消費者資訊保護標準建立指導綱領[1]

1999 年 11 月 12 日由美國總統柯林頓完成簽署通過之美國金融服務業現代化法[2]（簡稱 GLB Act），對銀行、證券業與保險公司跨業經營、功能性監理、保險等多項金融業務訂定規範；鑒於金融機構多角化經營，機構間藩籬日趨模糊，消費者資訊保護成為相關重要議題之一，因此 GLB Act 對機構間資訊交換與消費者隱私亦有相關規定。美國通貨監理署（簡稱 OCC）依據 GLB Act 規定，訂定消費者資訊保護標準建立指導綱領，並於 2000 年 12 月 21 日正式通過，要求各金融機構依據此指導綱領確實履行保護消費者非公開資訊；本文擬摘要介紹指導綱領內容與相關規定，俾供國內相關單位參考借鏡。

依據 GLB Act 第 501 條〝保護非公開個人資訊〞規定，要求聯邦政府銀行主管機關、全國信用聯盟委員會、證券交易委員會以及聯邦貿易委員會等機構，對消費者紀錄和資訊之管理、技術與實質保護等方面，就各單位管轄範圍建立適當標準，以期達到下列三項目標：（1）確保消費者紀錄和資訊安全性與機密性；（2）防止任何對該紀錄資訊安全性或完整性有潛在威脅與危險情形之發生；（3）防止未經授權管道或使用消費者紀錄或資訊，避免造成任何消費者實質傷害或不便情形；OCC 依據上述法令規定，公布消費者資訊保護標準建立指導綱領，要求各聯邦立案銀行建立資訊安全體系，保護所有顧客與銀行紀錄；訂定此指導綱領之目的，係提供各金融機構一指導原則，就管理、技術與實質等三方面建立兼具安全性、機密性與完整性之消費者資訊保護機制，據以執行；其內容訂定亦參照聯邦存款保險法（Federal Deposit Insurance Act，簡稱 FDI Act）第 39 條第 a 款、GLB Act 第 501 條及第 505 條第 b 款等相關規定，說明各機構權限。

按照美國聯邦交易委員會於 2000 年 5 月 12 日，發布金融服務業現代化法〈GLB Act〉有關消費者金融資訊隱私權保護施行細則[3]定義，所謂〝顧客〞，係指與機構間已建立起持續關係的消費者，前述機構主要提供單項或多項個人或家用目的為主的金融商品或服務；而企業以及未與金融機構間建立起持續關係之消費者（如鮮少使用金融機構自動櫃員機（ATM）或申辦貸款的個人戶），不在此限。原指導綱領草案將任何有關顧客非公開個人資訊紀錄視為顧客資訊，包含紀錄、資料、檔案、或其他電子及書面資訊、或其他任何代表機構提供服務者所維護之任何形式資訊。部分人士認為該項〝顧客資訊〞定義過於廣泛，係因該定義將所有〝包含〞非公開個人資訊文件納入考量；然而主管機關認為，為充分保護顧客資訊，金融機構資訊保護機制亦應將包含非公開個人資訊文件涵蓋在內。有鑑於此，金融機構可能考慮減少文件中所包含非公開個人資訊以規避資料保護相關規定，惟這些文件仍無法完全脫離指導綱領所訂定之規範。

經參酌多方意見，主管機關決議採用〝顧客紀錄〞以取代〝顧客資訊〞，其實質定義同指導綱領草案，然現行指導綱領已刪除包含〝紀錄〞或〝藉由書面、電子或其他形式〞中之〝資料、文件、或其他資訊〞等文字；因此，不論銀行或代表銀行者以書面、電子或其他形式維護包含非公開個人資訊在內之顧客相關紀

---

[1] 資料來源：OCC Bulletin, OCC 2001-8, February 15, 2001。

[2] 請參閱中央銀行外匯局編譯，「美國金融服務業現代化法」，財團法人金融聯合徵信中心出版，民國八十九年十
二月。

[3] 請參閱 Federal Register, Vol.65, No.101,pp.33677-33688, May 24, 2000。

錄者，皆屬〝顧客資訊〞。

顧客資訊系統係指以任何方式存取、蒐集、儲存、使用、傳送、保護或處理顧客資訊者，不論該項資訊是否存在於金融機構業務範圍內或該項資訊如何被使用，擴大其定義範圍將有助於保護所有顧客資訊。由於指導綱領在其他重大方面給予金融機構較高的彈性，同意各機構依其環境條件訂定合宜安全機制，因此即使該項定義範圍較為廣泛，應不致造成金融機構在處理顧客資料安全上過度負擔；主管機關認為，GLB Act 要求各金融機構採取廣泛地資訊安全計畫，將可有效防止未經授權存取或使用顧客非公開個人資訊情況。任何透過直接向銀行提供服務以維護、處理或以其他經允許之方式存取顧客資訊的個人或實體，即稱為服務提供者；服務提供者對金融機構個人或實體揭露資訊，將使被揭露資訊的安全與機密產生額外風險，為防止此類風險產生，金融機構應於提供資訊給服務提供者時，採取適當步驟以保護該項資訊。舉例而言，透過提供專業服務並兼顧金融機構適當保護資訊措施情況下，上述服務提供者將可獲得存取顧客資訊機會。據此，主管機關決定所謂的服務提供者，應廣泛地包含對金融機構提供服務之不同個人或公司，然而這並不表示金融機構對各服務提供者需採用同樣方式監管彼此間協定，仍應視其環境條件而訂定不同標準。

除此之外，各銀行應就其規模與複雜性以及業務本質與範疇，訂定包含管理面、技術面及實質面之適當且廣泛的資訊安全書面計畫。各銀行董事會或指導委員會應批准該項資訊安全計畫，並監督該項計畫之發展、執行及維持情況，其中亦應包含賦予管理階層與此計畫執行相關情形與檢視報告之權責。此外，各銀行應以理性態度辨識可能導致未經授權揭露、濫用、變更或破壞顧客資訊或顧客資訊系統之內部與外部潛在威脅，並考量顧客資訊敏感性而加以評估其內部與外部威脅之可能性與潛在傷害。透過評估資訊安全計畫指導方針、執行程序以及顧客資訊系統是否合宜，將可適時控制風險的產生。

由於資訊安全為現今金融業務重要議題之一，各銀行應就管理與控制風險層面，考量業務範圍、複雜性及資訊敏感性，設計適合的資訊安全計畫。指導綱領提出八種管理與控制方法供金融機構參考：(1) 顧客資訊系統的使用權控制，應避免員工提供顧客資訊給未經授權且欲以詐欺方式獲取資訊者，該資訊系統僅限於經授權者使用；(2) 顧客資訊存放所在地之使用限制，如建築物、電腦設備與紀錄儲存設備等，應僅限於經授權者使用；(3) 顧客電子資訊之加密措施，避免未經權者使用於網路或系統間傳送或儲存之資訊；(4) 訂定適當作業程序以確保顧客資訊系統修正後，仍與銀行資訊安全計畫目標一致；(5) 雙重控制程序；(6) 建立監視系統與程序，可預先察覺實際或企圖侵害或侵入顧客資訊系統行為；(7) 建立回覆系統，若銀行猜測或察覺有未經授權者使用顧客資訊系統等特殊行為發生，應適時向管理或執法機構報告；(8) 採取適當方式，以防止因潛在環境威脅而導致顧客資訊系統的破壞、損失或損害，如火災、水災或缺乏技術等因素。另外，管理階層應教育職員執行銀行訂定之資訊安全計畫，並定期測試資訊安全計畫系統、程序與關鍵控制情況，其測試頻率與內容由銀行風險評估部門決定，測試結果應交由獨立第三者或非發展或維持該安全計畫之職員處理或檢視。

各銀行應以積極態度選擇服務提供者，並於符合指導綱領所訂目標前提下，以契約方式要求該服務提供者以適當方式提供服務；再者，各銀行可依據契約監督服務提供者完成前述義務，並可檢視帳目、測試、或以其他同等方式評估該服務提供者。任何有關技術、顧客資訊敏感性、對資訊而言的內部與外部威脅等因素改變，或銀行業務協定變更，如合併、結盟或委外作業等，各銀行應適時監督、

評估與調整資訊安全計畫，以因應其環境條件之改變。

消費者資訊保護標準建立指導綱領將於 2001 年 7 月 1 日正式生效，過渡生效期間已延至 2003 年 7 月 1 日。主管機關為使各金融機構有充分時間與其服務提供者重新訂定契約協定，已要求各金融機構於 2003 年 7 月 1 日前完成契約協定換約工作，舊有契約協定僅可使用至 2001 年 3 月 5 日止。