正本

檔　　號：
保存年限：

金融監督管理委員會　裁處書

受文者：國泰世紀產物保險股份
有限公司

發文日期：中華民國110年5月18日
發文字號：金管保產字第11004918582號

受處分人：國泰世紀產物保險股份有限公司
營利事業統一編號：84445772
地址：台北市仁愛路四段296號
代表人或管理人姓名：
地址：台北市仁愛路四段296號

主旨：查貴公司辦理保險業務，核有違反保險法相關規定(詳一般業務檢查報告，編號109F128)，依保險法第171條之1第4項及第5項規定核處罰鍰新臺幣(下同)240萬元，並依同法第149條第1項規定予以5項糾正。

事實：

一、貴公司所訂「健康暨傷害保險-被保險人體況審核參考標準」，對被保險人達申領身心障礙證明之身體狀況，訂有保險金額限制或婉拒承保情形，有未比照一般之核保規則辦理，不利「保險業承保身心障礙者處理原則」第1點「各保險公司對身心障礙者之核保，應遵循下列原則：(1)對肢體障礙者宜比照一般之核保規則辦理，即對被保險人之身體狀況、所從事職業內容之危險程度、個人或家庭之財務狀況等因素予以評估。」規定之遵循，致影響身心障礙者投保權益(如檢查意見三(一))，如：

(一)「傷害險審核」對被保險人身體狀況「已達6-11級失

能」即予限制相同最高投保金額者，審核標準「限額」乙欄列示「※若保套裝商品，限1011意外死亡及失能為100萬（含）以內之方案」，惟前揭達申領身心障礙證明之身體狀況種類及輕重程度均有不同，公司即予限制相同最高保險金額，未比照一般之核保規則辦理。

（二）「各項疾病審核」被保險人身體狀況有病名「肢體障礙」者，核保參考「婉拒條件為：(1)四肢切斷或機能喪失者直接不同意承保。(2)肢體障礙已達坐輪椅狀況者；(3)脊椎外觀顯著運動障礙或畸型者。」，易使招攬人員誤解被保險人體況若達上述婉拒條件時，可以口頭婉拒保戶投保。

二、貴公司銷售「汽車延長保固費用保險」(原「汽車延長保固契約責任保險」)商品，承保被保險人(汽車經銷商)依汽車延長保固契約對被保固汽車車主負保固零件修復或更換責任時，於保險契約約定範圍及金額內就被保險人所支付修復費用負給付之責，承保對象為銷售國外進口二手高價車之經銷商，查辦理核保作業有未徵提汽車延長保固契約及未留存核算保費之佐證資料者，未依保險商品內容予以評估並簽署承保(如檢查意見三(二))，如：

（一）未徵提被保險人(同要保人)與被保固車主約定之汽車延長保固契約，確認被保險人須負擔之保固項目，僅以被保險人於要保書所載被保固汽車車主名稱、被保固汽車牌照號碼、原始發照日期、製造年份、廠牌型式、排氣量、引擎/車身號碼、保固期間或保固里程數，即認定被保險人對該汽車負有延長保固責任即予以承保，如：保單號碼1501TYEW****(起保日107.8.22)及1516UYEW****(108.1.11)。

（二）未留存核算保費之佐證資料者，如：公司商品送審資料，新車及中古車於加減費前總保費分別為7,929元及

6,938元，核保人員依個別危險差異進行核保調整訂價，按「被保汽車的車齡、行車里程數和使用狀況」、「保固零件的價格和取得難易度」及「保固期間、保固里程數及保額」等3指標加減費，個別指標加減費區間為-20%~20%，3指標合計加減費上下限為-60%~60%，本次查核資料期間公司承保保單計2,897件，保費為8千元及9千元之保單分別為480件及2,417件，經抽查31張保單皆未有加減費之佐證資料。

三、貴公司推出新服務有未由總機構法令遵循主管出具符合法令規章及內部規範之意見並簽署負責，致未落實法令遵循作業(如檢查意見三(四))，如：公司108.8.1首度與信義房屋(股)公司(下稱信義房屋)簽訂「商業火災保險服務合作協議書」，合作模式為信義房屋於租賃契約成交後，依據客戶所簽署之「租業大吉」專案同意書，將客戶個人資料及房屋資訊提供予公司辦理商業火災保險相關作業使用及由信義房屋代客戶繳交保險費，迄檢查基準日(109.5.31)止承保出單案件計有保單號碼157508BO10****（生效日108.9.20）等347件，合作案之簽呈於108.8.12會辦法令遵循部未表示意見，未由總機構法令遵循主管出具意見書。

四、貴公司於102年起與所屬金控集團暨子公司共用簽訂「資訊系統設備暨人員共用計畫框架合約書」，未訂定相關管理規範或控管機制，查有下列事項欠妥(如檢查意見四(三))：

(一)依合約內容，委由集團關係企業國泰人壽協助維護公司產險Infra系統及產險核心系統，惟未明定開放予國泰人壽存取之內部系統範圍，包括伺服器主機、資料庫及設備名稱等，及所授與之存取權限，不利權責劃分。另對前述委由集團關係企業辦理資訊維護作業，公司尚未訂定相關管理規範或控管機制，如：連線對象、連線範

圍、連線期間、得使用之高風險性網路通訊服務、防火牆開通相關申請及核准程序、定期檢視伺服器主機及資料庫存取權限及監控執行內容等，不利作業遵循。

(二)經查除前述允許國泰人壽依合約連線至公司內部正式應用系統及資料庫外，公司尚有開放集團其他關係企業（如：國泰世華銀行），連線至產險內部正式應用系統及資料庫網段之情形，惟前述合約並未有明確約定，無法確認其連線之合理性。

五、貴公司辦理住宅火災保險核保作業，有未依新送審費率及造價參考表出單者，致未落實金融服務業公平待客原則之訂約公平誠信原則(如檢查意見二)，如：108.11.20以國產精字第1081100029號函採備查方式送審住宅火災保險費率，並依據新送審費率及新版造價參考表調整網路投保及核心系統參考數值，分別於108.11.1及108.11.22上線，惟查生效日於109年度且於108年10月底前出單之網路投保新契約，經公司清查有未依調降費率承保者計保單號碼150108ROW0****(生效日109.1.1)等10件；對於國泰人壽通路貸款續保案件轉檔漏未檢核，致未依最新造價參考表調高保額、調降費率出單者計保單號碼150209RO10****（生效日109.1.7）等13件。

六、貴公司辦理新契約保單地址與業務員地址之檢核控管作業，未建立一致性建檔標準，查有下列欠妥情事(如檢查意見三(七))：

(一)有未將往來控管之保、經代公司地址納入應檢核對象者，如：109.7.16於公司之車險承保系統，將新契約保單地址以公司往來之福灣保險代理人公司及國泰世華銀行地址進行測試，皆無法有效檢核。

(二)所訂檢核機制採完全比對，惟尚未建立一致性建檔標準，致同一地址多加鄰里或調整排列時即判斷為不同地

址，不利進行比對作業，如：109.7.16於新契約保單以中山通訊處、清水通訊處及北投分公司地址建檔，並依序於原地址加上「里」、將「之2號」調整為「號之2」及「A.B室」調整為「A室」進行測試，皆無法有效檢核。

七、辦理國內債券ETF投資，投資分析及決策作業有欠完整，查有下列欠妥事項(如檢查意見三(十))：

(一)採次級市場賣出交易，未於分析報告評估採次級市場與初級市場基金贖回作業之成本效益，如：108.1.24自次級市場(未採鉅額交易)賣出元大20年美債ETF(00679B)500千單位，並以每單位38.26元~38.27元成交，惟成交價格低於前交易日(108.1.23)該標的每單位淨值38.2977元，選擇於次級市場賣出，決策過程未敘明評估因素。

(二)投資債券ETF之分析報告僅列出投資區域及產業配置比例，未就集中度高之地區及產業風險進一步評估，投資分析作業有欠完整，如：基準日(109.5.31)持有國泰10年投資級公司債ETF(00725B)187,686千元，區域配置72.2%投資於美國，產業配置21.4%於通訊業；持有國泰1-5年高收益債券ETF(00727B)167,863千元，區域配置88.7%投資於美國，產業配置22.7%於通訊業。

八、貴公司辦理實質關係人交易控管作業，雖訂定「與交易觀察對象從事放款以外之其他交易自律規範」，惟查有定義之交易範圍欠完整，致有與第三人進行有實質關係人參與之交易未加以控管者(如檢查意見四(一))，如：108.3.27經總經理核准續承租「兆豐銀行受託國泰二號不動產投資信託基金專戶」之世界大樓2樓A1室及13樓A1室(租期108.5.1-110.4.30，每月租金各為142千元及211千元)，基金受託人雖為兆豐商業銀行，惟查該銀行將基金之不動產標

的管理及營運委由國泰建築經理(股)公司負責並簽訂委任契約，且擔任本案租賃契約之簽約代理人，因國泰建築經理(股)公司為公司利害關係人國泰建設(股)公司(董事蔡O諺為金控母公司董事蔡O達一等血親)百分之百持有，為公司實質利害關係人，惟未將其參與之交易列入準利害關係人業務控管，有欠周延。

九、貴公司辦理防火牆管理作業，未依最小授權原則設定，查有下列事項欠妥(如檢查意見四(四))：

(一)經查防火牆設定作業有欠嚴謹，核未落實所訂「通訊安全管理注意事項」第五條一、（九）「防火牆設定之變更應審慎評估並應經權責主管核可」之規定，如：

1、有申請設定非必要之業務連線情事，如：109.3.9防火牆設定申請單（表單序號：200309001757）新增防火牆CheckPoint 5800規則編號#77，允許防火牆Gateway（192.168.1.254）以FTP服務直接連線至正式區產險核心系統主機（601CXI1CSXAP01、602CXI2CSXAP01、602CXI2CSXAP02、602CXI2CSXAP03、602CXI2CSXAP04、602CXI2CSXAP05、602CXI2CSXAP06）。

2、防火牆設定有與申請單不一致之情形，如：103.9.25防火牆設定申請單（表單序號：140925000273）新增CheckPoint 5800規則編號#133，允許國泰世華銀行連線至產險正式應用程式伺服器區，目的位置實際設定為10.176.2.240，與防火牆申請單內容所記載之目的位置10.178.2.114、10.2.178.115不符。

(二)有開啟遠端桌面連線服務（Remote Desktop Protocol，RDP），未評估其安全性及必要性，不利系統主機安全，如：外部防火牆CheckPoint 5800編號#293、#330、#331等三條規則允許產險內湖資訊單位及營業單位，使

用遠端桌面連線至「零事故正式機主機」（主機位置：神坊資訊），進行伺服器維護及上版作業；規則編號#332允許產險內湖資訊單位遠端桌面連線至越南國泰產險對其建置Subversion（SVN）程式版控伺服器提供技術支援。

(三)規則設定有網路服務設定為any或all，過於寬鬆者，如：外部防火牆Check Point 5800編號#502～503、#510、#538、#540、#546等6條規則；內部防火牆FortiGate 1200D編號#664～667、#1586～1588、#1627、#1629、#1992～1993、#2221、#2407～2408、#2411、#2787等16條規則。

(四)外部防火牆CheckPoint 5800規則有串接之情形，易遭利用為攻擊跳板或成為資料外洩之管道，不利網路安全連線，如：

1、規則編號#62允許內湖資訊單位連線至正式非武裝區（Demilitarized zone，DMZ）之流量管理主機（F5）；同時編號#60規則允許流量管理主機（F5）連線至產險核心系統備份主機。

2、規則編號#293、#330、#331允許內湖資訊單位連線至零事故正式機主機（主機位置：神坊資訊）；同時規則編號#436允許零事故正式機主機連線至電商資料庫（B2C、B2E）（主機名稱：SVB016）。

十、為資安防禦縱深考量與建構整合資安體系，貴公司雖已導入資訊日誌管理系統（ArcSight）蒐集系統伺服器之日誌，惟尚未訂定異常事件監控預警之標準作業程序，且實地檢查發現日誌收容範圍有欠完整之情事(如檢查意見四(六))，如：未納入旅責險（雄獅）、保經代B2B等第一類系統主機及屬第二類系統主機產險核心系統，不利即時發現異常事件。

十一、檢查期間(109.7.8)發現貴公司官網（https://www.cathay-ins.com.tw/cathayins/personal/ ）、B2B保經代系統（https://b2b.cathay-ins.com.tw/INSBAWeb/html/CM/loginb2b.jsp）及B2B旅責險系統（https://tl.cathay-ins.com/），設計存有下列安全漏洞，易受攻擊風險(如檢查意見四(十))，如：

（一）接受Diffie-Hellman不安全加密方式及不支援Forward Secrecy保密功能，此弱點具有造成資訊洩漏並導致攻擊者進行中間人攻擊（Man-in-the-Middle Attack，MITM）等風險。

（二）對用戶端瀏覽之設定，未採用安全標頭（Headers）設計，如：Referrer-Policy保護資訊洩漏、Feature-Policy管控特定應用程式介面（API）或瀏覽器功能及Content-Security-Policy防禦跨網站指令攻擊等安全標頭，不利防範網路攻擊。

（三）公司對外網站可接受使用不安全之密碼加密模式TLS 1.1，導致攻擊者可就網站伺服器與使用者間之通訊進行解密，不利網頁連線安全。

十二、貴公司對資料庫存取紀錄之稽核軌跡，雖已集中收容於資料庫稽核軟體（Imperva），並由系統產出「資料庫登入失敗」、「資料庫稽核軌跡備份還原測試紀錄」等月報表，陳核資深副總經理，惟對委託國泰人壽管理資料庫主機，並授與資料庫管理員帳號供其使用，經查對該等資料庫管理員權限之使用情形，尚未設計產製月報，不利及時發現異常使用行為(如檢查意見四(十二))，如：產險核心系統資料庫（CXI1CSDP01、CXI1HSDP01、CXI1CSDP09）、客服系統資料庫（SVB012）、電商資料庫（B2C、B2E）（SVB016、SVB021）、員工入口網資料庫（SVB018、SVB025）。

理由及法令依據：

一、上述事實一，公司辦理身心障礙者投保業務有未比照一般之核保規則確實執行核保評估作業，違規事實明確，核與保險法第148條之3第2項授權訂定之「保險業招攬及核保理賠辦法」第7條第1項第11款及第17條規定不符，依保險法第171條之1第5項規定，核處新臺幣60萬元整。

二、上述事實二，公司辦理核保作業有未徵提汽車延長保固契約、未留存核算保費之佐證資料及未依保險商品內容予以評估並簽署承保等情事，違規事實明確，核與行為時保險法第148條之3第2項授權訂定之行為時「保險業招攬及核保理賠辦法」第7條第1項第8款第2目及第17條不符，依保險法第171條之1第5項規定，核處新臺幣60萬元整。

三、上述事實三，公司推出新服務有未由總機構法令遵循主管出具符合法令規章及內部規範之意見並簽署負責，違規事實明確，核與保險法第148條之3第1項授權訂定之「保險業內部控制及稽核制度實施辦法」第32條第3項第3款規定不符，依保險法第171條之1第4項規定，核處新臺幣60萬元整。

四、上述事實四，公司委由集團關係企業辦理資訊維護作業，未明確訂定控管機制，不利權責劃分及作業遵循，違規事實明確，核與保險法第148條之3第1項授權訂定之「保險業內部控制及稽核制度實施辦法」第6條第1項第6款及第8款規定不符，依保險法171條之1第4項規定，核處新臺幣60萬元整。

五、上述事實五，公司辦理住宅火災保險核保作業，有未依新送審費率及造價參考表出單，核有礙健全經營之虞，依保險法第149條第1項規定予以糾正。

六、上述事實六、七、八，違失事實明確，核有礙健全經營之虞，依保險法第149條第1項規定各處1項糾正，計3項糾

正。

七、上述事實九、十、十一、十二，公司辦理資訊作業，有未依最小授權原則設定、未訂定異常事件監控預警之標準作業程序、官網、B2B保經代系統及B2B旅責險系統設計存有安全漏洞、未設計產製資料庫管理員權限之使用情形月報等情事，違失事實明確，核有礙健全經營之虞，依保險法第149條第1項規定予以糾正。

繳款方式：

一、繳款期限：自本處分送達之次日起10日內繳納。

二、請依本會保險局檢附之繳款單注意事項辦理繳納。

注意事項：

一、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二段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，受處分人仍應繳納罰鍰。

二、受處分人如逾本處分所定繳款期限不繳納罰鍰者，即依行政執行法第4條第1項但書規定，移送法務部行政執行署各分署辦理行政執行。

正本：國泰世紀產物保險股份有限公司

副本：本會檢查局、保險局

主任委員 黃天牧

授權單位主管決行