正本

檔　　號：
保存年限：

025199
(0900)

總務二科
108.9.18
收文章

金融監督管理委員會　函

地址：22041新北市板橋區縣民大道2段7號17樓
承辦人：賴虹文
電話：02-8968-0899分機0765
傳真：

10018
台北市仁愛路4段296號

受文者：國泰人壽保險股份有限公司(代表人黃調貴先生)

發文日期：中華民國108年9月16日
發文字號：金管保壽字第10804950581號
速別：普通件
密等及解密條件或保密期限：密(發文後解密)
附件：如主旨

主旨：關於本會對貴公司電子商務系統專案檢查報告（編號：107F133號）所列缺失事項，查貴公司辦理保險業務，核有礙健全經營之虞，依保險法第149條第1項規定予以4項糾正，檢附處分書一份，請查照。

說明：依據貴公司108年3月27日國壽字第108031109號函辦理。

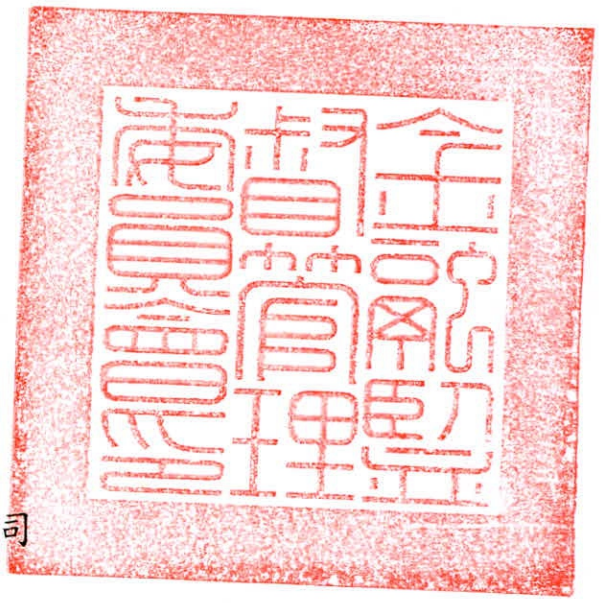
正本：國泰人壽保險股份有限公司(代表人黃調貴先生)
副本：金融監督管理委員會檢查局、保險局(均含附件)

主任委員 顧立雄
授權單位主管決行

正本

檔　　號：
保存年限：

金融監督管理委員會　處分書



10018
台北市仁愛路4段296號
受文者：國泰人壽保險股份有限公司(代表人黃調貴先生)

發文日期：中華民國108年9月16日
發文字號：金管保壽字第10804950582號
速別：普通件
密等及解密條件或保密期限：
附件：

相對人：國泰人壽保險股份有限公司
公司代表人：黃調貴先生
出生年月日：
性別：男
身分證統一號碼：
地址：臺北市大安區仁愛路4段296號

主旨：關於本會對貴公司電子商務系統專案檢查報告（編號：107F133號）所列缺失事項，查貴公司辦理保險業務，核有礙健全經營之虞，依保險法第149條第1項規定予以4項糾正。

事實及理由：

一、檢查意見二（一）第3點、辦理網路相關規劃管理作業，FTP伺服器未依規定置放於DMZ區，如：提供○○○等外部單位以SFTP或FTP連線使用之FTP伺服器係置放於內部伺服器區，核與自訂「網路設備管理施行細則」第17條「所有對外服務的伺服器主機(如：Web Server、FTP Server)一律放置於DMZ，外部連線只能透過置於DMZ之伺服器主機對內部存取，不允許直接由Internet存取Intranet中的任一主機」規定不符，核有礙健全經營之虞。

二、檢查意見二（三）辦理弱點掃描及安全漏洞修補作業，有

下列欠妥事項，核有礙健全經營之虞：

(一)雖每季辦理弱點掃描並出具掃描結果報告，惟卷查106年至107年第1季弱點掃描報告，均存在上千個中風險以上弱點，修補速度顯待提升；另對未能即時修補之風險弱點，掃描結果報告未併同說明相關補償性控管措施及預計改善日期，不利資訊安全控管，均核與所訂「弱點掃描及滲透測試管理辦法」第7條：「安全弱點與漏洞改善：管理單位除應將執行弱點掃描及滲透測試之評估報告予以建檔，交由各系統管理人員進行改善作業外，並應追蹤至改善為止，無法即時修補之弱點，系統管理人員需回報管理權責單位無法修補之原因、相關補償措施與預計改善日期。」規定不符。

(二)重要網路設備廠商發佈之漏洞，有未及時進行修補者，如：電子商務系統使用之負載平衡器F5具有中間人攻擊漏洞(○○○)，所執行弱點掃描報告亦有發現該等弱點，該漏洞已於106.11.18發布修補程式(○○○)，惟迄檢查日尚未修補完成；另網路交換器Cisco Switch 3750之韌體存有允許遠端攻擊者執行任意程式碼或阻斷服務攻擊，被歸類為嚴重等級之漏洞，該漏洞已於107.4.3發布修補程序，惟迄檢查結束日止尚未執行107年第2季弱點掃描，以致尚未修補。

(三)檢查期間測試官網www.cathaylife.com.tw及員工入口網w3.cathaylife.com.tw之安全性，顯示該等網站主機存有加密強度不足之弱點，如：未停用已被公告為不安全之傳輸協定TLS1.0，且攻擊者可執行機器人攻擊(ROBOT)以竊取傳輸中資料，不利系統安全。

三、檢查意見三（三）辦理個資保護管控對外傳輸之資料，經查有下列欠妥事項，均不利防範個資外洩，核有礙健全經營之虞：

(一)雖已利用NDLP閘道型資料外洩防護系統過濾外寄檔案，惟未將電子郵件地址納入偵測條件，另對不同個資組合已分別訂定一定門檻筆數以下個資郵件，僅記錄而不阻擋及審核，尚未建立對藉多次外寄低於門檻筆數個資之郵件，以規避現有防範個資外洩措施之監控機制。

(二)所建置NDLP僅設定利用網頁或電子郵件(http、https、network email)傳輸者，須經由NDLP檢核並留存紀錄，對防火牆已開放利用其他通訊埠對外傳輸內含個資檔案，尚未建立過濾或管控其適當性之機制。

四、檢查意見四（三）第2點，業務人員使用之行動投保APP，設計提供客戶於平板電腦上以電子簽名方式，作為投保確認依據，惟查於客戶簽名完成後，系統允許業務人員更改業經客戶確認之資料，包含地址、電話或電子郵件等，與保單寄送或辦理保單變更確認使用之重要資訊，管控設計有欠妥善，核有礙健全經營之虞。

法令依據：保險法第149條第1項規定。

附註：受處分人如不服本處分，應於本處分送達之次日起30日內，依訴願法第58條第1項規定，繕具訴願書經由本會(新北市板橋區縣民大道2段7號18樓)向行政院提起訴願。惟依訴願法第93條第1項規定，除法律另有規定外，訴願之提起並不停止本處分之執行。

正本：國泰人壽保險股份有限公司(代表人黃調貴先生)

副本：金融監督管理委員會檢查局、保險局

主任委員　顧　立　雄

授權單位主管決行