

200823807

發明專利說明書

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：P514301X

※申請日期：95.11.20 ※IPC分類：G07F19/00 · G06Q40/00 · 40/00

一、發明名稱：(中文/英文)

以電話號碼及識別碼做為金融服務系統中防弊之方法

二、申請人：(共1人)

姓名或名稱：(中文/英文)

林仲宇 CHUNG-YU LIN

代表人：(中文/英文)

住居所或營業所地址：(中文/英文)

高雄市左營區博愛四路 236 號 21 樓

21F., No.236, Bo-ai 4th Rd., Zuoying District, Kaohsiung City 813, Taiwan
(R.O.C.)

國籍：(中文/英文) 中華民國(TW)

三、發明人：(共1人)

姓名：(中文/英文)

林仲宇 CHUNG-YU LIN

國籍：(中文/英文)

中華民國 (TW)

四、聲明事項：

主張專利法第二十二條第二項第一款或第二款規定之事實，其事實發生日期為： 年 月 日。

申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

有主張專利法第二十七條第一項國際優先權：

無主張專利法第二十七條第一項國際優先權：

主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

主張專利法第三十條生物材料：

須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係提供一種「以電話號碼及識別碼做為金融服務系統中防弊之方法」，其是透過銀行開戶的帳戶擁有者向所屬銀行提供一組併列的「電話號碼或識別碼」，並將該組「電話號碼或識別碼」登錄儲存於該銀行內部的電腦資料庫內，使其做為銀行與帳戶擁有者之間各項金融服務上的授權認證依據，除能確保彼此各項金融交易上的更為安全外，更能有效杜絕金錢被盜領、詐領或信用卡被盜刷等犯罪行為發生。

【先前技術】

按，自從塑膠貨幣問世以來，許多金融市場的交易行為除傳統親臨銀行櫃台辦理外，更多的是已由金融卡、信用卡等非現鈔型式來完成，另加上網路的盛行與便利，使得金融卡或信用卡的使用更加延伸至網路線上的消費型態，但隨著其使用普遍性的擴大卻也衍生出許多金融交易上的缺失與弊端如下：

一、當金融卡不慎遺失或遭竊時：

由於銀行業者競爭的關係，許多人均同時擁有一張以上不同家銀行所製發的金融卡，而每年卻也都在發生

金融卡遺失的案件，雖然撿拾或偷竊而來的他人金融卡，在未知其密碼的情況下是無法盜領其金錢的，但只要持卡人週遭朋友或同事在別有用心下，並不難探知其密碼，例如：某些持卡人在 ATM 存取款的過程中，被周遭有心人士的蓄意偷窺下而得知其密碼，再尾隨持卡人伺機偷竊來取得其金融卡，或者，有些怕記不住自己金融卡密碼者，常會將其密碼書寫在小紙片上後再與金融卡置放一起，乃反而輕易地洩露了密碼，再者，更有許多人有將個人身份證件(如身份證、健保卡、駕駛執照、學生證、工作證等)與金融卡合置於同一皮夾內的習慣，遇有皮夾遺失或遭竊時，撿拾者或偷竊者即會將個人身份證件上的數字資料，先行多次排列組合，再經多次的嘗試錯誤修正後而得知密碼；凡此諸多原因及方法而獲取他人金融卡及其密碼後，而再加以盜領成功的案件確實不在少數，然而遭受這些實質損失金錢的遺失者或遭竊者除自嘆倒楣外，更得面對打電話趕緊一家一家銀行去掛失金融卡，以及後續請領補發金融卡等繁雜手續的精神損失負荷。

二、當包含金融卡在內的帳戶被金融罪犯使用時：

近來諸多的金融犯罪案件也有逐年增加的趨勢，政府與銀行業者莫不急於設立許多防範措施，諸如：規定

銀行開戶需具備第二身份證件、設定每日 ATM 轉帳金額上限、加強宣導金融犯罪型態之認識與檢舉、金融從業人員加強辨識金融犯罪之再教育、以及強力查緝人頭帳戶與通報註銷等，然而透過人頭帳戶（亦稱假帳戶）行詐騙轉帳匯款之案件仍是層出不窮，且最令警方扼腕的是，某些犯罪者配合具有電腦專長的人員，經由網路（Internet）擷取他人銀行帳戶，再輾轉由他人帳戶（非人頭帳戶）轉匯入犯罪者的帳戶內來取得贓款，有時為增加警方追緝的難度，會增加轉匯的次數，如此一來便會有許多不知情的帳戶擁有者被當成嫌疑共犯來被偵辦，而蒙受不白之冤與困擾，這些犯罪型態亦是對眾多使用網路銀行或從事網路商業活動者的拌腳石。

三、當信用卡不慎遺失或遭竊或遭偽造時：

持信用卡來從事日常食、衣、住、行、育、樂等消費已是現代人極為普遍的消費模式，再加上發行信用卡銀行各種優惠商業策略推波助瀾下，許多人更是同時持有多張的信用卡，因此，當信用卡遺失或遭竊時，也就成為金融犯罪者另一犯罪使用的對象，持用他人遺失或竊取而來的信用卡，去盜刷購物，再變賣來換取金錢便經常發生，遺失或遭竊信用卡的持卡人不但須蒙受金錢損失，同時還得撥電話向發卡銀行掛失，並承擔後續短

暫無卡使用的不便窘境，萬一被製造偽卡集團偽造自己的信用卡時，還得為涉嫌偽造文書罪之刑事官司的糾葛而煩腦，惟，為何信用卡屢遭偽造盜刷的案件至今仍不減反增呢？如第一圖所示，係為現行信用卡之使用流程，當信用卡持卡者 10 至店家或網路交易對象 1 行刷卡或線上刷卡時，該店家或網路交易對象 1 會主動向發行信用卡銀行 2 要求授權，經由發行信用卡銀行 2 內部資訊處理中心查核該信用卡持卡者 10 的信用資料後（如卡號資料、刷卡金額額度等），如條件符合則會回覆”同意授權”的指示予店家或網路交易對象 1，並在該店或網路交易對象 1 的刷卡機上或網路頁面上顯示刷卡成功；反之，若條件不符合，則回覆”不同意授權”的指示予店家或網路交易對象 1，並在該店家或網路交易對象 1 的刷卡機上或網路頁面上顯示刷卡失敗；前述刷卡交易過程中，店家人員僅能從刷卡單上的簽名來核對與信用卡上的簽名字跡是否相同，通常只要簽名不太離譜時，店家人員均會予以認可，而盜刷者要仿造簽名並非難事，只需在盜刷前依樣畫葫蘆多練習該信用卡上的簽名字跡幾次後，均能矇騙過關，再者，網路線上刷卡更不須看簽名字跡，只需依序輸入卡號，使用年限等資料即可，由此觀之，在現行信用卡的使用上既無任何簡易

又可靠的機制來做為防堵反制的措施下，不論真卡或偽卡的盜刷案件發生率一再地不斷升高，也就不足為奇矣。

【發明內容】

本發明之主要目的在提供一種「以電話號碼及識別碼做為金融服務系統中防弊之方法」，係由金融開戶之帳戶擁有者，自行提供一組併列「電話號碼及識別碼」的專屬授權認證資料，給其所有開立帳戶往來的金融單位，而該所有開立帳戶往來的金融單位在核對該帳戶擁有者的相關身份證明資料後，即將該組併列「電話號碼及識別碼」的專屬授權認證資料，給予登錄儲存在其金融單位的內部電腦資料庫；當各金融單位受理帳戶擁有者進行各項金融服務時，例如：臨櫃存取款或匯款、持金融卡至 ATM 存取款或轉帳匯款、網路銀行轉帳匯款等，除執行對原有帳號、密碼、動態密碼卡等查核比對外，更同步執行比對其與登錄儲存於該金融單位內部電腦資料庫中專屬「電話號碼及識別碼」的授權認證資料是否相符合，使銀行能同步確定該項或該次的交易服務，是否確為該帳戶擁有者真正授權下所為之交易，進而可避免因身份資料遭竊，或金融卡遺失及其密碼被竊知等，所導致金錢被盜領或詐領等弊端情事的發生。

本發明之另一目的在提供一種「以電話號碼及識別碼做為金融服務系統中防弊之方法」，係由金融開戶之帳戶擁有者，自行提供一組併列「電話號碼及識別碼」的專屬授權認證資料，給其所有開立帳戶往來的金融單位，而該所有開立帳戶往來的金融單位在核對該帳戶擁有者的相關身份證明資料後，即將該組併列「電話號碼及識別碼」的專屬授權認證資料，給予登錄儲存在其金融單位的內部電腦資料庫；當各金融單位受理帳戶擁有者持信用卡進行刷卡或線上刷卡時，除執行對原有卡號查核比對外，更同步執行比對其與登錄儲存於該金融單位內部電腦資料庫中專屬「電話號碼及識別碼」的授權認證資料是否相符合，使銀行能同步確定該項或該次的刷卡交易，是否確為該帳戶擁有者真正授權下所為之信用卡交易，進而可避免因信用卡遺失、遭竊等，所導致被盜刷弊端情事的發生。

【實施方式】

如第二圖所示，本發明是一種「以電話號碼及識別碼做為金融服務系統中防弊之方法」，其步驟包含：

a、至金融單位填寫「存款相關業務申請書」辦理開戶。

b、依法定「存款開戶總約定書」之規定，憑身

份證及第二身份證明文件，並就簽名或蓋章擇一或合併留存建檔於金融單位備查。

c、開戶者自行提供一組併列的「電話號碼及識別碼」給金融單位，以做為其專屬之授權認證資料。

d、由金融單位依「受理開戶作業檢核表」審查後，核准開戶並核發開戶帳簿及/或金融卡。

e、金融單位將開戶者之個人身分資料、帳戶名、金融卡號及密碼等資料，登錄儲存於其內部的電腦資料庫內，並將該開戶者所提供之「電話號碼及識別碼」授權認證資料，另登錄儲存於其內部電腦所設的”授權認證資料庫”內。

其中，前述各步驟中所述之「存款相關業務申請書」、「存款開戶總約定書」及「受理開戶作業檢核表」等書類或審核標準，其在格式或內容中所規定的諸多事項或合約條款，均係由各金融單位自行依據其所屬國家之法律來制定而成，不同國家及其所屬的金融單位，對其所使用的名稱雖會有些許不同，但相關法律所規範的本質仍屬相同，先併予說明。

而，在該步驟 c 中之「電話號碼」，係可為開戶者(即帳戶擁有者)家中或公司的固網電話號碼，或為個人行動電話號碼，或是冠有國別碼及區域碼的固網

電話號碼，或是冠有國別碼的行動電話號碼；且該「識別碼」係可由任何在電腦中可輸入的文字、數字、符號或其兩者以上之組合所構成，並得由開戶者(即帳戶擁有者)在提供登錄儲存後，依循金融單位所規範之流程或方式，逕自做隨時任意之修改或變更。

另外，步驟 e 中該金融單位內部電腦所設之”授權認證資料庫”，係可變更設置於非屬該金融單位內部的電腦系統所操控，而是屬於外界其他電腦系統中所建置之”外部授權認證資料庫”，使能降低該金融單位電腦作業系統的維護成本。

續如第三圖及第四圖所示，係本發明使用於親臨銀行櫃檯辦理金融服務之流程；當帳戶擁有者 20 攜帶開戶帳簿與簽章至銀行 30 臨櫃辦理存、取款或匯款手續時，先填寫金額於存款單或取款單或匯款單上，以及其帳戶的帳號與密碼，接著再輸入其授權認證資料 31 專屬之「電話號碼及識別碼」【例如：1234567（電話號碼）+ JohnLins007(識別碼)】後，該銀行 30 內部的銀行電腦資訊處理中心 32，除立即執行既有核對帳戶戶名、帳號、密碼等資料與金額外，並同時會對建置於該銀行 30 內的授權認證資料庫 33 發出”要求比對”的指令，在有比對得出與登錄

儲存於該授權認證資料庫 33 內完全相符合之一組「電話號碼及識別碼」時，該授權認證資料庫 33 即會回覆給該銀行電腦資訊處理中心 32 一個”認證符合”的指令，且該銀行電腦資訊處理中心 32 亦隨即向帳戶擁有者 20 發出存取款或匯款成功的訊息，使該帳戶擁有者 20 完成其所要求的存取款或匯款等手續，同時也表示該次的交易服務，確實是該帳戶擁有者 20 真正授權下所完成的一次金融交易。

反之，若比對得出與登錄儲存於該授權認證資料庫 33 內，無任何相符合的一組「電話號碼及識別碼」時，該授權認證資料 33 即會回覆給該銀行電腦資訊處理中心 32 一個”認證不符”的指令，並藉由該銀行電腦資訊處理中心 32 發出”重新輸入”的訊息給帳戶擁有者 20，換言之，除非是真正的帳戶擁有者 20 自己，或經該帳戶擁有者 20 同意所告知其「電話號碼及識別碼」的代理人之外，任何人即使出具帳戶戶名、帳號及密碼等資料，仍因在無法得知「電話號碼及識別碼」的情況下，而不能在臨櫃的情形下來取得該帳戶擁有者 20 帳戶內的任何金錢，因此，對於非由帳戶擁有者 20 真正授權下的非法臨櫃取款行為將能完全杜絕。再者，前述銀行 30 現有內

部金融電腦作業系統的軟、硬設備，在既有營運下均已非常完備，其可能不願額外花費建置本發明所需授權認證資料庫 33 的成本，因此，如第四圖所示，只要銀行 30a 將其銀行電腦資訊處理中心 32a 的軟體程式稍作修改，而將每次要求比對的指令，經由網路 W 傳送至建置於外界另一電腦系統中的外部授權認證資料庫 40，仍可達成比對相符合或不相符合的認證功能，因為該外部授權認證資料庫 40 係與許多銀行金融單位相互連網，每一位在各金融銀行 30a 開戶後的帳戶擁有者 20，其所提供專屬「電話號碼及識別碼」之授權認證資料 31a，均經由各金融銀行 30a 直接透過網路 W 而登錄儲存於該外部授權認證資料庫 40 內，故各銀行 30a 要導入本發明的技術程度極為簡單，除立即可實施外又不增加營運成本。

再如第五圖及第六圖所示，係本發明使用於 ATM 機器 50(俗稱自動櫃員機)金融服務之流程；當帳戶擁有者 20 攜帶金融卡至 ATM 機器 50，辦理存、取款或匯款手續時，先將金融卡插入 ATM 機器 50 內，經輸入金融卡密碼及金額後，該 ATM 機器 50 操作畫面上會出現一「電話號碼及識別碼」欄位 51，帳戶擁有者 20 必須在該「電話號碼及識別碼」欄位

51 內輸入其專屬「電話號碼及識別碼」的授權認證資料 52，否則無法進行後續的交易程序，若已輸入正確的「電話號碼及識別碼」之授權認證資料 52【例如：1234567（電話號碼）+ JohnLins007(識別碼)】後，該 ATM 機器 50 所屬銀行 60 的銀行電腦資訊處理中心 61，除立即執行既有核對金融卡號及密碼資料與金額外，並同時會對建置於該銀行 60 內的授權認證資料庫 62 發出”要求比對”的指令，在有比對得出與登錄儲存於該授權認證資料庫 62 內，完全相符合之一組「電話號碼及識別碼」時，該授權認證資料庫 62 即會回覆給銀行電腦資訊處理中心 61 一個”認證符合”的指令，且該銀行電腦資訊處理中心 61 亦隨即發出”同意存款或出鈔或轉帳”成功的訊息至 ATM 機器 50，而使該持有金融卡的帳戶擁有者 20，可從該 ATM 機器 50 上完成其所需之存款或出鈔或轉帳成功之交易手續，同時也表示該次在 ATM 機器 50 上的交易服務，確實是該帳戶擁有 20 真正授權下所完成的一次金融交易。

反之，若比對得出與登錄儲存於該授權認證資料庫 62 內，無任何相符合的一組「電話號碼及識別碼」時，該授權認證資料庫 62 即會回覆給該銀行電

腦資訊處理中心 61 一個”認證不符”的指令，並藉由該銀行電腦資訊處理中心 61 而使 ATM 機器 50 上的畫面出現”重新輸入”「電話號碼及識別碼」的訊息給帳戶擁有者 20；因此，任何撿拾或偷竊所取得的金融卡，即使得知其密碼，亦會因不知「電話號碼及識別碼」，而無法從 ATM 機器 50 上來取款或轉帳竊得贓款，相對地，因不慎遺失或遭竊金融卡的帳戶擁有者 20，也不必再害怕帳戶內的金錢遭盜領所導致的實質金錢損失，更不必急著打電話向核發金融卡的銀行來通報掛失之手續，故可消除來自偷竊他人金融卡及密碼的犯罪案件。

再者，如第六圖所示者，該 ATM 機器 50 所屬銀行 60a 導入本發明之方法時，其內部亦可免去建置授權認證資料庫 62 的成本，而選擇每次將來自 ATM 機器 50 的「電話號碼及識別碼」專屬授權認證資料 52，經銀行電腦資訊處理中心 61a 送出”要求比對”指令，再透過網路 W 傳送至外界的外部授權認證資料庫 40，仍可達成執行比對是否相符合之認證功能。

又如第七圖及第八圖所示，係本發明使用於網路線上轉帳匯款金融服務之流程；當帳戶擁有者 20 經由網路 W 連結至所屬帳戶的網路銀行 70 後，在其

顯示頁面的主欄位 71 內，除應輸入”使用者名稱及動態密碼(OTP)”之既有規定與金額外，必須再於另一增設的授權認證欄位中，輸入其專屬「電話號碼及識別碼」的授權認證資料 72【例如：1234567(電話號碼)+JohnLins 007(識別碼)】，否則無法進行後續的轉帳程序，若已輸入正確的「電話號碼及識別碼」之授權認證資料 72 後，該網路銀行 70 的電腦資訊處理中心 73，除立即執行既有核對使用者名稱及動態密碼(OTP)與轉帳金額外，並同時會對建置於內部系統的授權認證資料庫 74 發出”要求比對”的指令，在有比對得出與登錄儲存於該授權認證資料庫 74 內完全相符合之一組「電話號碼及識別碼」時，該授權認證資料庫 74 即會回覆給電腦資訊處理中心 73 一個”認證符合”的指令，且該電腦資訊處理中心 73 亦隨即發出”線上轉帳成功”的訊息，並直接顯示在網路銀行 70 的頁面上，得供帳戶擁有者 20 直接從其上網工具(例如電腦、PDA 等)的顯示屏幕上，而得知線上轉帳(付款)交易完成，同時也表示該次在線上的交易服務，確實是該帳戶擁有者 20 真正授權下所完成的一筆金融交易。

反之，若比對得出與登錄儲存於該授權認證資

料庫 74 內，無任何相符合的一組「電話號碼及識別碼」時，該授權認證資料庫 74 即會回覆給該電腦資訊處理中心 73 一個”認證不符”的指令，並藉由該電腦資訊處理中心 73 而使網路銀行 70 的頁面上，出現”重新輸入”「電話號碼及識別碼」的訊息給帳戶擁有者 20；因此，即便再具有高度電腦專長的專家，雖在竊得他人帳戶資料後，而想進行線上轉帳獲得贓款，仍會因無法得知其「電話號碼及識別碼」的授權認證資料下無法得逞，更遑論能進行掩飾犯行之多次轉帳伎倆矣。

再者，如第八圖所示者，該網路銀行 70a 所屬銀行的電腦資訊處理中心 73a，其內部亦可免去建置授權認證資料庫 74 的成本，而選擇每次將來自電腦資訊處理中心 73a 的「電話號碼及識別碼」專屬授權認證資料 72a，經該電腦資訊處理中心 73a 送出”要求比對”指令，再透過網路 W 傳送至外界的外部授權認證資料庫 40，仍可達成執行比對是否相符合之認證功能。

如第九圖所示，係本發明中以電話號碼及識別碼做為信用卡使用流程防弊之方法，其步驟包含：

- a、填寫信用卡發卡銀行所提供之「信用卡申請

書」；

b、於該「信用卡申請書」上留存簽名的形式，並提供身份證與第二身份證明文件及相關財力證明，以供信用卡發卡銀行建檔備存；

c、申請信用卡者自行提供一組併列的「電話號碼及識別碼」給信用卡發卡銀行，以做為其專屬之授權認證資料；

d、由信用卡發卡銀行審查後，核發信用卡並郵寄給信用卡持卡人；

e、信用卡發卡銀行將持卡人之個人身分資料及信用卡卡號等資料，登錄儲存於其內部的電腦資料庫內，並將該信用卡持卡人所提供之「電話號碼及識別碼」授權認證資料，另登錄儲存於其內部電腦所設的”授權認證資料庫”內。

其中，該步驟c中之「電話號碼」，係可為信用卡持卡人家中或公司的固網電話號碼，或個人行動電話號碼，或是冠有國別碼及區域碼的固網電話號碼，或是冠有國別碼的行動電話號碼者；且該「識別碼」，係可由任何在電腦中可輸入的文字、數字、符號或其兩者以上之組合所構成，並得由信用卡持卡人在提供登錄儲存後，依循信用卡發卡銀行所規範之流程或方

式，而可主動進行做隨時任意之修改或變更者。

又，步驟 e 中該信用卡發卡銀行內部電腦所設之”授權認證資料庫”，係可變更設置於非屬該信用卡發卡銀行內部的電腦系統所操控，而是屬於外界其他電腦系統中所建置之”外部授權認證資料庫”，使能降低該信用卡發卡銀行電腦作業系統的維護成本。

請參閱第十圖所示，係本發明使用於信用卡的實施例；當信用卡持卡者 10 至店家或網路交易對象 1 行刷卡或線上刷卡時，店家人員先將信用卡於刷卡機上過卡後，即會要求該信用卡持卡者 10，必須再於該刷卡機上按壓輸入其信用卡所相對應的「電話號碼及識別碼」之授權認證資料 3，假若，該信用卡持卡者 10 不願依店家人員之指示按壓輸入時，店家人員可立刻回絕該信用卡持卡者 10 當次的刷卡交易；同樣地，信用卡持卡者 10 於線上刷卡時，其網路頁面上亦會有要求輸入其信用卡所相對應的「電話號碼及識別碼」之授權認證資料 3，假如信用卡持卡者 10 不願輸入該授權認證資料 3 時，便會被拒絕其線上刷卡手續；上述之程序即可作為防止盜刷行為的第一道防衛機制。

因此，當信用卡持卡者 10 繼續依店家人員或線

上之指示，接著在刷卡機上按壓或網路頁面中輸入其「電話號碼及識別碼」之授權認證資料 3 後，信用卡發卡銀行 90 內部的銀行電腦資訊處理中心 91，除立即執行既有核對持卡者之卡號資料與刷卡金額外，並同時會對建置於內部系統的授權認證資料庫 92 發出”要求比對”的指令，在有比對得出與登錄儲存於該授權認證資料庫 92 內完全相符合之一組「電話號碼及識別碼」時，該授權認證資料庫 92 即會回覆給銀行電腦資訊處理中心 91 一個”認證符合”的指令，且該銀行電腦資訊處理中心 91 亦隨即發出”同意授權刷卡”的訊息給店家或網路交易對象 1，即可完成成功刷卡之手續；反之，除真正的信用卡持卡者 10 本人知道其「電話號碼及識別碼」以外，其他任何撿拾、偷竊或偽造所取得的信用卡，將因無法得知「電話號碼及識別碼」之授權認證資料 3 下，而無法盜刷使用該不當取得的信用卡，相對地，因不慎遺失或遭竊信用卡的信用卡持卡者 10，也不必再害怕被盜刷所導致的實質金錢損失，更不必急著打電話向核發信用卡的銀行來通報掛失之手續，故確實可完全消除信用卡被盜刷的犯罪案件。

綜上所陳，本發明應用「電話號碼及識別碼」作

為銀行與帳戶擁有者間之授權認證資料，使其做為銀行與帳戶擁有者之間各項金融服務上的授權認證依據，除能確保彼此各項金融交易上的更為安全外，更能有效杜絕金錢被盜領、詐領或信用卡被盜刷等犯罪行為發生，確具有高度創新與產業利用性；至於使用「電話號碼」及「識別碼」的優點，在本案發明人另外於民國93年4月30日（2004年4月30日）向鈞局所提出第93112373號「以數個特定電話號碼依序排列組合成之數字串列冠上識別碼作為搜尋網際網路特定電腦IP位址之系統」之發明專利中，已有揭露陳述，且本案發明人亦在隨後按依該技術內容而設立了「www.2udg.com」網站，來實際加以實施運作至今，完全達成所預期之功效，惟，有關其運用之電腦軟硬體技術均為熟悉該項技術人員所公知，且亦非本案之標的，故在此不予以贅述，特予說明。

【圖式簡單說明】

第一圖：係習知信用卡使用流程之方塊圖。

第二圖：係本發明之步驟方塊圖。

第三圖：係本發明使用於親臨銀行櫃檯辦理金融服務的流程圖之一。

第四圖：係本發明使用於親臨銀行櫃檯辦理金融服

務的流程圖之二。

第五圖：係本發明使用於 ATM 自動櫃員機之金融服務流程圖之一。

第六圖：係本發明使用於 ATM 自動櫃員機之金融服務流程圖之二。

第七圖：係本發明使用於網路線上轉帳匯款金融服務之流程圖之一。

第八圖：係本發明使用於網路線上轉帳匯款金融服務之流程圖之二。

第九圖：係本發明應用於信用卡使用流程之步驟方塊圖。

第十圖：係本發明使用於信用卡流程之流程圖。

【主要元件符號說明】

1-店家或網路交易對象

2、90-發行信用卡銀行

10-信用卡持卡者

20-帳戶擁有者

30、30a、60a-銀行

3、31、31a、52、72、72a-授權認證資料

32、32a、61、61a、73、73a、91-銀行電腦資訊處理

中心

200823807

33、62、74、92-授權認證資料庫

40-外部授權認證資料庫

50-ATM 機器

51-「電話號碼及識別碼」欄位

70、70a-網路銀行

71-主欄位

W-網路

五、中文發明摘要：

本發明有關一種「以電話號碼及識別碼做為金融服務系統中防弊之方法」，其係在現有各項金融作業系統中，經由帳戶擁有者另外提供一組併列的「電話號碼及識別碼」予其所有開立帳戶往來的銀行，而該所有往來銀行內部電腦資料庫中，除儲存該帳戶擁有者既有相關的個人身份證明資料、金融卡帳號密碼、信用卡資料或網路銀行之「使用者名稱」與「動態密碼卡(OTP ToKen)」等資料外，再增加登錄儲存其所專屬的「電話號碼及識別碼」之授權認證資料於該銀行內部的授權認證資料庫中；當銀行受理帳戶擁有者進行各項金融服務時，(例如：臨櫃存取款或匯款、持金融卡至ATM存取款或轉帳匯款、持信用卡刷卡或線上刷卡等)，除在銀行內部電腦資料庫中執行對原有帳號、密碼、動態密碼卡等查核比對外，更同步執行比對其與登錄儲存於該銀行內部授權認證資料庫中專屬「電話號碼及識別碼」的授權認證資料是否相符合，使銀行能同步確定該項或該次的交易服務，是否確為該帳戶擁有者真正授權下所為之交易，進而可避免因身份資料遭竊，或金融卡遺失及其密碼被竊知，或信用卡及其資料遺失遭竊等，所導致金錢被盜領、詐領或盜刷等弊端情事的發生。

六、英文發明摘要：

十、申請專利範圍：

1. 一種「以電話號碼及識別碼做為金融服務系統中防弊之方法」，其步驟包含：

a、至金融單位填寫「存款相關業務申請書」辦理開戶；

b、依法定「存款開戶總約定書」之規定，憑身份證及第二身份證明文件，並就簽名或蓋章擇一或合併留存建檔於金融單位備查；

c、開戶者自行提供一組併列的「電話號碼及識別碼」給金融單位，以做為其專屬之授權認證資料；

d、由金融單位依「受理開戶作業檢核表」審查後，核准開戶並核發開戶帳簿及/或金融卡；及

e、金融單位將開戶者之個人身分資料、帳戶名、金融卡號及密碼等資料，登錄儲存於其內部的電腦資料庫內，並將該開戶者所提供之「電話號碼及識別碼」授權認證資料，另登錄儲存於其內部電腦所設的”授權認證資料庫”內。

2. 如申請專利範圍第1項所述之「以電話號碼及識別碼做為金融服務系統中防弊之方法」，其中，步驟a所述之「存款相關業務申請書」、步驟b所述之「存款開戶總約定書」及其有關身份證明文件與簽章形式、以

及步驟 d 所述之「受理開戶作業檢核表」等書類或審核標準，其在格式或內容中所規定的諸多事項或合約條款，均係由各金融單位自行依據其所屬國家之法律來制定而成。

3. 如申請專利範圍第 1 項所述之「以電話號碼及識別碼做為金融服務系統中防弊之方法」，其中，該步驟 c 中之「電話號碼」，係可為開戶者家中或公司的固網電話號碼，或個人行動電話號碼，或是冠有國別碼及區域碼的固網電話號碼，或是冠有國別碼的行動電話號碼者。
4. 如申請專利範圍第 1 項所述之「以電話號碼及識別碼做為金融服務系統中防弊之方法」，其中，該步驟 c 中之「識別碼」，係可由任何在電腦中可輸入的文字、數字、符號或其兩者以上之組合所構成，且得由開戶者在提供登錄儲存後，依循金融單位所規範之流程或方式，而可主動進行做隨時任意之修改或變更者。
5. 如申請專利範圍第 1 項所述之「以電話號碼及識別碼做為金融服務系統中防弊之方法」，其中，步驟 e 中該開戶者所提供之「電話號碼及識別碼」授權認證資料，更可登錄儲存於非屬該金融單位內部電腦系統所操控之”外部授權認證資料庫”中者。

6. 一種「以電話號碼及識別碼做為信用卡使用流程防弊之方法」，其步驟包含：

a、填寫信用卡發卡銀行所提供之「信用卡申請書」；

b、於該「信用卡申請書」上留存簽名的形式，並提供身份證與第二身份證明文件及相關財力證明，以供信用卡發卡銀行建檔備存；

c、申請信用卡者自行提供一組併列的「電話號碼及識別碼」給信用卡發卡銀行，以做為其專屬之授權認證資料；

d、由信用卡發卡銀行審查後，核發信用卡；及

e、信用卡發卡銀行將持卡人之個人身分資料及信用卡卡號等資料，登錄儲存於其內部的電腦資料庫內，並將該信用卡持卡人所提供之「電話號碼及識別碼」授權認證資料，另登錄儲存於其內部電腦所設的”授權認證資料庫”內。

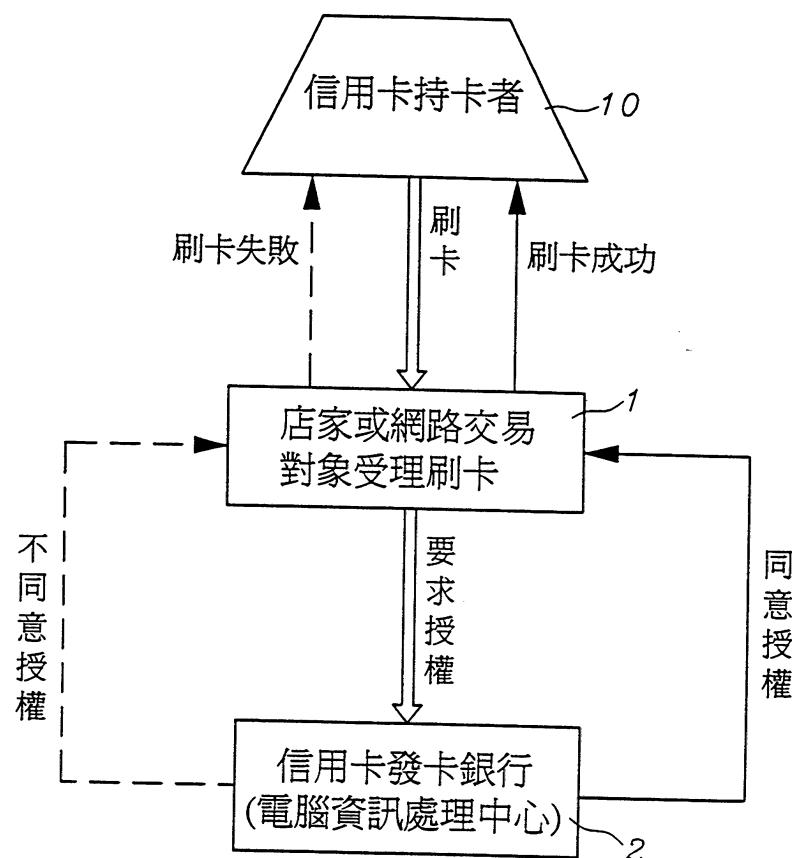
7. 如申請專利範圍第 6 項所述之「以電話號碼及識別碼做為信用卡使用流程防弊之方法」，其中，步驟 a 與步驟 b 所述「信用卡申請書」及其有關身份證明文件與簽章形式，其在格式或內容中所規定的諸多事項或合約條款，均係由各信用卡發卡銀行自行依據其所屬國

家之法律來制定而成。

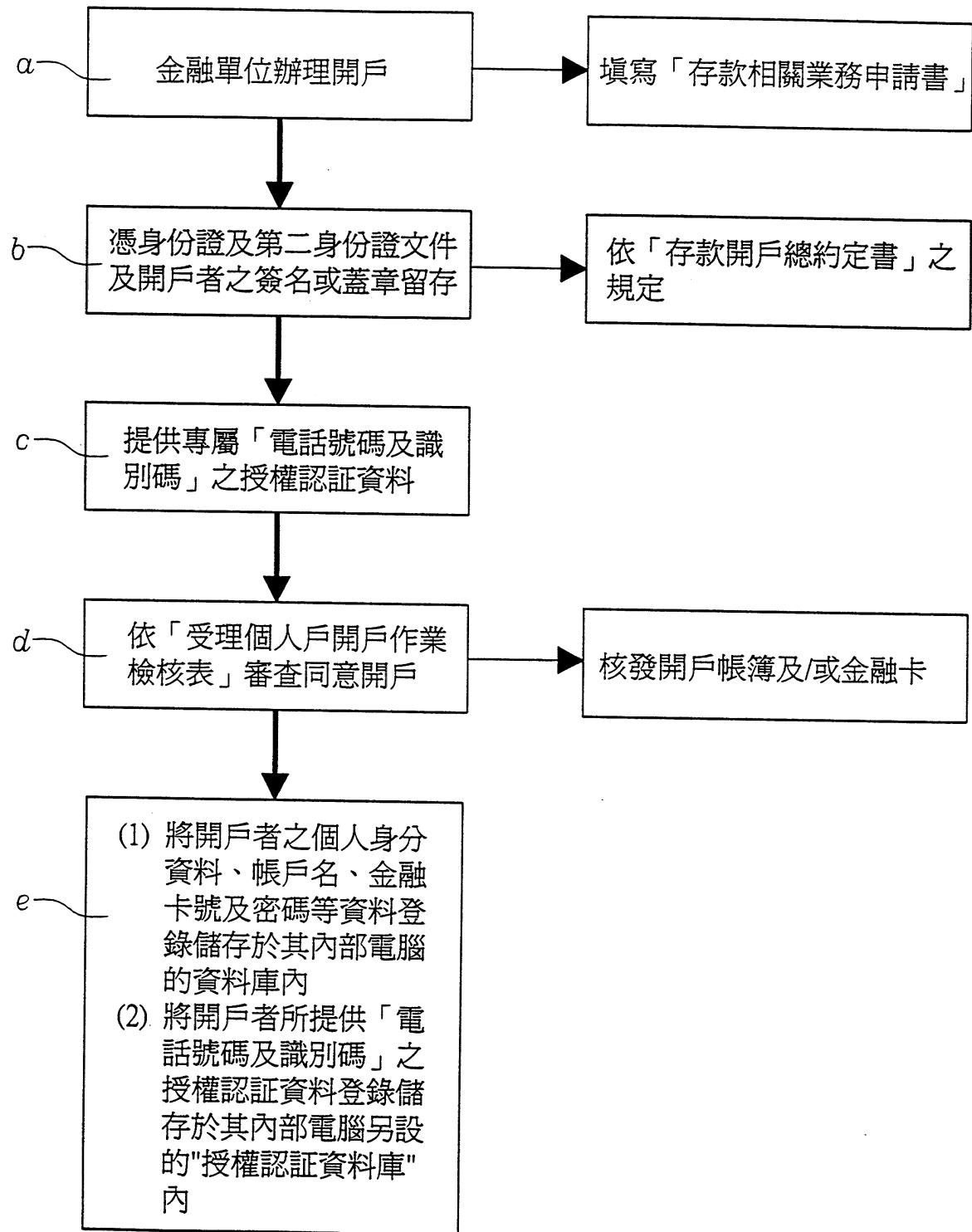
- 8.如申請專利範圍第 6 項所述之「以電話號碼及識別碼做為信用卡使用流程防弊之方法」，其中，該步驟 c 中之「電話號碼」，係可為信用卡持卡人家中或公司的固網電話號碼，或個人行動電話號碼，或是冠有國別碼及區域碼的固網電話號碼，或是冠有國別碼的行動電話號碼者。
- 9.如申請專利範圍第 6 項所述之「以電話號碼及識別碼做為信用卡使用流程防弊之方法」，其中，該步驟 c 中之「識別碼」，係可由任何在電腦中可輸入的文字、數字、符號或其兩者以上之組合所構成，且得由信用卡持卡人在提供登錄儲存後，依循信用卡發卡銀行所規範之流程或方式，而可主動進行做隨時任意之修改或變更者。
- 10.如申請專利範圍第 6 項所述之「以電話號碼及識別碼做為信用卡使用流程防弊之方法」，其中，步驟 e 中該信用卡持卡人所提供之「電話號碼及識別碼」授權認證資料，更可登錄儲存於非屬該信用卡發卡銀行內部電腦系統所操控之”外部授權認證資料庫”中者。

200823807

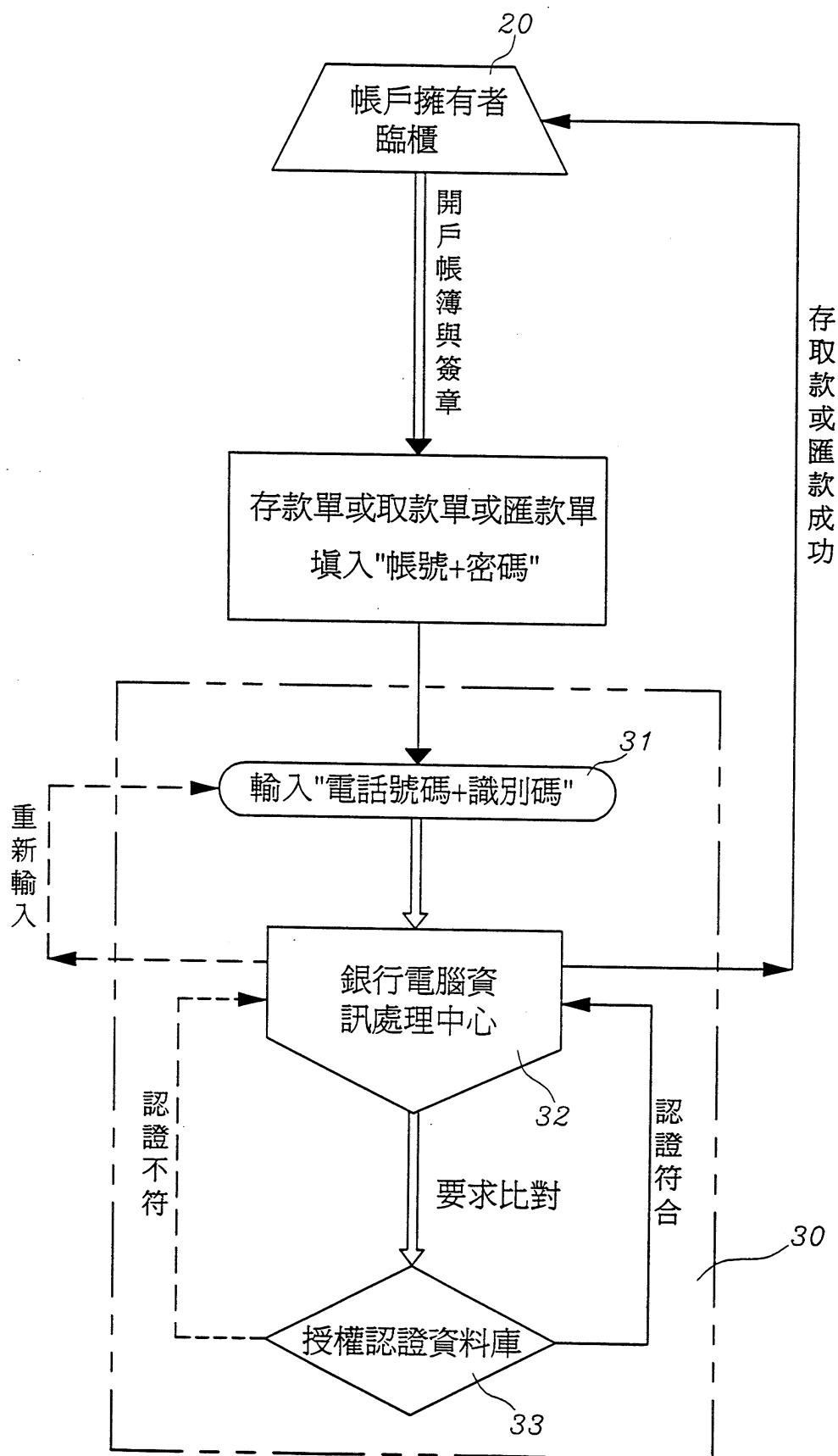
十一、圖式：



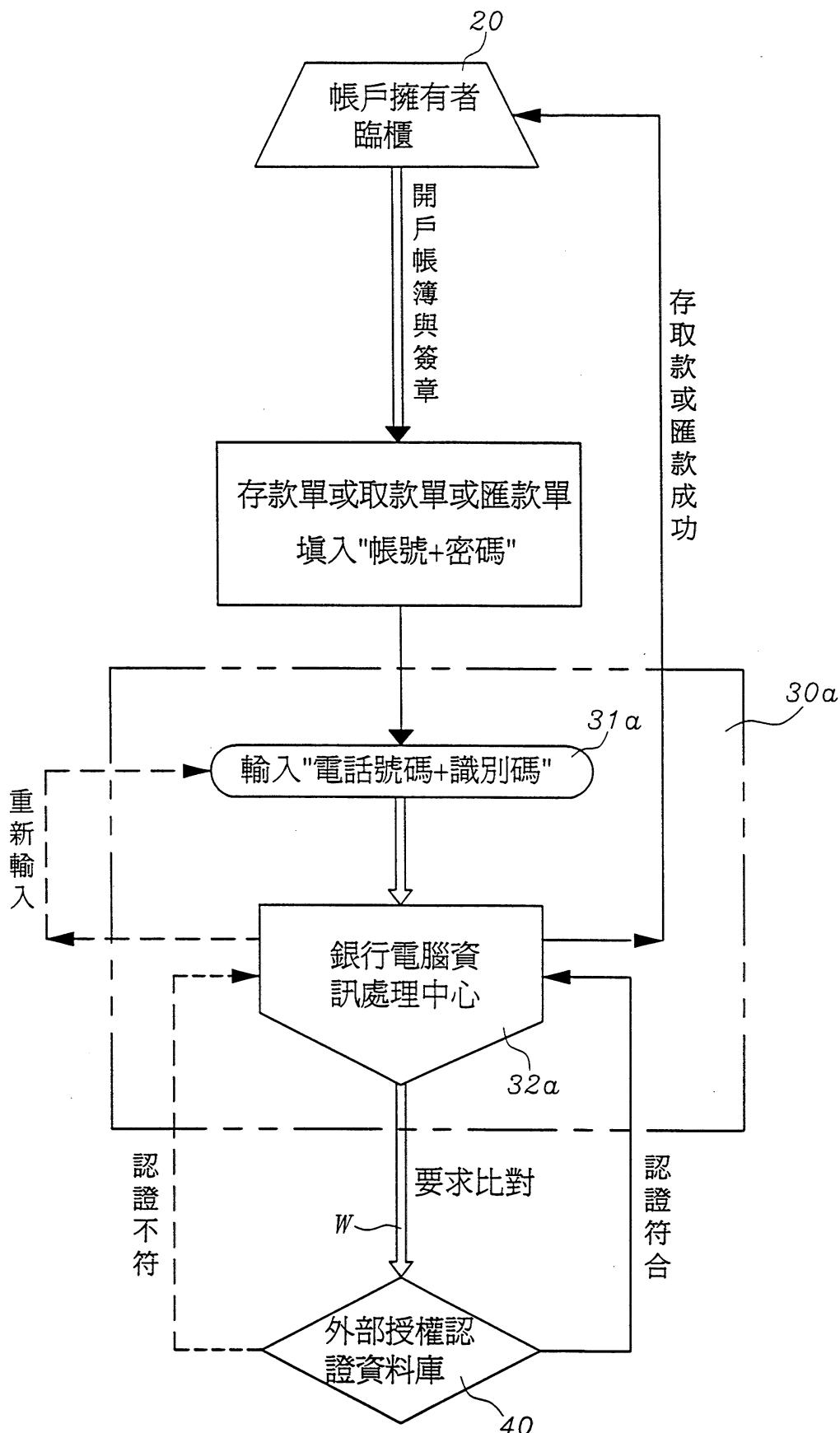
第一圖



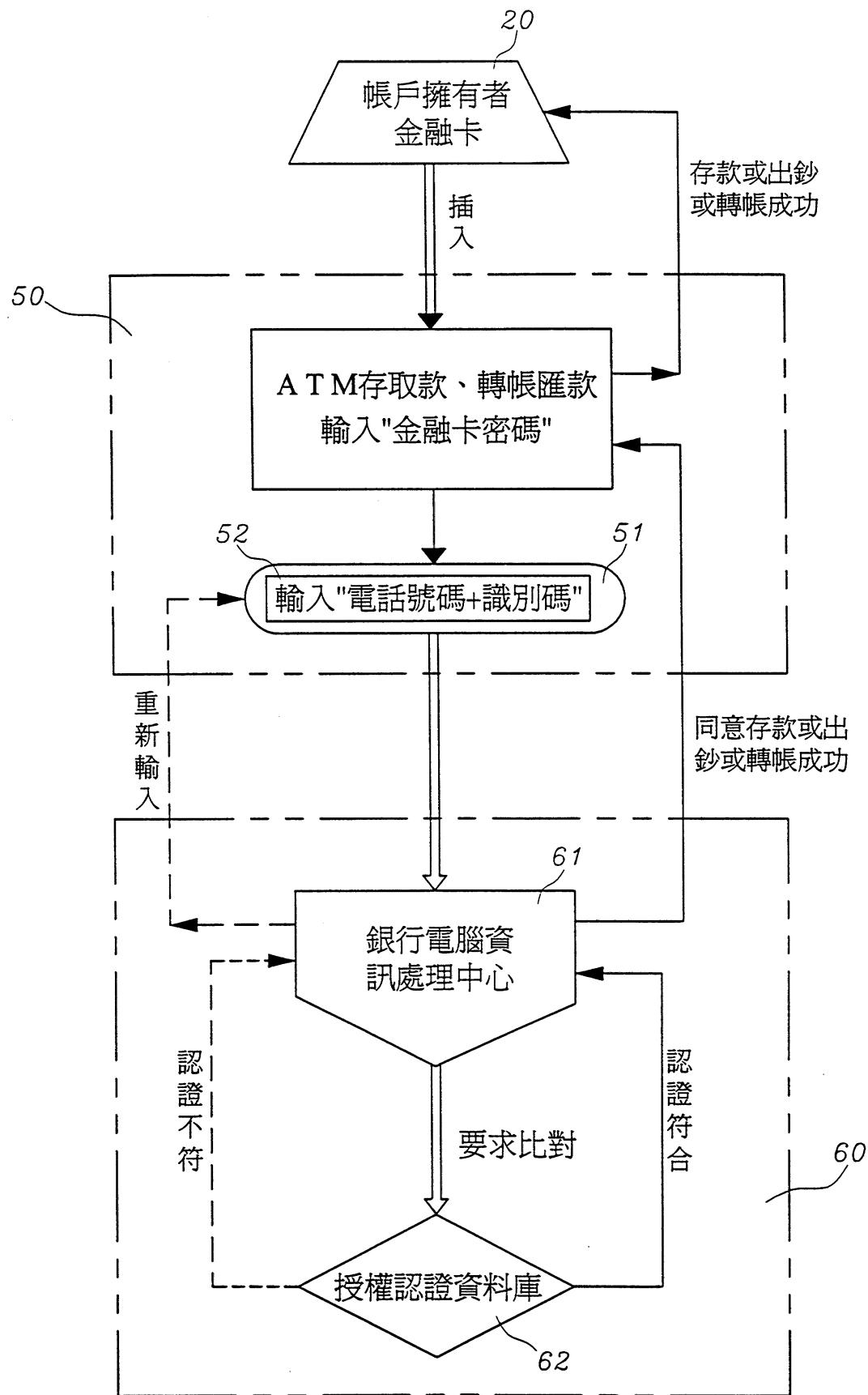
第二圖



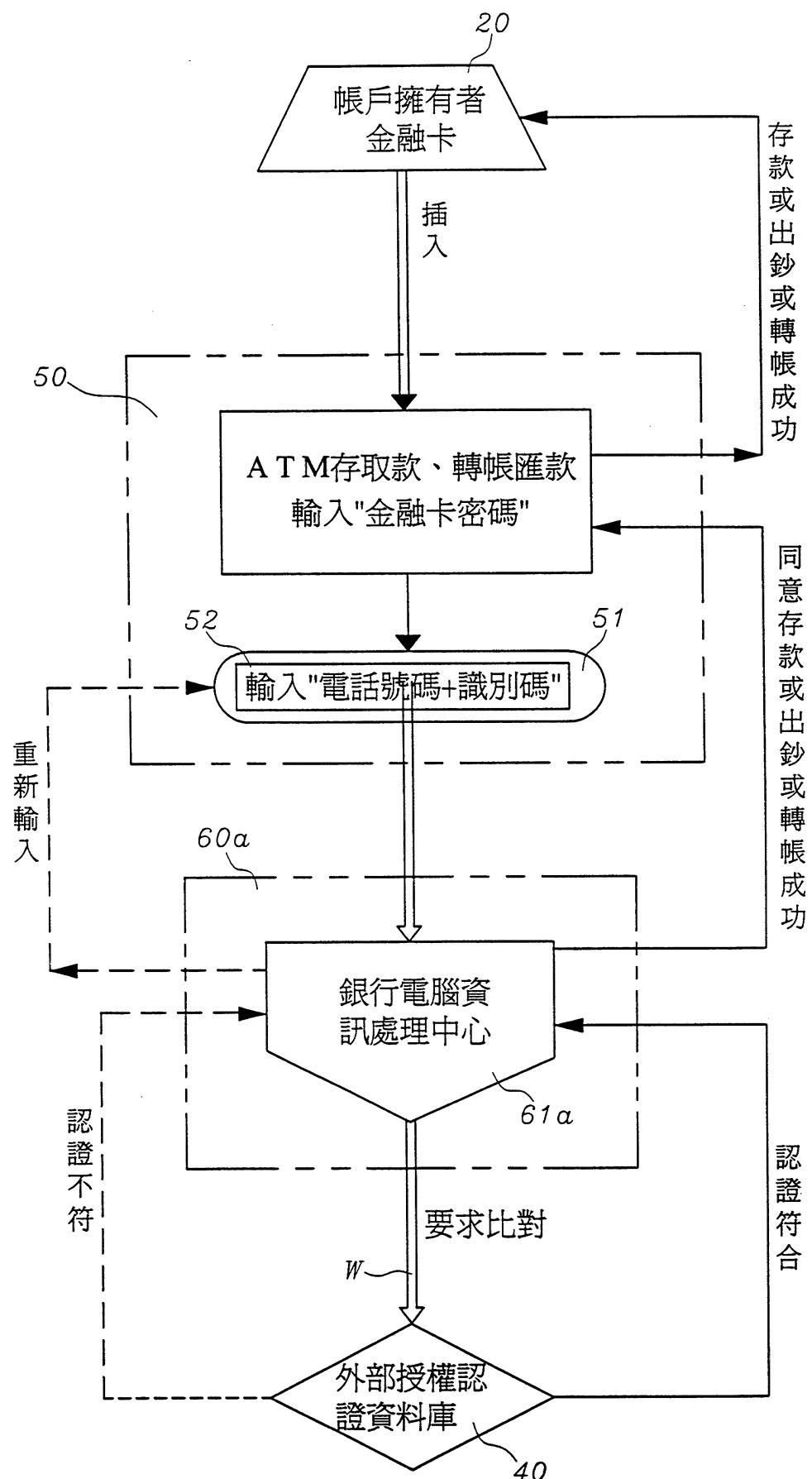
第三圖



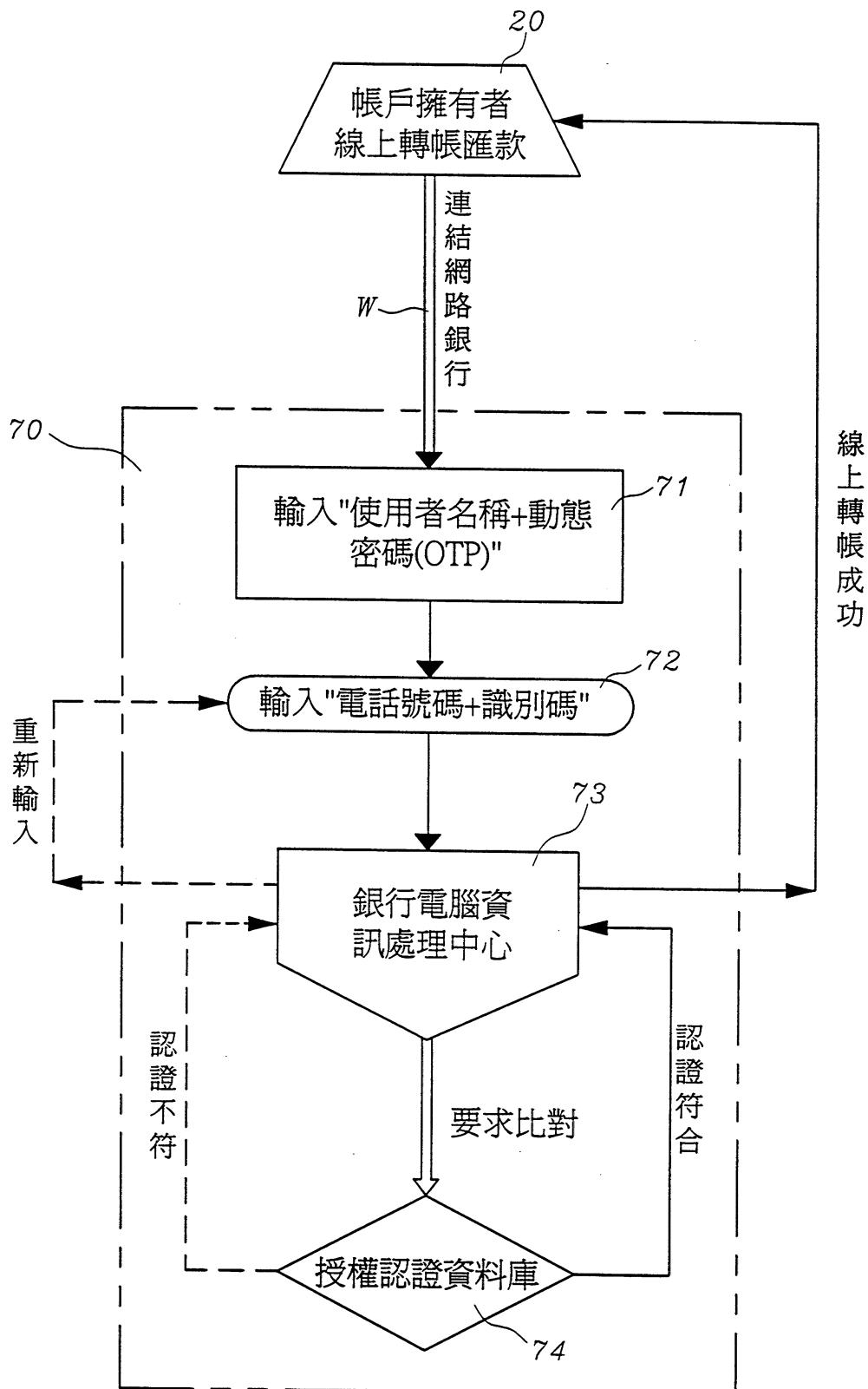
第四圖



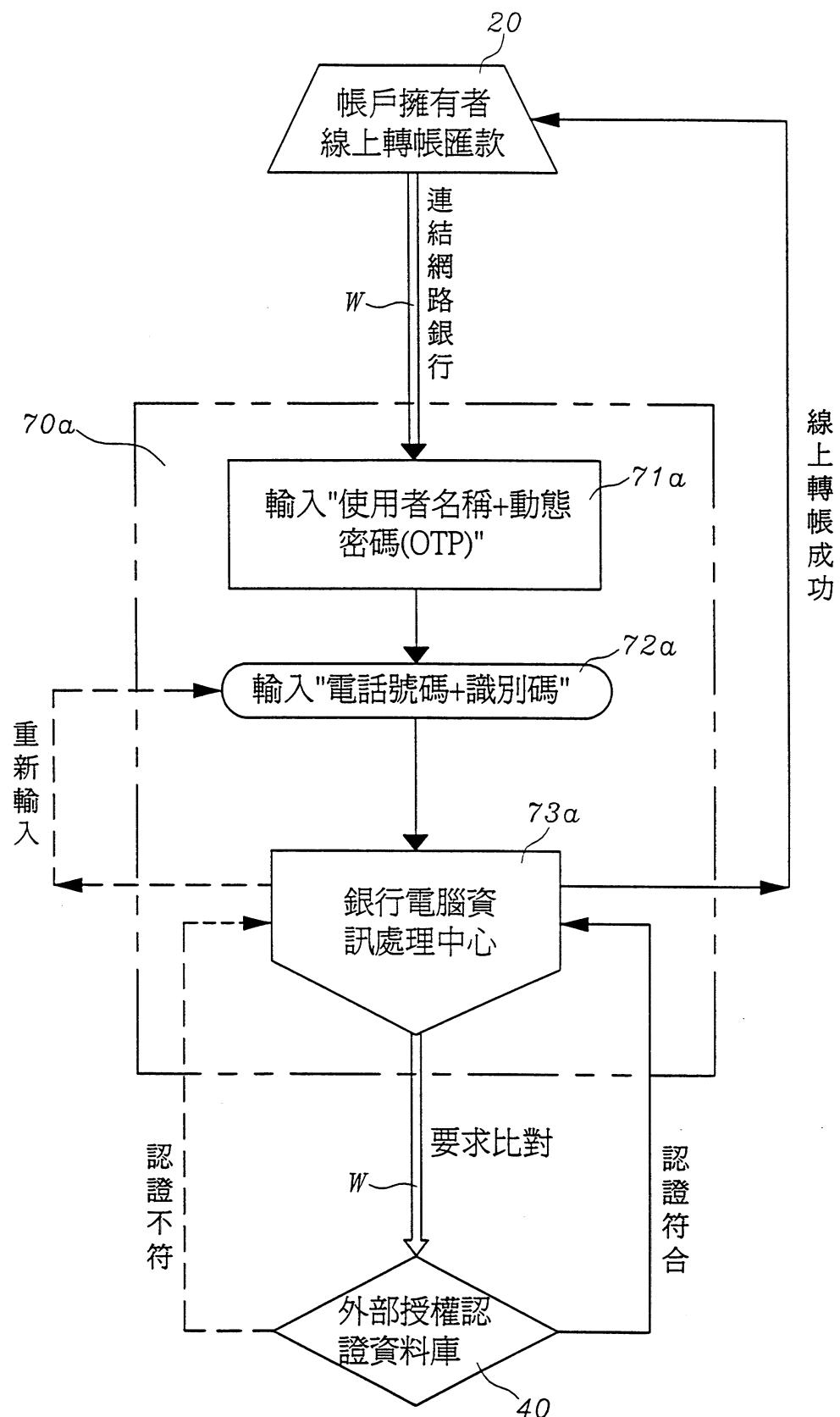
第五圖



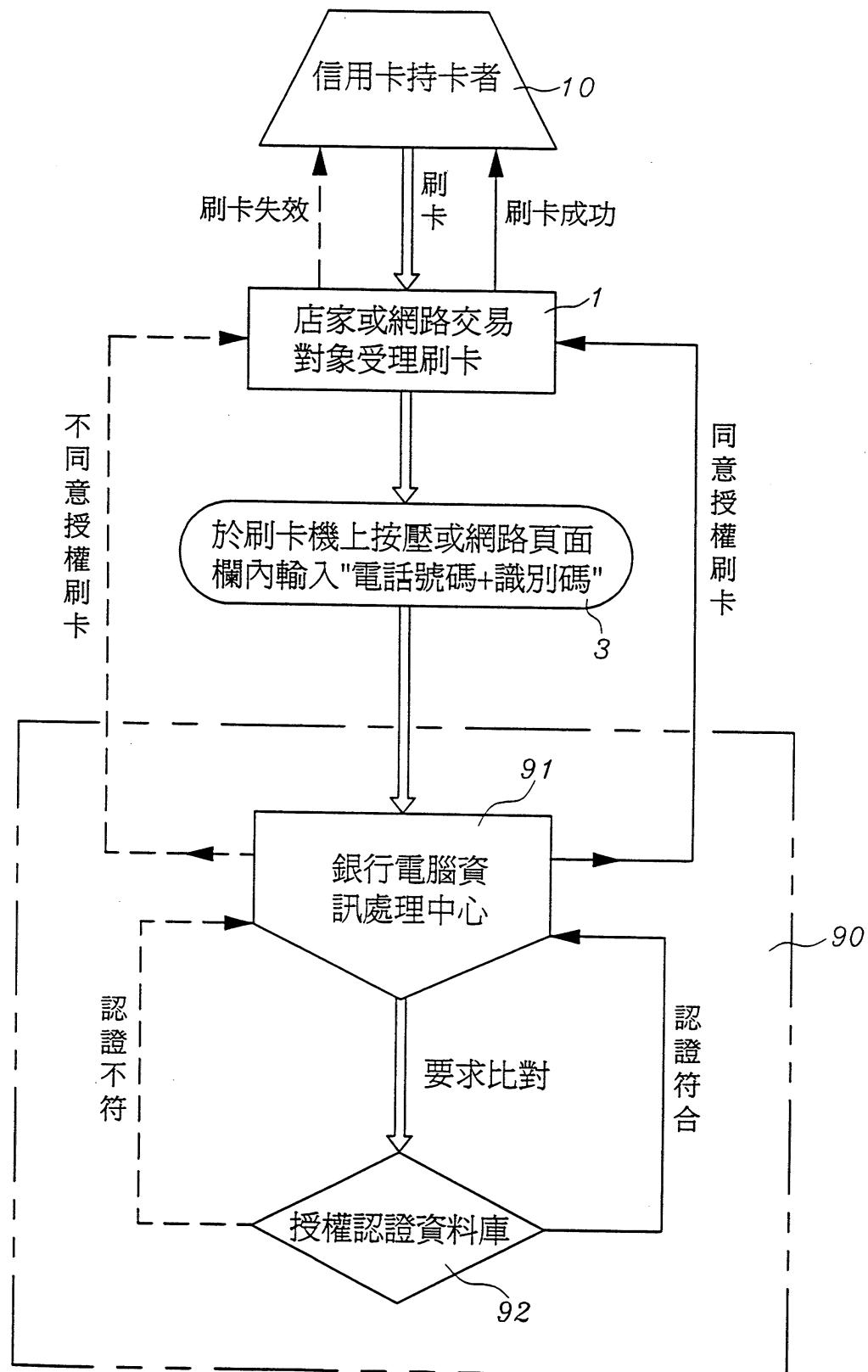
第六圖



第七圖



第八圖



第十圖

七、指定代表圖：

(一)本案指定代表圖為：第（二）圖。

(二)本代表圖之元件符號簡單說明：

本案的代表圖並無元件的代表符號，所以本案的代表圖中並無元件代表符號的簡單說明，合先敘明。

● 八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：