》第 229(2)、229(3)及 229(4)條
第 72 條	上訴不暫緩執行審裁處的裁定	● 《證券及期貨條例》第 230 條
第 73 條	無其他上訴權	● 《證券及期貨條例》第 231 條
第 74 條	指明決定的生效時間	● 《證券及期貨條例》第 232 條
第 75 條	終審法院首席法官訂立規則的權力	● 《證券及期貨條例》第 233(b)及 233(c)條
第 7 部	雜項條文	
第 76 條	行政長官會同行政會議訂立規例	● 《證券及期貨條例》第 376 條
第 77 條	舉證準則	● 《證券及期貨條例》第 387 條
第 78 條	有關當局就某些罪行提出檢控	● 《證券及期貨條例》第 388 條
第 80 條	法律專業保密權	● 《證券及期貨條例》第 380(4)及 380(5)條
第 81 條	關於在本條例生效前經營業務的貨幣兌換商及匯款代理人的過渡性條文	● 英國《規例》50

條次	標題	參考資料
附表 2	關於就客戶作盡職審查及備存紀錄的規定	
第 1 條	“實益擁有人”	● 英國《規例》6 ● 現行指引： – 金管局《補充文件》“闡釋備註”的“詞彙”； – 保監處《指引》第 5.2 段註 6； – 證監會《指引》沒有提述“實益擁有人”一詞，但《指引》第 6.1.2(c)及 6.4.1 分節訂明須識別的客戶類別。
	“對等司法管轄區”	● 現行指引： – 金管局《補充文件》“闡釋備註”的第 14 節； – 保監處《指引》第 6.6.6.4 段； – 證監會《指引》“詞彙”為“同等標準的地區”所下的定義。

條次	標題	參考資料
	“政治人物”	● 英國《規例》附表 2 第 4 條 ● 現行指引： – 金管局《補充文件》第 10.2 及 10.3 段； – 保監處《指引》第 6.6.5.1 及 6.6.5.2 段； – 證監會《指引》“詞彙”為“政界人士”所下的定義，以及證監會《指引》第 6.9.1 及 6.9.3 分節。
第 2 條	何謂客戶盡職審查措施	● 英國《規例》5 ● 現行指引： – 金管局《補充文件》第 3.2 段； – 保監處《指引》第 6.1.1 段； – 證監會《指引》第 6.1.2 分節。
第 3 條	何時須執行客戶盡職審查措施	● 英國《規例》7 及 9 ● 現行指引： – 金管局《補充文件》第 3.6、3.7、3.10 及 3.11 段； – 保監處《指引》第 6.1.9 至 6.1.13 段； – 證監會《指引》第 6.1.9 及 6.1.10 分節。

條次	標題	參考資料
第 4 條	簡化客戶盡職審查	● 英國《規例》13 ● 現行指引： – 金管局《補充文件》第 4.2 至 4.4、4.6 段及第 7 節； – 保監處《指引》第 6.1.4、6.3.2 及 6.3.4 段； – 證監會《指引》第 6.2.3、6.2.4、6.5 及 6.6 分節。
第 5 條	持續監察業務關係的責任	● 英國《規例》8 ● 現行指引： – 金管局《補充文件》第 3.8 段及第 13 節； – 保監處《指引》第 6.7.1 段； – 證監會《指引》第 6.1.2(d)、6.1.11 至 6.1.13 及 6.2.8 分節。
第 6 條	關於先前客戶的條文	● 現行指引： – 金管局《補充文件》第 12 節； – 保監處《指引》第 6.7 段； – 證監會《指引》第 6.1.12 及 6.1.13 分節。
第 7 條	關於先前受代理的銀行的條文	● 須與第 14 條一併閱讀

條次	標題	參考資料
第 9 條	客戶沒有為身分識別的目的而現身時適用的特別規定	● 英國《規例》14(2) ● 現行指引： – 金管局《補充文件》第 8 節； – 保監處《指引》第 6.6.4 段； – 證監會《指引》第 6.10 分節。
第 10 條	客戶屬政治人物時適用的特別規定	● 英國《規例》14(4) ● 現行指引： – 金管局《補充文件》第 10 節； – 保監處《指引》第 6.6.5 段； – 證監會《指引》第 6.9 分節。
第 11 條	關於保險單的特別規定	● 保監處《指引》第 6.2.3 段
第 12 條	關於電傳轉賬的特別規定	● 金管局《補充文件》第 3.14 段及第 9 節
第 13 條	關於匯款交易的特別規定	● 《有組織及嚴重罪行條例》第 24C 條及附表 6
第 14 條	關於代理銀行服務關係的特別規定	● 英國《規例》14(3) ● 金管局《補充文件》第 11 節
第 15 條	關於其他高度風險情況的規定	● 英國《規例》14(1)(b) ● 現行指引： – 金管局《補充文件》第 2.2 段； – 保監處《指引》第 6.6.1 及 6.6.2 段； – 證監會《指引》第 6.2.2、6.2.7 及 6.2.8 分節。

條次	標題	參考資料
第 16 條	匿名戶口等	● 英國《規例》16(3) ● 現行指引： – 金管局《補充文件》第 5.1 段； – 保監處《指引》第 6.1.1 段； – 證監會《指引》第 6.1.7 分節。
第 17 條	與空殼銀行的代理銀行關係	● 英國《規例》16 ● 金管局《補充文件》第 11.6 段
第 18 條	藉著中介人執行客戶盡職審查措施	● 英國《規例》17 ● 現行指引： – 金管局《補充文件》第 6 節； – 保監處《指引》第 6.8 段； – 證監會《指引》第 6.11 分節。
第 19 條	金融機構須設立程序	● 現行指引： – 金管局《補充文件》第 2.2 及 10.4 段； – 保監處《指引》第 5.2 段； – 證監會《指引》第 4.2、5.1 及 6.9.4 分節。
第 20 條	備存紀錄的責任	● 英國《規例》19 ● 現行指引： – 金管局《補充文件》第 7.4 段； – 保監處《指引》第 7.2.1 及 7.2.2 段； – 證監會《指引》第 7.4、8.1 及 8.2 分節。

條次	標題	參考資料
第 21 條	紀錄備存形式	● 現行指引： – 金管局《補充文件》第 7.5 段； – 保監處《指引》第 7.2.5 段。
第 22 條	責任擴及在香港以外的分行及附屬公司	● 英國《規例》15 ● 現行指引： – 金管局《補充文件》第 1.7 段； – 保監處《指引》第 1.4 、 4.1(a) 及 4.1(f)段； – 證監會《指引》第 4.3 分節。
第 23 條	金融機構須防止違反本附表第 2 或 3 部	● 《證券及期貨條例》第 279 條 ● 金管局《指引》第 4.3 段及金管局《補充文件》第 16.2 段；
附表 4	關於打擊洗錢及恐怖分子資金籌集(金融機構)覆核審裁處的條文	● 《證券及期貨條例》附表 8
第 1 條	釋義	● 《證券及期貨條例》附表 8 第 1 條
第 2 條	委出委員團	● 《證券及期貨條例》附表 8 第 2、3、4、5 及 6 條
第 3 條	主席的任期	● 《證券及期貨條例》附表 8 第 8、9 及 10 條
第 4 條	普通成員的委任	● 《證券及期貨條例》附表 8 第 12、13、14 及 15 條
第 5 條	關乎主席及普通成員的進一步規定	● 《證券及期貨條例》附表 8 第 11 條
第 6 條	程序	● 《證券及期貨條例》附表 8 第 16、17、18、20、21、22 及 23 條
第 7 條	初步會議	● 《證券及期貨條例》附表 8 第 25、26 及 27 條
第 8 條	同意令	● 《證券及期貨條例》附表 8 第 28、29 及 30 條

條次	標題	參考資料
第 9 條	主席作爲審裁處唯一成員	● 《證券及期貨條例》附表 8 第 31、32、33、34 及 35 條
第 10 條	特權和豁免權	● 《證券及期貨條例》附表 8 第 36 條