HONG KONG MONETARY AUTHORITY
香港金融管理局

指定零售支付系統的監察

附加指導

2022 年 **9** 月

結構

引言

1.1. 香港金融管理局(金管局)發出的《指定零售支付系統的監察指引》(《指引》)列載金管局在監察指定零售支付系統時所採用的高層次原則。為使指定零售支付系統的系統營運者及交收機構更了解應用《指引》所載原則的標準，金管局發出《指定零售支付系統的監察附加指導》(《附加指導》)，以按需要就《指引》的特定章節提供附加指導。

1.2. 指定零售支付系統的系統營運者及交收機構應視《附加指導》為在典型的情況下可如何符合某項原則性規定的具體說明；它們應透徹理解有關說明，並在考慮其具體情況後，適當調整其管控制度，以遵守《指引》的規定。《附加指導》應與《指引》的有關章節一併閱讀。

1.3. 為免引起疑問，《附加指導》適用於信用卡交易及存在類似安排(例如涉及第三方服務代理)的扣帳卡交易。此外，有關指定零售支付系統的監管規定，載於《支付系統及儲值支付工具條例》及《指引》。雖然《附加指導》旨在協助指定零售支付系統的系統營運者及交收機構更充分了解如何遵從有關規定，但《附加指導》不會凌駕或取代該等文件內的任何條文。

1.4. 《附加指導》只列載有發出附加指導的《指引》的特定章節。金管局日後可能會在有需要時修改《附加指導》，或就《指引》的另一些章節增發附加指導，並以修訂《附加指導》的形式發佈。

摘自《指定零售支付系統的監察指引》(《指引》) (於 2020 年 9 月發出)的相關規定

2. 安全規定

指引第 2.2 段 — 法律基礎

指引第 2.2.1 段	*指定零售支付系統應有充分、清晰及可強制執行的法律基礎，就其活動提供高度明確性；亦應有清晰的規則、程序及合約規管系統的成立及運作、界定系統及其參與者與其他相關人士的權利和義務，包括(如相關)指明對系統參與者的客戶的規定，並通過該等參與者及其客戶之間的合約安排強制執行。該等規則、程序及合約應與相關法律及規例一致。在多個地區經營業務的指定零售支付系統，應識別及減低因不同地區的法律任何潛在矛盾引起的、可能令指定零售支付系統未能符合《支付條例》下的規定(包括專員根據《支付條例》發出的任何適用規則或規例)的風險。*

指引第 **2.3** 段 — 管治、風險管理及管控程序

指引第 2.3.2 段	*指定零售支付系統的系統營運者及交收機構應有良好穩健並符合系統的業務性質、規模及複雜程度的風險管理架構，以識別、量度、監察及管理由系統產生或承擔的風險。一般適用於指定零售支付系統的主要風險類別包括但不限於業務運作風險、科技及網絡安全風險、資訊風險、金融風險(例如業務風險、信用風險、交收風險、流動性風險)、信譽風險、法律及合規風險，以及洗錢及恐怖分子資金籌集風險。負責監察及管理指定零售支付系統的系統營運者及交收機構的董事局及管理層應決定系統的適當承受風險水平及能力，並訂立與系統的承受風險水平及能力相稱的政策、程序及管控措施，尤其應有具備足夠獨立性及權限的有效風險管理、合規及審計部門。指定零售支付系統亦應訂有政策，以確保參與者及其客戶(如相關)管理及控制其可能對系統構成的風險。新的支付產品及服務、計劃規則及運作程序，以及對現有支付產品及服務、計劃規則及運作程序的重大修訂，應接受全面風險評估，並應在推出前妥善應對所識別的所有風險。此外，現有產品、服務及運作程序的風險狀況應受到定期檢視，並在相關情況出現轉變時得到適當更新。*
指引第 2.3.3 段	*指定零售支付系統的系統營運者及交收機構應有適當的管控機制，以確保系統妥善運作，並具備有效措施以防範、偵測及處理系統干擾及異常、錯誤與詐騙的情況，以及確保符合相關法定及監管規定。獨立及針對風險的審計應定期進行，以確保系統的安全及效率。*

4. 運作規則的規定

指引第 **4.3** 段 — 監察及強制執行符合運作規則的安排

指引第 4.3.1 段	*指定零售支付系統的系統營運者及交收機構應設立有效的管控機制，確保系統依照既定的運作規則運作，並監察參與者持續符合相關規則。*

附加指導

附加指導 (a)	指定零售支付系統的系統營運者及交收機構應制定穩健架構，規定參與者糾正出現於其第三方服務代理的資料外洩。
附加指導 (b)	指定零售支付系統的系統營運者及交收機構應規定參與者(例如發卡機構及收單行)： (i) 在引入第三方服務代理(例如支付代理及支付網關)前進行盡職審查，並查核其是否遵守適用的盡職審查標準；及 (ii) 與第三方服務代理訂立合約或服務協議，清楚列明所涉各方的權利及義務。
附加指導 (c)	參與者與第三方服務代理之間的合約或服務協議應可強制執行，讓參與者或(視適當情況)相關指定零售支付系統的系統營運者及交收機構對參與者的第三方服務代理採取所需行動，糾正出現於該第三方服務代理的資料外洩。
附加指導 (d)	有關合約或服務協議亦應規定參與者引入的第三方服務代理遵守指定零售支付系統的系統營運者及交收機構頒布的標準或規定(例如一般公認的業內數據安全標準)。有關標準或規定應包括資料保安標準等，以有效地防範、偵測、緩減及適時匯報資料外洩及網絡攻擊；尤其若系統營運者及交收機構合理地認為某些事故可能會對香港持卡人或該指定零售支付系統在香港的支付卡業務的整體安全及效率造成重大及不利影響，更應適時匯報。

2. 安全規定

指引第 2.5 段 — 運作可靠性及穩健程度

指引第 2.5.1 段	*指定零售支付系統的系統營運者及交收機構應實施有效措施，確保與系統有關聯的基礎設施提供足夠及持續的服務，以盡量減低對零售支付交易、結算及交收程序的干擾，並促進零售支付交易的完整性、保密性及可用性。*
指引第 2.5.6 段	*指定零售支付系統的系統營運者及交收機構應有全面的事故管理架構，並以書面形式訂明有關程序，以及有充足的管理層監察，妥善記錄、匯報及分析關於系統的所有運作事故(當中包括由系統參與者及參與者的客戶所引起或涉及的運作事故)，並妥善作出回應及恢復系統。有關架構應包括：* *(a) 按嚴重程度將事故及運作問題分類以及決定上報和處理程序的系統；* *(b) 盡快向金管局匯報可能會影響指定零售支付系統的安全及效率的重大事故；* *(c) 在發生事故時與參與者及其他持份者溝通的有效策略，以應對其可能產生的顧慮及恢復其對系統的信心；以及* *(d) 事故後檢討，以識別造成事故的根本原因和運作及/或業務持續運作安排所需的任何必要提升措施。有關檢討應(如相關)包括指定零售支付系統的參與者。*
指引第 2.5.7 段	*指定零售支付系統應有充足的措施，防範、偵測及減低經系統進行的欺詐交易引致的風險及造成的影響。有關措施包括監察經系統進行的付款活動，並就詐騙及該等活動引致的任何風險採取迅速行動。此外，應有妥善安排，以便利參與者分享資訊及進行有關詐騙認知的客戶教育活動，從而減低詐騙風險。*

指引第 **2.6** 段 — 保安

指引第 2.6.1 段	*指定零售支付系統的系統營運者及交收機構應有良好及穩健的保安架構，應對指定零售支付系統的所有潛在風險及威脅。保安架構應建基於對系統的保安風險的定期分析，並符合相關業界標準。對保安架構的遵守應受到持續監察。*
指引第 2.6.2 段	*指定零售支付系統的保安架構其中應包括：* *(a) 穩健的接觸管制，包括實體及邏輯管制，以防範未經授權人士及應用程式接觸或運作系統；* *(b) 充足的資料保安措施，涵蓋資料擁有權、分類、輸入、傳送、處理、接觸、儲存及保留，以確保指定零售支付系統所收集及使用的資料的保密性、完整性、真確性及隱密度；* *(c) 與指定零售支付系統處理不同類別的交易所涉及的風險相稱及充足的支付保安措施，包括支付交易的核實及傳送，以防範未經授權的活動；* *(d) 全面網絡防衛架構，以有效防範網絡攻擊及從中復原，並應隨時迅速調整以保護及應對系統免受日後可能出現的網絡攻擊。網絡防衛架構至少應持續監察網絡攻擊的趨勢、實施充足的保護措施，以應對不同的攻擊場景，包括會影響關鍵資訊科技所在地點及組成指定零售支付系統的系統運作的攻擊，並執行定期滲透測試及保安檢視。*

附加指導

(I) *防範*

附加指導 (a)	指定零售支付系統的系統營運者及交收機構應設立適當標準或規定，例如獲系統營運者及交收機構視為適用於該指定零售支付系統的運作的一般公認的業內數據安全標準，作為旨在保障支付資料及支付卡資料的技術及運作規定的基準。有關標準或規定應適用於該指定零售支付系統，並透過適用安排(例如有關系統的規則與程序、參與者與其第三方服務代理之間的合約安排)向下引伸至負責儲存、處理或傳送卡資料及/或敏感驗證資料，或可影響卡資料環境安全的所有實體(例如其參與者及視乎情況其參與者的客戶及第三方服務代理)。有關標準或規定應至少涵蓋敏感資料分類、就支付資料實施強效的加密、穩健的密碼匙管理、妥善的邏輯及實體管制、資料存廢、有效的打擊惡意軟件及打擊網釣機制。
附加指導 (b)	指定零售支付系統的系統營運者及交收機構應設立適當安排，例如有關系統的規則及程序，以使只有能夠充份及定期證明本身已遵守相關安全標準或規定的實體(例如其參與者及視適當情況其參與者的客戶及第三方服務代理)才獲准儲存、處理或傳送與該指定零售支付系統相關的卡資料及/或敏感驗證資料。為此，指定零售支付系統的系統營運者及交收機構應設立相關安排，按需要在其參與者的協助下定期識別應遵守有關標準或規定的實體。
附加指導 (c)	指定零售支付系統的系統營運者及交收機構應在考慮相關因素(例如科技發展)的情況下採取適當行動，制定或頒布有助防範未經授權交易的適當規程或安排，以致即使卡資料外洩，騙徒亦無法輕易使用外洩的卡資料進行欺詐交易。就網上交易而言，有關規程或安排的例子包括卡資料代碼化及利用 3-D Secure 驗證卡交易。

(II) *偵測*

附加指導 (a)	指定零售支付系統的系統營運者及交收機構應設立規定(例如規則及程序)，規定參與者須： (i) 定期監察第三方服務代理遵守該指定零售支付系統的系統營運者及交收機構頒布的數據安全標準；及 (ii) 向該指定零售支付系統的系統營運者及交收機構適時匯報出現於其第三方服務代理的懷疑及/或實際資料外洩及網絡攻擊；尤其若系統營運者及交收機構合理地認為某些事故可能會對香港持卡人或該指定零售支付系統在香港的支付卡業務的整體安全及效率造成重大及不利影響，更應適時匯報。
附加指導 (b)	應制定適當及風險為本的方法，查核相關實體是否遵守由該指定零售支付系統的系統營運者及交收機構所頒布的安全標準或規定，並透過適用安排(例如有關系統的規則及程序及參與者與其第三方服務代理之間的合約安排)向下引伸至相關實體。上述查核的例子包括定期進行查核(並以書面形式記錄)，以及就與有關標準或規定相關的環境出現重大變動後進行的查核。該指定零售支付系統的系統營運者及交收機構亦應設立適當及風險為本的措施，透過向下引伸安排，規定相關實體證明其已遵守相關安全標準或規定，並即時處理任何不合規的情況。
附加指導 (c)	指定零售支付系統的系統營運者及交收機構應設立防騙監控系統，以偵測不尋常的卡交易模式，並分析其參與者匯報的欺詐資訊，後者可能有助及早識別懷疑及/或實際資料外洩。

(III) *緩減*

附加指導 (a)	一旦指定零售支付系統的系統營運者及交收機構獲悉懷疑及/或實際資料外洩及網絡攻擊事故，應採取適當行動，包括迅速應對及按需要規定其參與者及/或透過向下引伸安排，規定其參與者的第三方服務代理展開法證調查及為該等調查提供所需支援，以達致下述各項： (i) 識別事故成因； (ii) 處理資料安全事項；及 (iii) 實施緩減措施，以免發生同類事故。
附加指導 (b)	指定零售支付系統的系統營運者及交收機構應對其不遵守資料安全標準的參與者採取適當及風險為本的執法行動，並應透過向下引伸安排，規定其參與者對其不遵守資料安全標準的第三方服務代理採取適當行動。有關行動的例子可由加強檢視或查核、加強資料保安措施或規定、警告、罰款，以至禁止接觸指定零售支付系統的網絡不等。
附加指導 (c)	指定零售支付系統的系統營運者及交收機構應設立機制，以及時、有效及以適當方式與其參與者分享有關資料外洩及欺詐的資訊及/或情報，以助提高參與者的防騙意識及促進參與者採取適當行動，例如加強詐騙監察、及時通知客戶，以及考慮更換支付卡。

(IV) *匯報事故*

附加指導 (a)	指定零售支付系統的系統營運者及交收機構應設立安排，確保除本身系統的事故外，亦就交易流程中與其網絡相關而涉及其他實體(例如收單行及支付網關)的資料外洩事故，向金管局適時發出通知及維持高效的訊息流通；尤其若系統營運者及交收機構合理地認為某些事故可能會對香港持卡人或該指定零售支付系統在香港的支付卡業務的整體安全及效率造成重大及不利影響，更應適時匯報。

附加指導(b)	在評估某事故是否重大及/或是否需要向金管局匯報時，指定零售支付系統的系統營運者及交收機構應考慮相關因素，包括但不限於以下各項： (i) 對該指定零售支付系統在香港的運作、可靠性、安全及效率、健全程度、資料完整性、風險管理及管制、穩健程度及/或穩定有重大不利影響的事故(例如影響系統運作的網絡攻擊、資料外洩)； (ii) 與該指定零售支付系統處理的交易相關，且已經或可能對大量香港人士(例如其營運者、參與者及(若屬相關)參與者的客戶)造成重大財務影響或財務損失的事故，而不論是否已設有安排(例如退款)，以處理該等事故所造成的任何財務影響或損失； (iii) 屬重大規模，且對香港持卡人有重大或不利影響的懷疑或實際詐騙或資料外洩；及 (iv) 可能對該指定零售支付系統造成重大及不利信譽風險，或影響香港公眾對該指定零售支付系統信心的事故。
附加指導(c)	一旦指定零售支付系統的系統營運者及交收機構獲悉對香港持卡人或其在香港的支付卡業務的整體安全及效率有重大不利影響的事故(例如影響系統運作的網絡攻擊或資料外洩)，該系統營運者及交收機構應即時通知金管局，並向金管局提供當時與該事故有關的任何可用資訊(例如事故成因、預期或實際影響、已經或將要採取的補救措施，以及對潛在查詢的回應)。
附加指導(d)	指定零售支付系統的系統營運者及交收機構應評估事故是否涉及潛在或實際違規行為，並是否有責任根據指定零售支付系統相關的法律或法規以外的任何適用法律或法規(例如《個人資料(私隱)條例》)，向其他監管機構匯報有關潛在或實際違規行為。若是，指定零售支付系統的系統營運者及交收機構除向金管局作報告外，亦應向其他相關監管機構報告該事故。
附加指導(e)	為免引起疑問，零售支付系統的系統營運者及交收機構不應等待直至所有相關資料收集完畢及/或問題得到糾正後，才向金管局匯報該系統營運者及交收機構合理地認為可能會對香港持卡人或其在香港的支付卡業務的整體安全及效率造成重大不利影響的任何事故。若需要進一步調查以確定事故相關的基本事實，亦應向金管局發出預警，而不是在調查之後才作出此舉。
附加指導(f)	金管局可要求指定零售支付系統的系統營運者及交收機構提供進一步資料或更新(舉例說，如適用時，初步及最終調查結果)。