

有關工作的主要發現及應達到的監管標準

有關工作在外聘顧問的協助下，以現場視察的方式進行，涵蓋 12 家中小型證券經紀行並著眼於這些經紀行為保障客戶資產而設的內部監控措施。下文撮述有關工作所發現的主要缺失及應達到的監管標準。以下載列的措施及監控程序並非詳盡無遺。各持牌法團應檢視本身的運作及特定情況，確保設立並實施適當而有效的監控程序。

1. 更改客戶資料

- a) 沒有定期就客戶資料庫的更改紀錄生成系統稽查紀錄，或沒有由獨立於作出更改的員工的指定職員檢視相關稽查紀錄，以偵測任何在未經授權下更改客戶資料的行為。
- b) 某些持牌法團沒有在接獲更改要求時及在作出更改後，將確認通知發送到客戶的登記地址、電子郵箱或流動電話。
- c) 沒有將客戶的新聯絡資料與客戶資料庫的資料進行對比，從中識別任何共用或採用類似模式的通訊地址、電郵地址及電話號碼的模式，這些都是出現潛在不合常規情況的跡象。
- d) 沒有就客戶以電郵發出的更改資料指示設立既定程序，透過公司正式紀錄內該客戶的其他聯絡資料，向該客戶核實其指示。

應達到的監管標準

- e) 持牌法團應審慎地處理更改客戶資料（包括通訊地址、電郵地址、電話號碼、指定銀行帳戶、授權代表）的要求，以確保其為來自帳戶持有人的真確要求。持牌法團應實施適當措施以核實提出要求者的身分及簽名，以及更改要求是否真確。例如：
 - i) 有關更改應以客戶的書面授權作為憑證¹。持牌法團應至少以合理的抽樣方式²或在發現不確定更改要求是否來自客戶時，透過其正式紀錄內客戶的其他登記聯絡資料，直接與客戶進行獨立核實。此舉至關重要，原因是即使更改指示上看似附有客戶的簽名，這些簽名仍可能由騙徒偽冒而成。
 - ii) 持牌法團在接獲更改要求時及在作出更改後，應迅速將確認通知發送到未經更改的客戶登記地址，電子郵箱或流動電話³。

¹ 《提高商號遵守〈證券及期貨（客戶證券）規則〉及〈證券及期貨（客戶款項）規則〉的能力的建議監控措施及程序》〈《建議監控措施及程序》〉第 3(b)段及於 2016 年 2 月 5 日發出的《致獲發牌從事證券交易的持牌法團的通函——保障客戶資產免受內部失當行為影響》附錄 2 第 2(b)點。

² 於 2016 年 2 月 5 日發出的《致獲發牌從事證券交易的持牌法團的通函——保障客戶資產免受內部失當行為影響》附錄 2 第 2(b)點。

³ 於 2022 年 3 月 24 日發出的《致持牌法團的通函——管理商業電郵騙案的風險》及於 2018 年 12 月 19 日發出的《致持牌法團的通函——檢視有關保障客戶資產及監督客戶主任的內部監控措施》夾附的自我評估查檢表第 9 點。

iii) 持牌法團應對更改客戶資料的要求保持警惕，以識別及跟進任何異常情況⁴。例如：

- 新電郵地址的用戶名稱或域名並不尋常，例如將原有的真實電郵地址“clientname@domain.com”改為“mahjong123@domain.com”。
- 新銀行帳戶雖以客戶的名義開立，卻設於其通常居住或工作地點以外的國家。
- 新通訊地址、電郵地址或電話號碼與其他客戶的相同或非常相似。

f) 為防範及偵測在未經授權下更改客戶資料的情況，持牌法團應就更改客戶資料庫實施適當的輸入與核對的分工監控措施⁵，以及指派合適的職員定期檢視系統稽查紀錄，以審閱客戶資料庫的更改紀錄⁶。

2. 處理電郵要求

- a) 沒有為職員提供正式指引及定期培訓以提高他們提防電郵騙案的意識，並確保他們了解適當的處理程序。
- b) 某些持牌法團沒有訂立書面政策及程序以管理電郵騙案的風險，包括核實由客戶發出的電郵指示的真實性。

應達到的監管標準

- c) 持牌法團應實施政策及程序，以應對接納有關交易指令、資產轉移或更改客戶資料的電郵要求的相關風險，因為客戶的電郵帳戶可能已被騙徒入侵並用作發出詐騙指示⁷。
- d) 除了將要求者的電郵地址與持牌法團的正式紀錄核對外，持牌法團應設有程序，以核實可疑電郵指示和涉及金額超過合理門檻的交易指令或資產轉移的電郵要求的真實性，例如透過客戶的其他登記聯絡資料向客戶確認指示，而非直接回覆相關電郵要求⁸。
- e) 持牌法團應向職員提供充分指引及定期培訓，以提高他們對識別電郵騙案的警覺性，並讓他們加深了解適當的處理程序⁹。

3. 第三者存款及付款，以及由第三者收取實物股票

- a) 除了在極少數的情況下，大部分持牌法團一般不接受第三者存款及付款。然而，某些持牌法團沒有就第三者存款及付款的處理方式訂立書面政策及程序，特別是關乎可接納此類存款及付款的特定情況，以及就接納它們而應採取的相關監控措施。

⁴ 於 2016 年 2 月 5 日發出的 [《致獲發牌從事證券交易的持牌法團的通函——保障客戶資產免受內部失當行為影響》](#) 附錄 2 第 1(h) 點。

⁵ 《建議監控措施及程序》第 7 段。

⁶ 於 2016 年 2 月 5 日發出的 [《致獲發牌從事證券交易的持牌法團的通函——保障客戶資產免受內部失當行為影響》](#) 附錄 2 第 1(m) 點。

⁷ 於 2022 年 3 月 24 日發出的 [《致持牌法團的通函——管理商業電郵騙案的風險》](#)。

⁸ 於 2012 年 9 月 7 日發出的 [《致全體中介人的通函——小心“電郵騙案”》](#) 及於 2022 年 3 月 24 日發出的 [《致持牌法團的通函——管理商業電郵騙案的風險》](#)。

⁹ 於 2022 年 3 月 24 日發出的 [《致持牌法團的通函——管理商業電郵騙案的風險》](#)。

- b) 某持牌法團沒有就客戶指派第三者代其領取實物股票的提取要求，向客戶進行獨立確認，以核實有關要求的真實性。

應達到的監管標準

- c) 持牌法團應採納盡量拒絕第三者存款及付款的政策，並僅在特殊及合法的情況下和在合理地符合客戶的概況及一般商業作業手法時才可接納有關存款及付款¹⁰。
- d) 如允許第三者存款及付款，持牌法團應實行政策及程序以確保遵守相關監管規定¹¹。特別是，這些政策及程序應由高級管理層批准，並涵蓋以下各項（其中包括）：
- 可接納第三者存款或付款的特殊及合法情況，及相關評估準則；
 - 為評定第三者存款或付款是否符合接納的評估準則而進行的盡職審查程序；及
 - 指定負責執行有關政策及程序的相關管理人員或職員¹²。
- e) 在客戶所提取的資金及證券是供轉移予第三者，或是由第三者代客戶領取實物股票之前，持牌法團應與客戶獨立確認有關提取要求的真實性，例如按客戶的登記電話號碼致電給客戶以確認提取要求¹³，並對照客戶的書面授權以核實代客行事的第三者的身分¹⁴。

4. 銀行帳戶的操作

- a) 某些持牌法團沒有實施妥善的獲授權簽署人的安排。例如，公司的股東、董事或其代名人雖不參與公司的日常營運，但卻獲准授權從公司的客戶銀行帳戶執行付款。
- b) 某些持牌法團容許其職員獨自從公司及客戶銀行帳戶執行付款，而有些持牌法團則未有為獲授權簽署人設置銀行付款的授權限額。
- c) 沒有適時將已離職的職員從獲授權簽署人的名單中剔除以移除其權限。
- d) 有些職員獲准共用同一個用戶帳戶，以操作持牌法團的網上銀行帳戶。
- e) 獲授權簽署人預先簽署空白支票。

應達到的監管標準

- f) 證監會要求：
- 可從持牌法團的客戶銀行帳戶執行任何形式付款的獲授權簽署人，只應由該持牌法團的負責人員、核心職能主管或獲其轉授職能的人擔任；及

¹⁰ 《打擊洗錢及恐怖分子資金籌集指引（適用於持牌法團及獲證監會發牌的虛擬資產服務提供者）》（《打擊洗錢指引》）第 11.3 段。

¹¹ 包括《打擊洗錢指引》第 11 章及證監會不時發出的相關通函及常見問題。

¹² 《打擊洗錢指引》第 11.3 段。

¹³ 於 2016 年 2 月 5 日發出的《致獲發牌從事證券交易的持牌法團的通函——保障客戶資產免受內部失當行為影響》附錄 2 第 2(d) 點。

¹⁴ 《建議監控措施及程序》第 2 段。

- 可從持牌法團的公司銀行帳戶執行任何形式付款的獲授權簽署人，只應由(i)該持牌法團的負責人員、核心職能主管或獲其轉授職能的人擔任，或(ii)任何其他人士擔任，前提是該人必須聯同負責人員、核心職能主管或獲其轉授職能的人共同執行付款¹⁵。
- g) 持牌法團應考慮規定其公司及客戶銀行帳戶（包括網上銀行）的付款必須由兩名或以上獲授權簽署人共同執行，並為每名獲授權簽署人設置適當的授權限額¹⁶。
- h) 持牌法團應定期檢視及更新其銀行帳戶的獲授權簽署人安排以及其網上銀行平台的使用權，當中包括及時撤銷已離職或不再擔任相關職務的獲授權人的權限¹⁷。
- i) 每名網上銀行用戶的登入資料（例如密碼）及保安編碼器應妥善保管，並不應透露予他人，以便能夠獨特地識別出每名曾登入銀行帳戶並進行交易的用戶及偵測未經授權的交易¹⁸。
- j) 持牌法團向客戶支付款項的支票必須是劃線支票¹⁹。此外，除非持牌法團的支票已填妥發票日期、指定收款人及付款金額，否則在任何情況下均不應簽署有關支票²⁰。

5. 不動帳戶

- a) 某些持牌法團沒有制定及實施書面政策及程序以定期識別不動帳戶，及定期檢視有關帳戶內的交易及其他活動以識別異常情況。
- b) 某些持牌法團沒有就對不動帳戶內的交易及資產活動所作的檢視備存任何文件。

應達到的監管標準

- c) 若帳戶在一段時間內（不超過 24 個月）並無任何由帳戶持有人發起的交易及資產活動，該帳戶應被歸納為不動帳戶。
- d) 不動帳戶容易招致未經授權交易或其他欺詐活動。持牌法團應制定政策及程序，以定期識別不動帳戶及檢視有關帳戶內的交易及其他活動（如有）以識別異常情況²¹。
- e) 持牌法團應備存妥善的紀錄及文件，以證明在處理不動帳戶時已遵守應達到的標準。

6. 更新及備存客戶資料

- a) 就確認客戶帳戶狀況方面而言，在發送至客戶的電郵或通訊地址的確認書總數當中有約 8% 被退回，意味著相關持牌法團在其正式紀錄內備存的客戶聯絡資料已經過時。

¹⁵ 於 2021 年 6 月 28 日發出的《致持牌法團的通函——銀行帳戶的操作》第 10 及 11 段。

¹⁶ 《適用於證券及期貨事務監察委員會持牌人或註冊人的管理、監督及內部監控指引》（《內部監控指引》）附錄第 19 段。

¹⁷ 《建議監控措施及程序》第 12 段。

¹⁸ 於 2021 年 6 月 28 日發出的《致持牌法團的通函——銀行帳戶的操作》第 15 段。

¹⁹ 《內部監控指引》附錄第 14 段。

²⁰ 《內部監控指引》附錄第 19 段。

²¹ 於 2016 年 2 月 5 日發出的《致獲發牌從事證券交易的持牌法團的通函——保障客戶資產免受內部失當行為影響》附錄 2 第 1(c)點。

- b) 一家持牌法團沒有在其辦事處內就其一部分客戶的開戶表格及簽署式樣紀錄備存實體或電子副本，反而將這些客戶文件備存於外部倉庫中，這令人憂慮該持牌法團及其職員是否能在日常營運中核實書面指示上的客戶簽名。

應達到的監管標準

- c) 備存最新的客戶聯絡資料有助客戶及時收取交易文件，亦有助持牌法團迅速通知客戶有關其帳戶及公司的緊急或重要事宜。持牌法團應制定監控措施來定期審查和更新儲存於客戶資料庫的客戶聯絡資料紀錄，以確保有關客戶聯絡資料是準確及反映現況²²。如未能送達成交單據及／或戶口結單，持牌法團應迅速與客戶跟進有關情況，以確保其聯絡資料屬準確及反映現況²³。
- d) 持牌法團應實施程序以記錄及保留所有相關的客戶資料、有關的簽署式樣及證明文件²⁴。持牌法團應確保這些資料可隨時供相關職員查閱以作參照之用。

7. 職責劃分

- a) 某些持牌法團在沒有實施補償監控措施的情況下，允許其交易人員或客戶主任處理客戶資產（包括處理客戶的資金及證券的存取要求）以及更改客戶資料的指示。
- b) 某些持牌法團沒有就其主要運作職能實施輸入與核對的分工監控措施。例如，持牌法團授予職員輸入和授權的權限，使其能夠獨自在中央結算及交收系統（中央結算系統）內執行交收指示及實物股票的提取指示。

應達到的監管標準

- c) 持牌法團應確保主要責任及職能適當地加以劃分，以盡量減少出現衝突、錯誤或濫權的可能性²⁵。若職責未能完全予以劃分，持牌法團在分配職責時，應確保設有所需的制衡機制，並就有關主要責任及職能制定充足的管理層檢視程序，以識別任何錯誤、濫權及欺詐行為²⁶。
- d) 除非設有補償監控措施（例如安排後勤職員（如交收部職員）直接向客戶核實由客戶主任傳送出來的有關指示），否則持牌法團應禁止其前線職員（例如交易人員及客戶主任）處理與交易無關的事宜（例如資金或證券的存取指示及客戶資料的更改）²⁷。
- e) 持牌法團應就主要運作責任及職能（例如操作中央結算系統終端機及網上銀行平台）設立輸入與核對的分工監控措施。持牌法團亦應只按實際需要向每名獲授權人授予適當的輸入限額或授權職能²⁸。

²² 於 2022 年 3 月 24 日發出的《致持牌法團的通函——管理商業電郵騙案的風險》。

²³ 《建議監控措施及程序》第 7 段。

²⁴ 《內部監控指引》附錄第 1(a)段。

²⁵ 《內部監控指引》第 II 部。

²⁶ 於 2013 年 2 月 1 日發出的《致持牌法團的通函——防範客戶資產被挪用的風險》。

²⁷ 於 2016 年 2 月 5 日發出的《致獲發牌從事證券交易的持牌法團的通函——保障客戶資產免受內部失當行為影響》附錄 2 第 3(b)點。

²⁸ 《建議監控措施及程序》第 16 段。

8. 系統接達監控措施

- a) 某些持牌法團沒有按實際需要適當地向其職員授予系統接達權限。例如，有些後勤職員獲授前線系統的接達權限，能夠輸入及授權交易指示，儘管這些職員從未接達有關系統。

應達到的監管標準

- b) 持牌法團應確保僅在有需要時向職員授予系統接達權限²⁹。
- c) 持牌法團應執行進出管制及資訊系統安全監控（例如登入設定和修改紀錄），以防範及偵測在未經授權下取覽或更改電腦數據庫和規避電腦監控的行為³⁰。

9. 就客戶資產紀錄進行對帳

- a) 某些持牌法團沒有就其分類帳與外部紀錄（例如銀行結單及中央結算系統紀錄）進行適當的對帳。例如，某些持牌法團僅每月進行一次客戶款項對帳，因此未能於一個營業日內妥善地將客戶款項存放於客戶銀行帳戶內，導致違反了《客戶款項規則》³¹。某些持牌法團沒有定期就存放於執行買賣盤的經紀的客戶證券進行對帳。

- b) 某些持牌法團沒有及時和妥善地跟進在對帳過程中發現到的差異。

應達到的監管標準

- c) 持牌法團應定期將公司的內部紀錄及報告與由第三者，例如結算所、銀行、託管商、執行買賣盤的經紀等發出的紀錄加以核對³²，特別是：
- 持牌法團應每天核對其內部股份紀錄與中央結算系統股份存量紀錄的資料。至於在其他地方存管的股票，持牌法團應最少每月核對其股份紀錄與第三者託管人的紀錄³³。
 - 持牌法團應每天更新分類帳、核對客戶及銀行分類帳帳戶的結餘，以及按照《客戶款項規則》的規定，將款項轉撥至客戶銀行帳戶或將客戶銀行帳戶的款項轉撥至其他帳戶。此外，持牌法團應最少每月核對銀行結單與分類帳的資料³⁴。
- d) 所有客戶資產紀錄的對帳工作應由適當的高級職員查對、覆核和批准，以確保對帳工作妥善執行³⁵，且所有差異和未決事項妥善及迅速地得到跟進³⁶。

²⁹ 《內部監控指引》附錄第 20 段及《建議監控措施及程序》第 11 段。

³⁰ 於 2013 年 2 月 1 日發出的《致持牌法團的通告——防範客戶資產被挪用的風險》。

³¹ 《證券及期貨（客戶款項）規則》（《客戶款項規則》）第 4(4) 及 10 條。

³² 《內部監控指引》第 VII 部第 10 段。

³³ 《建議監控措施及程序》第 17 段。

³⁴ 《建議監控措施及程序》第 23 及 24 段。

³⁵ 《內部監控指引》第 VII 部第 10 段。

³⁶ 於 2016 年 2 月 5 日發出的《致獲發牌從事證券交易的持牌法團的通告——保障客戶資產免受內部失當行為影響》附錄 2 第 1(a) 點。