

電腦詐欺與不正方法*

許 恒 達**

要 目

壹、導 論	二、自動收費設備詐欺罪
貳、電腦詐欺的源起、立法及困境	(一)收費設備的交易結構
一、電腦操縱與電腦詐欺	(二)收費設備的定義及範圍
二、我國電腦詐欺罪的立法與其適用	(三)不正方法的認定
(一)自動收費設備詐欺罪	三、付款設備詐欺罪
(二)自動付款設備詐欺罪	(一)付款設備的交易結構
(三)不正使用電腦詐欺罪	(二)解釋「不正方法」的理論選擇
三、電腦詐欺罪的解釋疑義	(三)付款設備的定義及範圍
(一)罪質定位不清	(四)檢討具體案例
(二)電腦與資料處理特點不明	四、不正使用電腦詐欺罪
(三)法定犯行概念模糊	(一)變更財產權紀錄的交易結構？
四、小 結	(二)構成要件的解釋與因果連結
參、重新解釋電腦詐欺罪	(三)類型化的觀察取徑
一、解套進路的探尋	肆、結 論

DOI : 10.3966/102398202015030140002

* 本文承蒙兩位匿名審查人提供極具參考價值的意見，大大充實本文的可讀性，筆者敬致謝忱，惟文責仍由筆者自負。

** 政治大學法學院副教授，德國法蘭克福大學法學博士。

投稿日期：一〇二年五月十五日；接受刊登日期：一〇二年七月十二日

責任校對：阮玉婷

摘 要

本文討論一九九七年刑法新增的電腦詐欺三則罪名（第三三九條之一、之二及之三），這些罪名以自動設備或電腦系統作為侵害客體，從而取得不法利益，然應如何認定其成罪界限，尤其是如何判定成罪的構成要件行為「不正方法」，學說與實務往往面臨困擾。本文認為，要認定不正方法的實質內容，應觀察條文預設的交易結構，不同交易結構下的不正方法即有不同，分述如下：

一、第三三九條之一的交易結構是「財產給付／對待給付」，故僅當使用者的給付不具財產性時，才算是不正方法；

二、第三三九條之二的交易結構是「人別憑證／對待給付」，只要使用者出示形式正確，卻未得本人授權的憑證，即屬不正方法；

三、第三三九條之三欠缺上述交易結構，但至少規定了「輸入虛偽資料及不正指令」等犯行，不正方法即為上述行為，至於成罪重心，則是個別要素因果關聯性的判斷。

關鍵詞：電腦詐欺、交易結構、不正方法、電腦資料處理、收費設備、付款設備

壹、導 論

一九九七年立法院通過刑法修正案，開啟分則各罪章的修正列車，自此截至二〇〇五年的刑法總則大修正為止，我國刑法有了完全不同於二十世紀初剛立法時的面貌。一九九七年修正之初的變動，主要與電腦犯罪新立法有關，其中最值得關注的部分，無非是在詐欺罪主要條文第三三九條之後，另外新增了第三三九條之一的自動收費設備詐欺罪、第三三九條之二的自動付款設備詐欺罪及第三三九條之三的不正使用電腦詐欺罪，這三個條文全部置於詐欺罪章，理論上看來，可以說擴大了詐欺罪章適用範圍。

當時立法者也針對個別條文的增訂，提出了具體理由：「目前社會自動付款或收費設備之應用，日益普遍，如以不正方法由此種設備取得他人之物或得財產上不法利益，不特有損業者權益，而且破壞社會秩序，有加處罰之必要」（第三三九條之一立法理由）；「利用電腦或其相關設備犯詐欺罪，為常見之電腦犯罪型態，為適應社會發展需要，爰參酌日本現行刑法第二百四十六條之二立法例增列處罰專條規定」（第三三九條之二立法理由）；「以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，為電腦犯罪型態，為適應社會發展需要，爰增列處罰專條」（第三三九條之三立法理由）。

從立法理由不難看出立法反應的社會期待，當時電腦、網路及自動服務設備逐漸普及，社會上出現許多相關犯罪，為了滿足社會需求，刑法必須有所反應，立法者修法處罰透過電腦或相類設備而詐取他人財物或財產利益的行為。雖然新修法實現了透過刑罰捍衛新秩序的希望，但是否三個電腦詐欺的條文能夠真正解決問題，其

實不無疑問¹，尤其在當時修法之後，許多學者針對修法成果提出擲地有聲的批評²，新增三個電腦詐欺條文能否符合立法者的管制企圖更是廣受質疑³。而在一九九七年增修之後，立法院又於二〇一四年再次修正這三則條文，只不過這次修正限於增加罰金刑，同時在各條二項後納入未遂犯處罰，但基本的規範體例則沒有變動。

無論如何，三個位列詐欺罪之後的罪名，自一九九七年出現於刑法典後雖然有若干修正，但其本質性的結構則未曾改變，而為了解決實務解釋的需求我國實務上也發展出具有實踐意義的判斷標準以操作電腦詐欺三則罪名。本文寫作初衷，即是在立法增訂十餘年後，再一次從刑法學理角度思考相關條文的妥適性，礙於條文文字相當簡約，無法直接從文義解釋中得到具有說服力的思考成果，因此筆者將引入學理觀點、實務見解及體系結構等三個面向，設法詮釋法條的規範重點，並從三個不同觀察基礎回顧、檢討這十五年來有關電腦詐欺規範界限的變動。

以下討論，將先說明第三三九條之一、之二及之三在刑法財產犯罪中的功能及定位，筆者將於討論中演繹出一個初步看法，此即

¹ 雖然第339條之1、之2及之3等三則條文，不必然涉及「電腦處理資料」的特色，嚴格而論不能統稱為電腦詐欺，尤其是條文規範初衷與電腦處理資料特性有相當差異的第339條之1，但一般學理上為求行文簡捷，仍以電腦詐欺（Computerbetrug）稱呼這三則條文，參見蔡蕙芳，電腦詐欺行為之刑法規範，東海大學法學研究，18期，頁28，2003年6月。（「1997年10月6日起，與電腦詐欺行為有關之刑法規範，刑法第339條之1、刑法第339條之2與刑法第339條之3開始施行」）。

² 黃榮堅，刑法增修後的電腦犯罪問題，載：刑罰的概限，頁314-324，1999年4月；李茂生，資本、資訊與電腦犯罪，載：權力、主體與刑事法，頁206-233，1998年5月；黃常仁，「困頓新法」——論刑法第三三九條之一、第三三九條之二與第三三九條之三，台灣本土法學雜誌，27期，頁1-12，2001年10月。

³ 從資本主義角度分析本次修正的專論，參考李茂生，同前註，頁233-294。

在解釋時，必須先確認三則條文法定構成要件行為，才能具體限定處罰界限，在第三三九條之一及之二，該法定犯行是以「不正方法」描述，而第三三九條之三的法定犯行除了「不正方法」之外，另外又涉及「輸入虛偽資料或不正指令」，如何解釋個別條文的不正方法及相關規定，勢必左右電腦詐欺的成罪邊界。而為了探討個別條文的行為定性，筆者將於接續的論文中觀察學說及實務見解，並從法益、條文預期的交易結構及構成要件要素的關聯性等思考脈絡中，開展出一條有別於現有見解的看法，為了有效證成筆者個人見解，本文也將設法分析具有代表性的實務意見。

貳、電腦詐欺的源起、立法及困境

一、電腦操縱與電腦詐欺

電腦犯罪立法約在一九八〇年代於歐美各國出現，最初的立法規制架構是從「使用電腦侵害財產」的角度設計，這一點特別可從影響我國刑事立法相當深遠的德國學者Ulrich Sieber見解中看得出來⁴。

在出版於一九七七年的專論「電腦犯罪與刑法」（Computerkriminalität und Strafrecht）中，Sieber先強調電腦犯罪主要涉及濫用（Missbrauch）電磁資料運算功能（elektronische Datenverarbeitung, EDV），與刑法相關的面向有三，包括個別人民的資料保

⁴ Sieber, Computerkriminalität und Strafrecht, 2. Aufl., 1980. 我國早期研究電腦犯罪的專論，幾乎都參考了德國學者Sieber的看法，這一點尤其可從早期我國最重要的論文之一：林山田教授於1984年的論述中看得出來，參見林山田，電腦犯罪之研究，載：刑事法論叢（一），頁135-146，1987年5月。較早期文獻中亦有不同的分類方式，參考蔡蕙芳，電腦犯罪與刑事立法的課題，月旦法學雜誌，0期（試刊號），頁103-107，1995年4月。

護、國家的資料保護以及財產犯罪⁵。而對於電腦與財產犯罪關係，Sieber進一步區別出三種利用電腦處理資料功能干擾財產的犯罪行為：電腦操縱（*Computermanipulation*）、電腦毀損（*Computersabotage*）、電腦間諜（*Computerspionage*）。

電腦操縱指的是行為人無權變更電磁紀錄內容，進而實現財產權的非法移轉；電腦毀損專指行為人無權毀損電腦硬碟內部儲存的資料；電腦間諜則涉及無權取得他人電磁紀錄內容的行為⁶。除了三類最主要與電腦相關的財產犯罪之外，Sieber又提出一個當時較少受關注的亞型「時間竊盜」（*Zeitdiebstahl*），時間竊盜專指行為人無權使用他人電腦，由於行為人未取得他人財產，只是無權使用而已，如何管制這一類的行為即有討論空間⁷。

至於使用電腦而涉及詐欺罪的情況，依Sieber看法，屬於電腦操縱的次類型⁸，不過刑罰管制的真正困難在於，詐欺罪的成立以相對人因詐術而陷於錯誤為前提，然而電腦依據程式、指令而運作，本身不會陷於錯誤，如何處罰無權變更他人電腦內部資料，進而「詐騙電腦」取得財產的行為，在解釋上非常不容易，其中若干案例也無法構成傳統的詐欺罪⁹。此外，針對已於一九三五年就已經訂於德國刑法第二六五a條的巧取財產給付罪（*Erschleichen von Leistungen*）¹⁰，Sieber認為在電腦時代開始後，若行為人透過電腦

⁵ Sieber, aaO., S. 23-30.

⁶ Sieber, aaO. (Fn. 4), S. 39f.

⁷ Sieber, aaO. (Fn. 4), S. 123f.

⁸ Sieber, aaO. (Fn. 4), S. 200.

⁹ Sieber, aaO. (Fn. 4), S. 234ff.

¹⁰ 本罪第1項規定：「意圖脫免給付，而詐騙取得自動設備提供之服務、公用目的之電信服務、交通工具之服務，或參與活動、進入設施者，若未受其他罪更重之處罰，處一年以下有期徒刑或罰金」。（*Wer die Leistung eines Automaten oder eines öffentlichen Zwecken dienenden Telekommunikationsnetzes,*

操縱而非法變更他人資料，再詐取給付時，可能會超出條文本身的規制範疇，形成處罰上的漏洞¹¹。

縱觀Sieber對電腦犯罪以及電腦詐欺的研究，可以注意到兩個特點：第一，Sieber從處理電磁資料的角度開展其電腦犯罪論述，其重點在於透過濫用電腦自動運算功能，侵犯他人的既有財產犯罪，不過Sieber並未將電腦系統獨立於傳統法益之外而構成新的法益；第二，Sieber將透過電腦進行的詐欺行為，歸類為電腦操縱項下的一種，其重心是行為人虛偽變更既有儲存資料，再實施財產移轉行為，損害他人財產，只不過依據當時德國刑法詐欺罪及詐得給付罪規定，這些行為不必然能夠受到合理制裁，為了妥適解決問題，增訂相關規定似乎成為唯一解決之道¹²。

很快地，德國立法者對電腦操縱的詐欺行為有了回應。一九八四年德國新增訂刑法第二六三a條電腦詐欺罪¹³，該條在結構上被

die Beförderung durch ein Verkehrsmittel oder den Zutritt zu einer Veranstaltung oder einer Einrichtung in der Absicht erschleicht, das Entgelt nicht zu entrichten, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.)

¹¹ Sieber, aaO. (Fn. 4), S. 238. Sieber的著作後來於1980年再版，第2版中Sieber除了增加討論若干專論出版後的學者迴響之外（Vgl. Sieber, aaO. (Fn. 4), S. 2/2 ff.），另外針對1980年德國刑法修正草案建議增訂的電腦詐欺罪（Computerbetrug）、1979年美國的電腦犯罪立法有進一步的討論。

¹² 對Sieber見解的檢討，vgl. Lenckner, Computerkriminalität und Vermögensdelikte, 1981, S. 13-21.

¹³ 德國立法過程，vgl. Lackner, Zum Stellenwert der Gesetzestechnik, in: Herbert Tröndle-FS, 1989, S. 43ff.; Mitsch, Strafrecht Besonderer Teil 2, Teilband 2, 2001, § 3 Rn. 4-5; Kraatz, Der Computerbetrug (§ 263a StGB), Jura 2010, S. 36f. 而德國電腦詐欺罪名與歐盟指令間的關係，另參考Duttge, Vorbereitung eines Computerbetrug: Auf dem Weg zu einem „Grenzlosen“ Strafrecht, in: Ulrich Weber-FS, 2004, S. 288ff.

當作是詐欺行為的接續規範，屬於特別型詐欺，條文中詳盡規範透過電腦操縱而實施的財產詐取行為，並限定成罪的四種手法：(一)編製不正確程式；(二)使用不正確或不完整之資料；(三)無權使用資料，及(四)其他無權影響資料處理過程的行為。若行為人出於為自己或第三人不法獲取財產的意圖，實施上述行為任何一種，影響電腦處理資料的正確性，進而損害他人財產利益時，就可處五年以下有期徒刑¹⁴。

雖然德國新規定的電腦詐欺罪名仍有許多解釋問題，但至少一九八四年的新增訂立法中，已經以電腦處理資料的特質為中心，以侵害財產利益為保護對象，積極展開刑法規制。相對於此，我國法一直欠缺類似規定，不僅欠缺與現代電腦運算不必然相關聯的詐領給付罪，也缺乏領先性的電腦詐欺罪名，一直等到一九九七年的立法時才完全改變。

二、我國電腦詐欺罪的立法與其適用

一九九七年立法院正式通過刑法修正案，在詐欺罪之後增訂三個與自動設備及電腦相關的罪名，以下就簡要說明這三個罪名的具體內容及實務解釋方向¹⁵。

¹⁴ 有關德國立法參考Rengier, *Strafrecht Besonderer Teilband 1*, 11. Aufl., 2009, § 14 Rn. 7ff.; *Arzt/Weber/Heinrich/Hilgendorf*, *Strafrecht Besonderer Teil*, 2. Aufl., 2009, § 21 Rn. 32; *Maurach/Schroeder/Maiwald*, *Strafrecht Besonderer Teil*, Bd. 1, 10. Aufl., 2009, § 41 Rn. 230-235. 討論德國法的重要中文文獻，參考蔡蕙芳，同註1，頁29-50。

¹⁵ 相關立法過程，參考林山田，評詐欺罪章中之新增三罪，*月旦法學雜誌*，49期，頁85-89，1999年6月。

(一)自動收費設備詐欺罪

先談刑法第三三九條之一，該條專門規範對自動收費設備的詐欺行為，條文結構也仿造詐欺罪體例，分別依行為人取得財物或財產利益而分列為第一項及第二項，此外也規範不法所有意圖的特殊主觀要件，成罪要件則以行為人實施「不正方法」，從收費設備取得他人財物或財產利益為必要，刑度選擇上，立法者似乎將本罪與投幣販賣機或投幣按摩椅等價值較低的損害形態相互連結，直接規範刑事責任為一年以下有期徒刑的較低度制裁。

立法當時對於本罪的想像，應該是局限機械式且以物理機制感應效果作出給付的機器，例如常見的飲料自動販賣機，或是公共場所投入硬幣就會自動服務的按摩椅¹⁶。這些機會會先設定若干物理感應程式，比如測量十元硬幣的重量、大小的程式，藉以篩選消費者提出的價金是否屬實，不過，也因為物理感應程序只能測量硬幣的物理效能，無法絕對地確認該硬幣是否為真，倘若行為人投入相等大小、重量的假幣，依機器程式仍將判定已得到金錢給付，故可移轉財物或服務予行為人，但實際上行為人根本未提出給付，就已取得飲料或服務，此時即可成立本罪¹⁷。

除了上述投假幣以兌換販賣機飲料或按摩椅服務的情況外，實務比較常出現的案例，還包括投入假幣換真幣的行為，我國實務上即有判決認為，當行為人對咖啡機自動販賣機投入形狀、大小與真幣近似的代幣，再按退幣鈕而取得真幣的行為，屬於本罪所謂的不正方法¹⁸。

另一類常見案例，則涉及干擾收費設備的機械功能，例如行為

¹⁶ 參考林山田，刑法各罪論（上），頁469，2006年11月，5版。

¹⁷ 同前註，頁470。

¹⁸ 臺灣高等法院臺中分院90年度上易字第2268號判決。

人使用自製工具，伸入夾娃娃機的投幣口內，干擾機台內部的感應器，使其誤判行為人已經投入硬幣，而讓行為人在未付款情況下，多次提供夾娃娃的遊戲服務長達一小時，而行為人也夾得若干娃娃¹⁹；又例如以自製工具，干擾計數器而使機器誤判投幣金額，免費自販賣機內取得飲料²⁰。法院均認為這一類干擾機械式計數功能的行為，屬於不正方法而成立本罪。

隨著網路技術的發達，純粹機械式的收費設備愈來愈少，以連線方式判斷有無提供給付的收費機制愈益常見，一九九七年的立法只預想到機械型收費機制，能否將本條適用至電腦連線型的收費機制，不無疑問²¹。對此我國實務採取肯定見解，實務近期有判決認為，行為人拾獲他人遺失的信用卡，在無人服務的加油站，使用信用卡自助加油（僅須過卡而無須簽名），法院認為此時應成立第三三九條之一犯罪²²；又例如行為人竊得被害人所有的信用卡後，因信用卡具有悠遊卡功能，一旦悠遊卡內儲值用完後，會直接從信用卡內扣款加值，行為人消費完原有餘額後，又持之於悠遊卡特約商店內消費，致使悠遊卡後端設備自動加值，再以之消費，行為人遂未付費即獲得商品及服務，法院亦認為成立第三三九條之一罪名²³；又例如行為人以他人信用卡，盜打不需要簽名的國際電話，

19 臺灣高等法院90年度上易字第2613號判決。

20 臺灣高等法院98年度上易字第2418號判決。

21 採肯定說者，見甘添貴，刑法各論（上），頁329，2009年6月；盧映潔，刑法分則新論，頁689，2012年9月，5版。

22 臺灣高等法院98年度訴字第1579號判決。

23 臺灣高等法院100年度上易字第1577號判決。該判決的內文殊值特別介紹：「告訴人陳○○之上開國泰世華銀行悠遊聯名信用卡，係信用卡兼具悠遊卡、悠遊錢包功能，在儲值於悠遊卡、悠遊錢包內之款項低於一定金額或不足以支付當次消費金額時，可經由交易設備自持卡人信用卡可動用額度中，將一定之金錢價值撥付於悠遊卡公司進行『悠遊卡』或『悠遊錢包』儲值，

法院也認為構成第三三九條之一罪名²⁴。

最後，倘若行為人先拾得他人遺失的身分證，再以之冒名向電信業者申請門號，之後再使用該門號通訊，但因屬冒名申請²⁵，電信業者無法追討資費，針對這類事例後階段撥打冒名申請門號的行為，法院則認為：「電話之使用，必須付費，本質上即為『收費設備』之一種，公共場所投幣或插卡式之公用電話，係屬『收費設備』固無疑義，私人所申請之行動電話，實際上亦係依使用時間計算之收費設備，與公用電話並無不同，二者所差異者，僅在費用之收取方式（私人電話按月結帳，公用電話按次結帳），而此項差異，並不影響行動電話作為收費設備之屬性[……]本件被告甲冒名申請行動電話撥打行為，應屬刑法第三百三十九條之一第二項以不正方法由收費設備得財產上不法利益行為」²⁶。

即所謂自動加值，是在儲值於悠遊卡、悠遊錢包內之款項低於一定金額或不足以支付當次消費金額時，特約機構悠遊卡端末設備即會自動加值，此時被告並無何施用詐術之行為，不過係收費設備誤認被告為持卡人本人而予以自動加值，被告亦因而獲得持該悠遊聯名信用卡於特約商店消費時無需付費之不法利益。且因悠遊聯名信用卡不限於本人始可持卡消費，任何人持卡輕觸悠遊卡端末設備上感應區，即可感應扣款，等同現金而用以支付商品及服務對價，此時悠遊卡特約商店亦無因持卡人非本人而陷於錯誤之情事。是被告與另案被告周○○接續於上開時間、地點，持告訴人陳○○之國泰世華銀行悠遊聯名信用卡消費，並因該悠遊聯名信用卡內之款項低於新臺幣100元不足以支付消費金額，經便利商店之悠遊卡端末設備自動加值，使被告及另案被告周○○因而獲得持該悠遊聯名信用卡小額消費而無需付費之財產上不法利益，應係犯刑法第339條之1第2項、第1項之以不正方法由收費設備得財產上不法之利益罪，並無違誤」。

²⁴ 臺灣高等法院93年度上易字第769號判決。

²⁵ 冒名申請應考慮偽造文書刑責，但申請時只要由行為人自行繳納申請費用，仍不成立任何電腦詐欺罪名，此一見解亦為法院所贊同，參考臺灣高等法院89年度上訴字第3945號判決。

²⁶ 臺灣高等法院89年度上訴字第3945號判決。

(二)自動付款設備詐欺罪

其次是付款設備的第三三九條之二。就條文文字而言，第三三九條之二與第三三九條之一幾乎完全相同，僅侵奪對象有其差異，第三三九條之二攻擊付款設備，從立法者的規制企圖來觀察，付款設備顯然指涉在立法當時相當普遍的自動櫃員機（automated teller machine, ATM），只要行為人出於不法所有意圖，從自動櫃員機中不正取得他人財物（第一項）或取得財產利益（第二項），即構成第三三九條之二犯罪²⁷。此外，或許立法者認為自動櫃員機已經非常普遍，從中無權取得他人財產不算是太過分的事情，所以未依財產犯罪的五年有期徒刑一般行情設計本罪的刑度，最高刑度反而調降到三年的有期徒刑。

依我國實務見解，第三三九條之二所稱的不正方法，指的是一切不正當的手段，亦即，只要行為人不合法地取得卡片及密碼，或使用卡片取款或轉帳本身不合法，都算是不正方法，實務曾有見解指出：「刑法第339條之2第1項之罪，其所謂『不正方法』，係泛指一切不正當之方法而言，並不以施用詐術為限，例如以強暴、脅迫、詐欺、竊盜或侵占等方式取得他人之提款卡及密碼，再冒充本人由自動提款設備取得他人財物，或以偽造他人之提款卡由自動付款設備取得他人財物等等，均屬之」²⁸。

上述觀點是我國實務的判斷原則，若再考察判決內容，大致上可以將不正方法分為兩類。第一類涉及外部侵奪型的前行為，此類行為人與被害人間並無任何關係，行為人先以不法手段取得或產生被害人的卡片、密碼，之後再前往自動櫃員機領取他人帳戶內的餘

²⁷ 參見林山田，同註16，頁471；甘添貴，同註21，頁333；盧映潔，同註21，頁691-692。

²⁸ 參見臺灣高等法院高雄分院98年度上訴字第125號判決。

額²⁹。最明確適例是竊盜他人卡片後的提款行為，法院明確認為嗣後的取款行為是本條不正方法³⁰；又例如竊取他人信用卡之後，以該信用卡至自動櫃員機預借現金，法院也認為後階段的提款行為屬於不正方法³¹。如果前行為如果涉及併同人身侵害的奪取卡片行為，例如強盜甚至殺害原卡片持有人後，再持原所有人的卡片到ATM取款，亦屬不正方法。這些案例都構成第三三九條之二犯罪³²。

第二種不正方法，則是行為人先獲得被害人內部授權，可以合法使用被害人卡片提款，然而行為人違法逾越被害人所授予的權限，持用卡片從自動櫃員機提出超出授權的款項³³，實務上常見的案例有二，第一種是被害人原先就授權行為人使用提款卡提領特定金額，未料行為人未得被害人同意，擅自使用被害人的卡片提領超額款項，依我國實務見解，該行為屬於不正方法³⁴；另一種則是行

29 甘添貴，同註21，頁332。

30 參考臺灣高等法院臺南分院96年度上易字第238號判決、臺灣高等法院高雄分院88年度上易字第2311號判決。

31 參考臺灣高等法院93年度上更(一)字第517號判決。

32 強盜型的案例如臺灣高等法院高雄分院98年度上訴字第125號判決；若行為人殺害被害人之後，再以該被害人身上的信用卡至自動櫃員機預借現金的案例，如臺灣高等法院臺中分院91年度上重更(二)字第14號判決。

33 盧映潔，同註21，頁691-692。

34 參考臺北地方法院99年度訴字第230號判決：「乙意圖為自己不法之所有，利用秀國際公司總經理吳○義指示其轉帳員工預借薪資交付金融卡之機會，基於利用自動付款設備詐欺之犯意，於左列時間持該金融卡至不詳地點之自動櫃員機即自動付款設備前，逾越甲之授權，插入該金融卡，鍵入密碼及金額，使自動付款設備辨識系統陷於錯誤，誤認其係有正當權源持卡人，以該不正方法由該自動付款設備轉帳新臺幣（下同）六千三百元至不知情之友人張○之借予其使用之臺北富邦商業銀行忠孝分行帳號第三〇五一六八六一六九五九號帳戶內，而取得屬於付款銀行帳戶內之款項，嗣後乙再予提領花用

為人受被害人委託保管其金融卡，但僅許可保管，未授權提款，行為人卻自行取用卡片領取款項，實務亦認構成不正方法³⁵。

以上案例限於建置於公共場所的實體ATM，本來就是立法時預期規制對象。但隨著網路及電子交易機制逐漸發達，金融交易已經不再限於實體ATM，銀行交易實務上，最初出現的是電話語音轉帳系統。實務曾有案例，詐欺集團先詐得被害人銀行帳戶及語音轉帳密碼，之後就直接打電話到銀行，以電話按鍵輸入資料後淨空其帳戶。該案檢察官原先認為應構成第三三九條之三罪名，但第一審法院卻堅持應成立第三三九條之二罪名。檢察官後來上訴至二審法院，二審法院則認為語音轉帳應屬第三三九條之二的付款設備而駁回上訴³⁶，不過近來實務卻又變更見解，認為語音轉帳不是第三三九條之二，而是第三三九條之三的處罰範圍³⁷。

[……]乙犯非法由自動付款設備取財罪。」

35 參考臺北地方法院100年度訴字第788號判決：「黃○○於九十九年三月至同年八月間，擔任法威實業有限公司（址設臺北市大安區○○○路○段七九號六樓之五，下稱法威公司）之會計人員，負責法威公司之記帳、存款、提款等工作，並保管法威公司之支票、相關款項及法威公司設於玉山商業銀行（下稱玉山銀行）福和分行帳號第○○○○○○○○○○○○號活期儲蓄存款帳戶（下稱玉山銀行帳戶）存摺、金融卡（含密碼）[……]黃○○明知法威公司並未授權其得任意使用上開玉山銀行帳戶內之資金，分別基於意圖為自己不法之所有，以不正方法由自動付款設備取得他人之物之犯意，而各別於如附表三編號一至二十四所示之日期，前往自動提款機前，插入前開所持有之玉山銀行帳戶金融卡，鍵入金融卡密碼，使該自動付款設備辨識系統陷於錯誤，誤認其係有正當權源持卡人，以此不正方法由自動付款設備提領如附表三編號一至二十四所示之金額[……]被告此部份之所為，各係犯刑法第三百三十九條之二第一項之以不正方法由自動付款設備取財罪。」

36 參見高等法院臺中分院97年度上易字第1635號判決。

37 參見高等法院臺中分院100年度上訴字第1784號判決。

近年來技術上更加提升的網路銀行（透過銀行的網頁介面，由存戶設定特定密碼，直接在網路上進行金融交易）及網路ATM（卡片所有人先購買讀卡機，在家透過網路連線至金融機構的伺服器，將提款卡插入讀卡機而與伺服器內建的ATM功能連線，進行金融交易），若干實務見解認為，盜用他人卡片而在網路ATM轉帳的行為人，同樣也算是第三三九條之二的自動付款設備³⁸。不過筆者必須強調，對於這種非實體型的網路銀行機制，實務見解一直搖擺於應適用第三三九條之二或第三三九條之三的規定，目前未絕對統一，但似乎有認定為第三三九條之三的趨勢³⁹。

（三）不正使用電腦詐欺罪

最後是不從侵犯客體規定的第三三九條之三，相對於前兩條，本條規定侵害手法比較接近理想的電腦犯罪⁴⁰。從條文看來，損害因果歷程可分為三個相互接續的進展歷程，行為人必須先以不正方法輸入有問題的資料到電腦中，該資料接著變更了原有財產權利的電磁紀錄儲存內容，最後實現取得財物或獲利結果。至於刑度部分，第三三九條之三是刑度最重的條文，或許立法者考量行為人非法影響的層面較大，所以設定刑度高達七年以下有期徒刑。

雖然第三三九條之三的條文用字較多，但實際解釋結果卻更加模糊，尤其在網路、電信及電子交易日益重要的今天，許多交易活動均以電子資訊方式留下紀錄，只要行為人變更紀錄，進而改變財產分配秩序時，很容易成立本條罪名。實務判決適用本罪時，往往欠缺清楚可循的演繹脈絡，只要與電子儲存財產資料變動有關，即

³⁸ 參考高雄地院98年度審訴字第2251號判決。不過實務也有反對見解，認為應該構成第339條之3的罪名，參見臺灣高等法院98年度上更(一)緝字第6號判決。

³⁹ 此問題的討論，另見第339條之3部分。

⁴⁰ 甘添貴，同註21，頁335-336。

認定成立本罪⁴¹。實務上曾有案例，行為人利用彩券行老闆不注意時，自行輸入選號於投注機，透過連線而列印出指定號碼的彩券，之後再取走系爭彩券，法院認為行為人除構成紙本彩券的竊盜罪，其使用投注機列印出彩券，也構成第三三九條之三第一項罪名⁴²。

即便實務有一些不太明確的見解，我們仍然可以從中找到限定本條解釋的蛛絲馬跡。第三三九條之三揭明行為人必須「不正方法輸入虛偽資料或不正指令」，既然必須輸入資料或指令，行為人當然得先取得接近使用（access）電腦的權限及機會，否則根本不可能輸入資料或指令至電腦系統內，絕大多數儲存財產權資料的電腦系統，都會限定接近使用儲存資料的使用者範圍，只有一開始預先許可的特定人士，才可能直接在單機或透過連線機制，變更儲存在中央伺服器的財產權資料，從接近使用電腦的線索追起，檢視實務判決，筆者認為條文所稱的「不正方法輸入資料或指令」，大致上可分為三種類型。

第一類為「管理權限濫用型」，行為人基於特定的身分關係，對於儲存於伺服器內的電腦資料有管理權限，得合法接近使用系爭儲存資料，行為人卻濫用其權限，故意變更儲存財產權的資料。這類的行為人通常是企業或組織內部成員，對於財產權資料負有管理義務，卻未遵守管理人應盡義務，先利用其權限登入系統後，篡改

⁴¹ 目前實務尚未發生，但可以想像的案例是：行為人在自己的汽車車牌上貼上假的號碼，然後經過高速公路的收費站，由於未裝設e-tag或ETC，收費站會用車牌顯示系統記下車牌，再向該車牌使用者索取過路費。上述案例主要是偽造及行使偽造文書的問題，應該與電腦詐欺無直接關係，卻因車牌顯示系統有涉及財產資料的連線電腦紀錄，直接變身成為第339條之3的罪名。就此部分的討論，參考蔡蕙芳，不正利用電腦取財得利罪，月旦法學教室，46期，頁76-77，2006年8月。

⁴² 參考板橋地院97年度易字第2245號判決。

其內的財產權資料，或利用其權限在系統內植入特定程式，使得關於他人財產權的儲存資料有誤，進而得到財物或利益。

上述案例可說是我國實務適用第三三九條之三規定的大宗型態，我國實務自一九九七年立法迄今，累積了許多案例：例如銀行行員利用150萬以下匯款不須上級審核的管理漏洞，自行登入銀行電腦系統，製作不實匯款紀錄，使其共犯的戶頭餘額增加，法院認為行為人同時構成銀行法的背信罪及第三三九條之三的罪名⁴³；銀行職員利用使用銀行轉帳系統的權限，盜刻存戶印鑑，並製作不實的存款紀錄，該行為同樣構成銀行法的背信罪第三三九條之三罪名⁴⁴；郵局承辦儲匯業務人員，利用其權限將客戶的定存契約提前解約，再將款項提領出來，法院雖未認定被告構成背信，但仍適用刑法第三三六條的業務侵占罪及第三三九條之三處罰行為人⁴⁵；行為人利用在電玩門市擔任業務專員的機會，違法加值原本應繳回公司的作廢會員卡，再將這些會員卡送人或自己使用，使得原公司受到損失⁴⁶；又例如捷運公司員工，在出站時故意不刷悠遊卡，而由其他同事代為銷去其乘車紀錄，從而免於支付車資⁴⁷。以上這些案例的特點，都是行為人因業務管理而有權登入伺服器，竟濫用權限而變更原有財產紀錄，再基於該紀錄而移轉真正的財產，實務見解均認成立第三三九條之三罪名。

第二類則是「侵入電腦型」，這一類的特點在於行為人非有權使用者，但透過無權或越權侵入（unauthorized access）行為，使其

43 臺灣高等法院95年度上易字第914號判決，類似案例另可參考臺灣高等法院95年度上更(一)字第523號判決。

44 臺灣高等法院95年度上訴字第1674號判決。

45 臺灣高等法院101年度上訴字第1106號判決。

46 臺灣高等法院96年度上訴字第3671號判決。

47 臺灣高等法院97年度上更(一)字第518號判決。

得以接近使用儲存資料，然後進一步於主程式中植入木馬程式，或下達特殊指令，致使電腦的主程式系統作出誤判，將他人的財產紀錄移轉至行為人指定的帳戶中，一般而言，本型除了第三三九條之三罪名外，還會同時成立第三五八條的侵入電腦罪，不過由於本型技術門檻較高，一般實務較少出現類似案例。

第三類稱為「資料操縱型」，這一類行為人既非有權使用者，也未侵入主機系統，而是以系統使用者身分依循電腦或網路系統既有的操作機制，輸入不正確資訊，致令系統誤判其資料的正確性，製作錯誤財產權紀錄，最後實現財產關係的不當變動，此類行為人無權使用他人資料，但僅於特定情況下另構成侵入電腦罪名。

舉例而言，實務上為數不少的資料操縱型案例，都與第三三九條之二的處罰界限有關，例如前文提過的語音銀行轉帳，近來判決傾向認定成立第三三九條之三而非之二罪名；也有案例認為網路銀行的交易不是第三三九條之二的付款設備，而是構成第三三九條之三，因此當行為人破解網路銀行的密碼系統，登入網路銀行後，再將他人帳戶金額轉至自己帳戶內，也會成立本罪⁴⁸。不過實務也有判決認為，如果行為人盜用他人金融卡帳號及密碼，登入網路銀行後，將他人銀行帳戶餘額轉給第三人後，再從銀行領出款項，法院認為此時同時構成第三五八條、第三五九條的妨害電腦使用罪及第三三九條之三，不過未再討論是否可能構成第三三九條之二⁴⁹。

除此之外，還有一些與第三三九條之二無關的事例，例如行為人是便利商店店員，知悉由便利商店代收刷卡資費時，銀行會給付便利商店手續費，行為人就借用他人現金卡向銀行借款，再以同筆

⁴⁸ 臺灣高等法院95年度上訴字第4568號判決，必須說明的是，構成第339條之3的行為人是訴外人，而該判決被告是訴外人的幫助犯。

⁴⁹ 臺灣高等法院98年度上更(一)緝字第6號判決。

借出金額假裝至便利商店繳費還款，羅織繳費紀錄，藉以使得賺得實際上不存在繳費交易的手續費數筆，法院也認為成立第三三九條之三罪名⁵⁰。此外，若行為人違法使用他人網路遊戲帳號，將他人網路遊戲的點數移轉至自己的帳號下，法院認為行為人可能構成第三五八條侵入電腦罪之外，還另外構成第三三九條之三罪名⁵¹。相對於此，倘若行為人打電話給電信服務公司，謊報其為本人並通過身分認證之後，變更本人原有的電信資費計算方式，使本人支出更多資費，法院認為行為人僅構成第三五八條及第三五九條刑責，因為資費調整只是服務契約內容的變動，還稱不上財產權的得喪變更，不構成第三三九條之三刑責⁵²。

三、電腦詐欺罪的解釋疑義

上述三個條文在二〇一四年修法後，就最高刑度七年以下有期徒刑的第三三九條之三，其處罰未遂犯尚稱合理，但第三三九條之二的最高刑度只有三年，雖然刑法典中也有類似規定，但似乎還需要有更強說服力的擴張處罰理由⁵³，至於第三三九條之一的最高刑

⁵⁰ 臺灣高等法院96年度上重訴字第14號判決。

⁵¹ 本案即著名的盜取他人「天堂」網路遊戲角色之虛擬武器案例，法院在本案中是以第339條之2第2項判處被告刑責，不過因犯罪時第358條的侵入電腦罪尚未立法通過，法院只針對財產犯罪部分判決，參見臺灣高等法院95年度上訴字第1825號判決。學理上的討論，參見甘添貴，虛擬遊戲與盜取寶物，台灣本土法學雜誌，50期，頁182，2003年9月。

⁵² 臺灣高等法院高雄分院100年度上訴字第830號判決。

⁵³ 第339條之2處罰未遂犯的修法理由謂：「原條文第二項未修正；另考量本法就三年以下有期徒刑之罪，多設有未遂犯之處罰規定，爰增訂第三項」，雖然刑法對於既遂犯最高本刑3年的罪名，並非絕對排除未遂犯，例如刑法第137條第1項及第2項的詐術考試罪、第161條第1項及第4項的脫逃未遂罪，但在財產法益犯罪的基本行情，只要最高本刑低於5年，幾乎不設未遂犯，例如

度只有一年，這麼輕的罪名還納入未遂犯即有疑慮⁵⁴。

除了任意擴張未遂罪名的不合理以外，實務透過眾多案例累積條文解釋方向，已建立若干成罪標準與可罰類型，但從學理角度仔細地觀察這三則條文的解釋適用，其實可以發現若干規範缺失，以下分別從罪質定位、電腦特性、犯行品質等三個不同層面，說明現有立法疑義。

(一)罪質定位不清

三則電腦詐欺的罪名規定在詐欺、背信罪章，條號設定又位列第三三九條詐欺罪之後，其罪質理應屬特殊形態的詐欺，解釋上必須符合詐欺罪的犯罪基礎結構：「行為人施行詐術，使相對人陷於錯誤，進而處分財產，致生財產損害」⁵⁵，然而以現有條文的規範機制而言，其實與詐欺行為的損害結構有一定差距⁵⁶。

最關鍵的問題是錯誤要素。所謂被害人陷於錯誤，相對人誤虛偽訊息為真實，這專指人類以其智力觀察外在事實後，發生理解意義不符合真正實情的主觀想像（*Vorstellung*）⁵⁷，既然是人類想法

第354條的毀損罪，只有既遂而無未遂；基此，第339條之2是否適合增加未遂罪名，即有進一步討論空間。

⁵⁴ 第339條之1增加未遂犯處罰的修正理由，僅寥寥數語：「原條文第二項未修正；另考量第一項及第二項之罪有未遂犯之可能，爰增訂第三項」，此一理由除了提到該條無未遂犯以外，根本無實質擴張處罰的論證，也欠缺從體系觀點比較的思辨。

⁵⁵ 有關詐欺罪損害結構，參考林東茂，詐欺罪的財產損害，警大法學論集，3期，頁200-203，1998年3月；吳耀宗，詐欺罪詐術行使之解析，月旦法學雜誌，163期，頁51-52，2008年12月。

⁵⁶ 甘添貴，同註21，頁331-332；黃常仁，同註2，頁3-4；蔡蕙芳，不正利用收費設備取財得利罪，月旦法學教室，44期，頁65-68，2006年6月。

⁵⁷ *Wessels/Hillenkamp*, *Strafrecht Besonderer Teil/2*, 30. Aufl., 2007, § 13 Rn. 508; *NK-Kindhäuser*, 3. Aufl., 2010, § 263 Rn. 168.

與外在事實的偏差，錯誤必然以具思考、認知者上當為前提，可是三則條文中，實施犯行的對象並不是具體個人，而是只接收程式、指令的機器或連線電腦，行為人其實是利用程式及指令設計上的缺失及弱點，規避正常支付、人別或財產資料檢控程序，直接引致不當的財產讓渡關係，整個流程中其實無任何自然人參與，不存在相對人的認知誤會理應無錯誤可言⁵⁸，如何能將三則條文置於詐欺罪章，不免滋生疑義。

正因為機器或電腦不可能陷入錯誤，我國有力見解傾向認為是三則條文本質上是竊盜行為⁵⁹，行為人利用機器程式或電腦機能的缺陷，違反原財物或利益持有者意思而取得財物或利益⁶⁰。上述見解確實掌握了關鍵重點，我們可以比對兩個案例，就可以發現電腦詐欺罪與竊盜罪之間有非常高的類似性，例如甲使用萬能鑰匙，打開保險箱後取走放置其中的珠寶；乙投入與10元硬幣等重的金屬圓塊到販賣機，取得飲料一瓶；丙將偽造的提款卡放入自動櫃員機內，從中領走3,000元。這三個案例的行為人，都是針對存放財物設備進行攻擊，但他們的侵害手法都非直接破壞機器外形，而是利

58 參見黃榮堅，電腦犯罪的刑法問題，載：刑罰的極限，頁179-185，1999年4月。

59 黃榮堅，刑法解題——關於詐欺等財產犯罪，載：刑法問題與利益思考，頁84-86，1995年6月；李茂生，同註2，頁227-230；林東茂，刑法綜覽，頁2-158，2012年8月，7版；張麗卿，機器與詐欺，載：新刑法探索，頁329-330，2006年8月。進一步討論，參考蔡蕙芳，自動化設備濫用行為之刑法規範，中原財經法學，11期，頁47-50，2003年12月。值得一提的是，黃榮堅教授認為在收費設備案例中，成立竊盜罪，但付款設備則不成立竊盜罪，參見黃榮堅，同註58，頁184-185。

60 我國刑法雖不罰使用竊盜，但若我們認為三則條文均為本質上的竊盜行為，這將使得我國實質上處罰了「未得同意而據他人財產利益為己有」的行為，而這個行為正巧是使用竊盜的處罰範疇，就此而論，三則條文實有偷渡處罰使用竊盜的疑慮。

用設備或程式設計的缺陷，使用表面上符合機器或設備運作機制，實際上卻致令防護功能完全喪失的作法，違反財物原持有人最終意願而奪取財物，甲、乙、丙三個行為人理論上應該構成最高刑度為五年的竊盜既遂罪，但依我國現行法，乙構成第三三九條之一的收費設備詐欺罪（一年以下有期徒刑），丙則構成第三三九條之二的付款設備詐欺罪（三年以下有期徒刑），基此，上述三個案例既然都是竊盜罪，卻因電腦詐欺的罪名設定，而存在不同的刑事責任，自然引起學理解釋第三三九條之一及之二等條文的重大困擾⁶¹。

很有意思的是，上述見解確實同於德國部分學說，均認為電腦詐欺罪本質上是竊盜行為⁶²，不過，較受支持的德國學說反而認為，對於收費或付款設備的電腦詐欺行為，本質上仍與竊盜行為不同，真正的竊盜被害人必須自始欠缺移轉意思，例如前例提到的保管箱內財物所有人，雖然透過鑰匙的物理性質而設定開啟條件，但其從來沒有要移轉存放財物給任何開啟者的意思⁶³，然而不論收費或付款設備的設置者，對於所存放財物的意思，並非絕對抗拒移轉該財物，設置者毋寧自始許可在一定條件下（相對人提供對待給付，或相對人為存戶本人或得本人授權者），願意移轉存放財物所

⁶¹ 至於如何處理競合，詳細討論，參考蔡蕙芳，刑法第339條之1不正利用收費設備取財得利罪之適用問題——四則地方法院判決之檢討，月旦法學雜誌，138期，頁236-238，2006年11月。

⁶² 相近於此的意見，Vgl. *Kindhäuser*, Der Computerbetrug (§ 263a StGB) – ein Betrug?, in: Gerald Grünwald-FS, 1999, S. 286; *Ranft*, Zur „betrugsnahen“ Auslegung des § 263a StGB, NJW 1994, S. 2576; *Mitsch*, Strafbare Überlistung eines Geldspielautomaten – OLG Celle, NJW 1997, 1518, JuS 1998, S. 310 ff.; *Neumann*, Unfares Spielen an Geldspielautomaten – OLG Celle, NStZ 1989, 367, JuS 1990, S. 538.

⁶³ *Achenbach*, Die „kleine Münze“ des sog. Computer-Strafrechts – Zur Strafbarkeit des Leerspielens von Geldspielautomaten, Jura 1991, S. 226.

有權予相對人，質言之，設置者意思並非反對移轉，而是附條件的同意移轉，行為人只不過利用機器或電腦判別程序的缺陷，不符合設置者的終端意思而取得財物，就移轉持有的形式條件看來，應認為行為人滿足設置者附條件同意而取得持有，不成立竊盜罪。舉例來說，販賣機設置者的終局意思應該是「取得10元價金即給付飲料」，但實質表現在機器上的設定，則是「投入與10元等重物品即給付飲料」，本說主張者似乎認為，如果凡事取決於終局意思，可能引起刑責界限的不穩定，因而轉從表現於外的販賣機設置者意思觀察移轉飲料有無同意⁶⁴。

由於電腦詐欺罪不同於傳統竊盜與詐欺，行為人利用機器或電腦程序缺點而取得財物或利益，該行為顯然與詐欺罪須有相對人陷入錯誤不同，但是否同時也是竊盜行為又有不同意見，糾結在兩種不同的犯罪類型間，應該如何拿捏其界限，實有深入討論必要⁶⁵。

(二)電腦與資料處理特點不明

除了難以明確區別竊盜及詐欺的問題之外，這三個條文是否屬於「電腦」詐欺？三個條文之間有什麼樣的差別？這兩個針對電腦詐欺條文關係的疑惑，其實更難以解決。

雖然條文裡面根本沒明白指出這是電腦詐欺，但至少在第三三九條之二及之三的立法理由中，都提及電腦處理資料特點，不過所謂電腦犯罪並不是涉及電腦就好，還必須犯罪手法或攻擊對象涉及到電腦處理資料的特性。電腦特色在於，操作者先透過指令輸入特定內容（input）予電腦運算程式，程式運算後，會依據原先設計反應出特定的結果（output），電腦運算過程的重心在於資料處理

⁶⁴ 接近於此一見解者，參考黃常仁，同註2，頁8。

⁶⁵ 德國法上電腦濫用行為與詐欺關係的討論，vgl. *Lenckner*, aaO. (Fn. 12), S. 22-33.

(Datenverarbeitung)⁶⁶，這個過程與一般機器的物理運作有相當差距，如果第三三九條之一所規定收費設備的建置核心若只是採用物理原理⁶⁷，未運用到電腦資料運算的特色時，其實不算是真正的「電腦」詐欺⁶⁸。

此外，這三則條文相互關係，也難以直接理解。第三三九條之一及之二是透過侵害客體功能是收費還是付款區分，收費從概念上來看，應該是使用者必須支付對價，再從設備取得給付；而付款則是使用者出示人別憑證，再從設備取得金錢。雖然隨著技術發展，有時不免有些模糊空間，但大致上還可透過文字定性，從而掌握之一及之二兩條輕罪系列的保護對象。

問題是之三條文中，並未如同前兩條透過客體限定處罰範圍，立法者毋寧強調犯罪手段，只要以不正方法傳輸不實資料或指令到他人電腦中，進而影響財產權，就會成立犯罪。然而，當收費設備附有連線至其他伺服器的功能時，以不正方法取得收費設備內的對價，必定同時符合輸入不正指令而變更電腦內財產紀錄的要件，構成第三三九條之三，此時同時成立第三三九條之三與之一兩項罪名，到底要構成較重的之三還是屬於特別規定的之一，不免發生疑問⁶⁹，具體適例即透過連線電腦盜刷他人不用簽帳、只須過卡的信

⁶⁶ Wessels/Hillenkamp, aaO. (Fn. 57), § 13 Rn. 602; NK-Kindhäuser, § 263a Rn. 12; Lackner/Kühl, Strafgesetzbuch Kommentar, 26. Aufl., 2007, § 263a Rn. 3-4; Maurach/Schroeder/Maiwald, aaO. (Fn. 14), § 41 Rn. 229; Rengier, aaO. (Fn. 14), § 14 Rn. 3-4.

⁶⁷ 例如飲料販賣機偵測投入硬幣的大小及重量，以決定購買者投入金額，當滿足時再給予飲料，這種流程本身只是應用物理原則，稱不上具有電腦運算的特點。

⁶⁸ 有關電腦處理資料特性的討論，參見蔡蕙芳，同註1，頁31-32。

⁶⁹ 事實上，與第339條之3犯罪型態比較接近的是第339條之2的付款設備，因為付款設備原則上必然要連線到中央處理伺服器，否則無從確認使用者有無提

用卡購物，從過卡後即給付財物來看，該連線電腦可認為是付款設備，但行為人未直接損害設置付款設備之人，而是透過付款設備設置者的請款，實現原持卡人的損害，這樣的交易結構應該適用第三三九條之一還是之三，自然引起困擾。

至於第三三九條之二，雖然付款設備幾乎均透過網路與銀行中央伺服器連線，並在中央伺服器處理電腦資料，否則不可能計算帳戶餘額而判定給付數額，不過一旦連線的特徵不明顯時，是否還算是具有電腦連線運算特質的收費設備，即生問題。前文提到的語音轉帳方式即為適例，正因為行為人並未直接使用卡片或是輸入電腦資料，而是利用具有中間介面性質的語音電話輸入資料，這也使得實務往往莫衷一是。

總結而論，第三三九條之一及之二等兩罪強化客體，之三則重視行為方式，這樣前後不相一貫的立法政策，在電腦及網路日益發達的今天，勢必產生許多難以解決的問題。一來這些條文的電腦特質何在？二來如何從電腦交易結構來區辨個別條文的適用範圍？這些問題都有賴進一步的解釋。

(三)法定犯行概念模糊

除了罪質定位及電腦特質不清，這三個電腦詐欺的條文還有犯行描述過度模糊的問題。這三個條文都屬於特種形態的電腦詐欺行為，立法者設計條文時，對行為人成立犯罪所需要的犯罪手法，完全不考慮個別情況差異，直接採用內容相當模糊的「不正方法」描述法定犯行，然而什麼是不正方法，不僅無法從條文文字中看得出來，立法者也未於立法理由中澄清。倘若進一步追問：第三三九條

款權限，德國刑法第263a條將付款設備及連線型的電腦詐欺合併規定，相對於我國立法例應是比較合理的作法。

之一收費設備詐欺罪的不正方法，是否與第三三九條之二付款設備詐欺罪的不正方法相同？這一點完全無法從條文本身規定得知答案。

一個常被提及的對比型例子是：甲拾獲他人遺失的10元銅板，投到販賣機購買飲料；乙拾獲他人遺失的真正提款卡（假設卡片上寫有密碼），持之到自動櫃員機領出10,000元。暫且不論甲、乙行為人侵害財產價額高低，僅思考拾獲他人物品卻予以使用的甲、乙兩人行為，是否構成第三三九條之一及之二的「不正方法」？從某個角度觀察，甲、乙均於拾獲他人物品後，故意據為己有而享受其用益機能（甲拿10元至販賣機買飲料；乙使用卡片提款），甲、乙在取得飲料及10,000元之前，都構成侵占遺失物罪，甲之所以能啟動接下來的電腦詐欺行為，實因已完成不法前行為，在刑法評價上看來，後行為屬於前行為不法狀態的延續與擴大，自應認定為「不正當」的方法，然而，如果轉從飲料商及銀行的角度來思考，其實飲料商並不在乎丟進販賣機的錢是不是侵占所得，只要是能夠合法交易的法定貨幣，對飲料商而言完全正當；相反地，縱然提款者不必然是卡片及戶頭所有人，但至少必須得到戶頭所有人的內部授權，否則銀行並不樂意支付這一筆款項。上述兩種說法都有其道理，但究應採用什麼觀點掌握不同罪名間的「不正方法」定義，學說及實務即發展出各式各樣的學理意見⁷⁰。

部分見解認為既然條文都使用了不正方法用語，因此三個犯罪的不正方法，應該採相同解釋標準，否則勢必影響刑法適用的安定性⁷¹。相反而論，我們也可以認為，不正方法的解釋應該考慮個別

⁷⁰ 相關整理，可參考蔡蕙芳，同註59，頁50、55-58；蔡蕙芳，同註1，頁64-87。

⁷¹ 參考蔡聖偉，論盜用他人提款卡的刑事責任，月旦法學雜誌，144期，頁29-

侵害對象差異性，收費設備及付款設備的建制與交易結構理由並不相同，自應有不同標準。至於應該採用什麼觀點，我們其實無法從法條得知，只能留待進一步解釋。

倘若再觀察第三三九條之三，就可發現該條的不正方法，其實只是條文對犯罪行為的描述之一，條文中還進一步限縮行為方式，行為人必須「輸入虛偽資料或不正指令」，問題是：倘若條文已然透過「輸入虛偽資料或不正指令」描述構成要件的法定犯行，那麼條文最初所謂的「不正方法」到底有何定性功能，自不無疑義。

綜上，雖然立法者廣泛地使用不正方法，並以之作為替換「詐術」的電腦詐欺犯行，但實質內容到底是什麼？在條文中有何功能？都無法從條文中觀察得知，這一點實有賴釋義學深入研析。

四、小 結

以上簡要說明我國現行法缺失，以及立法政策上可能的困境。不過筆者必須承認，即便充滿著罪質、電腦特性及犯行內容的浮動，但從第三三九條之一至之三等罪名立法以來，適用這三條罪名的案件數量頗多，實務已經找到了一個平衡學理及現實的作法，甚至構建了較為折衷的解釋方向，以下討論，將暫時停止立法面及政策面的針砭，轉以現行刑法的三條規定為中心，筆者將先提出個人主張的共通解釋立場，再逐條分析，討論過程中也會一併說明前文提過的實務具體案例。

參、重新解釋電腦詐欺罪

一、解套進路的探尋

在討論個別條文解釋前，必須先說明若干共通基礎觀點。

先談三個條文的罪質定位，第三三九條之一至之三則條文雖然規定在詐欺罪章，但不論是機械式或連線式的收費及付款機制，都只依程式設定，決定是否以及如何給付予系統使用者，其規範根本踩在竊盜與詐欺兩種罪名的灰色界限上，平心而論，竊盜、詐欺等不同罪名本應相互獨立，並依個別結構而位於財產犯罪各罪章，然而，我國立法者竟然先從中抽繹出所謂的「自動設備或電腦」要素，合併規定在普通詐欺罪後面，從而統合／規避了兩類不同侵害態樣，甚而建構出三則新獨立的電腦詐欺條文。這種內在結構及外在形式完全不吻合的景況，顯然源自社會對電腦發達後社會生活可能因而改變的遲疑，過快又未經仔細思量的立法程序完全體現了這種漫散於社會的焦慮感⁷²。不過，既然條文已經這樣訂了，短期內也難以看到任何改變，作為刑法學研究者，無非僅能從散落且無關的條文中，設法找到一條合理解釋的可行作法。

雖然各罪名間差異甚大，但既然條文結構上已經被強行綁在一起，罪名及章節也已確定下來，若仍堅持第三三九條之一及第三三九條之二本質上均非詐欺，而是財物或利益竊盜，顯然難以回應為什麼竊盜罪出現在詐欺罪章的質疑，筆者認為解釋第三三九條之一及之二的可行方向，應該是回歸詐欺罪的原始結構，設法透過釋義學操作，把詐欺罪的犯罪結構整合到第三三九條之一、之二及之三的條文中，設法讓電腦詐欺罪產生近似於詐欺罪的損害結構，如此

⁷² 有關電腦發達後的社會焦慮，參見李茂生，同註2，頁288-300。

不僅可以解決電腦詐欺罪名實相符的疑義，也可以清楚地區別三個罪名之間的差異⁷³。

依現行刑法通說，詐欺罪具有特別的損害結構⁷⁴：行為人必須先實施詐術，導致相對人陷入錯誤，相對人接著實施財產處分，最後發生財產損害。而因電腦只依程式運算，不可能有思考、認識或想像上的誤會，所以主流學說一直認為電腦詐欺其實不能算詐欺行為，不過，即便沒有任何自然人陷入錯誤，當行為人輸入形式符合、卻實質悖反正當財產移轉效能的資料，卻可以稱得上是致令機器或電腦作出不合原訂財產移轉條件的「欺騙式指令」，依本文之見，這種違反其預設目的，卻又無法透過既有程式進行判斷的資料，正是電腦詐欺條文所稱的「詐術」⁷⁵，亦即條文所稱的不正方法，透過這種詐術／不正方法，才能造成機器或電腦的「錯誤」，從而移轉財物或利益予行為人。認定行為人輸入的資料或指令是否構成「欺騙式指令」時，重點即為透過交易結構與交易資訊間的關係，判斷時，應具體考量設置機器或電腦時，預期的「財產移轉實質前提」是什麼，即便行為人輸入資料完全符合系統移轉財產的形式條件，但只要該資料違反了系統期待並預設的實質條件，該行為仍屬欺騙式指令，得成立電腦詐欺行為，相反地，如果系統並未要求嚴格的實質移轉財產條件，縱然行為人違反法律或道德而取得設

⁷³ 我國多數見解對於這三則條文的解釋立場，也大多從此觀點出發，參考黃榮堅，電腦的心事，月旦法學教室，37期，頁21，1998年6月；甘添貴，同註21，頁330、332。

⁷⁴ 有關詐欺罪的損害結構，參考張麗卿，同註59，頁323-329。Vgl. Rengier, aaO. (Fn. 14), § 13 Rn. 1a; Wessels/Hillenkamp, aaO. (Fn. 57), § 13 Rn. 490; NK-Kindhäuser, § 263 Rn. 43; Artz/Weber/Heinrich/Hilgendorf, aaO. (Fn. 14), § 20 Rn. 28.

⁷⁵ 出發點相同但結論有異的看法，vgl. Kindhäuser, aaO. (Fn. 62), S. 290.

備或系統給付財產，仍非電腦詐欺行為。

事實上，類似思考方式早已見於詐欺罪的討論之中。依據現行通說見解，詐欺罪的詐術行使方式共有三種：明示詐欺、默示詐欺（前兩者均為作為型詐術）及不作為詐欺，在此要特別討論的是默示詐欺行為⁷⁶，所謂默示詐欺指行為人未明確告知相對人不實訊息，但依據交易習慣與市場通念，行為人既已實施的作為中，已經傳達對交易過程極為重要的訊息⁷⁷，常見案例如行為人明知無資力支付食宿，而仍走入餐廳點用高級牛排，在這個案例中，行為人未曾告知餐廳他的支付能力，餐廳也未真正地詢問顧客，但從我們社會生活慣習來看，前往餐廳消費高級牛排的人，幾乎必然具有支付對價的能力及意願，簡言之，進入餐廳並點餐的消費行為（作為），同時表達了具有「支付能力及支付意願」，若實質上欠缺支付能力或支付意願時，即構成默示的詐欺行為⁷⁸。

從上述例子可以發現，默示詐欺的行為人同樣實施了形式上符合財產移轉條件（進入餐廳點餐）、但實質上卻不符合交易預設條件（欠缺支付能力或意願）的行為，由於其行動符合形式的交易慣例，餐廳才願意提供餐點、服務給行為人，但事實上卻欠缺支付能

⁷⁶ 明示詐欺是行為人以積極方式，傳達不實資訊給相對人；至於不作為詐欺則是，在交易習慣上行為人有義務告知相對人特定事項，但行為人故意不為告知。行為人只要採用這三類行為方式之一，即屬實施詐術，可以構成詐欺罪，參見吳耀宗，同註55，頁55-63。Vgl. auch Rengier, aaO. (Fn. 14), § 13 Rn. 5; Wessels/Hillenkamp, aaO. (Fn. 57), § 13 Rn. 497-507. 有關默示詐欺與不作為詐欺的區別，另可參考李聖傑，靜靜都有事？，月旦法學教室，104期，頁28-29，2011年6月。

⁷⁷ Vgl. Rengier, aaO. (Fn. 14), § 13 Rn. 5a; Arzt/Weber/Heinrich/Hilgendorf, aaO. (Fn. 14), § 20 Rn. 37. 當然，行為人主觀上必須明知該默示傳達的訊息不實，才能成立詐欺罪。

⁷⁸ 參考吳耀宗，同註55，頁56-58。

力及支付意願，因此構成默示詐欺行為。

把同樣論述轉換到第三三九條之一及之二的解釋，即可發現對電腦或相關設備的詐欺行為，有著相近默示型詐術行為的成罪結構：行為人輸入符合移轉財產形式條件的資料或指令，該形式條件成就時，同時表示了行為人符合移轉財產的實質條件⁷⁹，但當實質條件根本不能滿足時，這種形式符合、實質違反交易條件的行為，即構成對電腦的詐欺。舉例來說，如果預期實質移轉前提不在乎使用者身分、人別，只在乎能否取得對待給付，那麼縱使他人先竊取、侵占或搶奪他人金錢，並將該金錢投入設備中，雖然錢是不法取得，但此時形式、實質上均符合程式要求，行為人自然不能認定為對機器詐欺了。

既然重點是機器或電腦系統預設的財產移轉實質條件，當然必須考量個別條文才能決定其內容，在此就涉及到前文提到的第三點批判，由於現行電腦詐欺三個罪名的法定犯行，全部都與「不正方法」字眼有關，立法者放棄具體明確地定義犯罪行為的結果，正是無法直接從條文「不正方法」字眼得知，到底電腦系統或設備要求的財產給付實質條件是什麼，為了確認不正方法，必須展延條文結構的觀察視域，才能具體判斷個別條文不正方法的定義。

基此，解釋第三三九條之一時，必須考量不正方法施用對象「收費設備」的交易結構；理解第三三九條之二犯行時，同樣必須以不正方法施用對象「付款設備」的給付財產基本條件，作為掌握不正方法內容的依歸；至於第三三九條之三則較為特別，條文中不

⁷⁹ 例如：行為人持用他人提款卡及正確密碼到自動櫃員機提款，該行為符合形式上的取款要件，同時實質上表達「提款者是有權取款人，或至少受有權取款人之委託」，如果行為人只符合形式條件，但卻不符合實質條件（例如盜用他人提款卡），即可認為屬於利用取款的形式／實質條件落差，從而取得他人財產利益之行為。

正方法不像前兩條連結到施用對象，而是連結到接續的行為內容「虛偽資料或不正指令輸入電腦或其相關設備」，接著再實現「製作財產權之得喪、變更紀錄」的中間結果，最後才實現財產損害，在此必須思考若干重點：(一)「不正方法」與「輸入虛偽資料或不正指令」的關係為何？(二)資料的「虛偽性」或指令的「不正性」，是相對於什麼樣內容的「真實」資料或「適正」指令？(三)行為人如何製造財產權得喪、變更紀錄？(四)該財產權紀錄與最終財產損害的關係為何？

無論如何，解釋第三三九條之一至之三等條文時，應該搭配條文中的其他要素才能認定不正方法的定義，尤其應該考量整體交易結構的財產變動關係，以及個別要素間的因果聯結。

至於學說提出的問題：解釋不正方法時，三個條文均應採取相同的解釋立場？抑或應該考量不同電腦詐欺類型而發展不同角度的解釋觀點？雖然三個條文都提到不正方法，看似應該採取相同定義⁸⁰。然而，不正方法是對機器或電腦的類詐術行為，其標準即是形式上符合、但實質上不符合移轉財產條件的資料輸入或指令下達，判斷重心應該是個別條文所關切的「移轉財產實質條件」是什麼，這一點必須借助構成要件的個別要素才有辦法確認，包括類詐術施用的機器或電腦屬性，該機器或電腦設定的交易架構及財產移轉程序等等。比方第三三九條之一侵害收費設備，而第三三九條之二則規範付款設備，這兩種不同設備在交易架構上就有莫大區別，前者著重「收費」，在移轉財物或利益時，當然關切使用者是否如實支付費用，付款者只要支付正確價額，就已經符合收費設備的預期效果；相反地，後者則強調「付款」，前來取款的人不必提出對待給付，但付款銀行卻必須清償消費寄託的債務，整個交易結構的

⁸⁰ 主張應採相同解釋觀點的看法，參見蔡聖偉，同註71，頁29-31。

重心自然是取款者證明自己有權受領款項，因此人別、身分確認或權限授予的存在，自然會是付款設備始終重視的付款實質條件。從這兩個例子中，可以很清楚地發現兩者交易架構不同，推論上就會導出完全不同的實質條件。因此筆者認為，第三三九條之一至之三等三個條文所稱的「不正方法」，應從交易架構及設備操作方式個別觀察，每個條文的不正方法都有順應個別交易結構的不同意義⁸¹。

進一步的問題則是：筆者看法能不能解決前文提到的三重批評？對此筆者初步意見認為：第一，電腦詐欺罪的罪質本身過度複雜，為了統一解釋並區別三個條文間的關係，筆者主張應從詐欺罪的結構來定位三則條文處罰界限；第二、三則條文中，除了第三三九條之二及之三，理論上必然有電腦處理資料特性外，第三三九條之一則同時有涉及與不涉及的事例，但這一點其實並非解釋的關鍵，釋義時的重心毋寧是個別條文的交易結構，亦即該結構所要求的交易實質條件為何；第三，由於釋義學上應朝詐欺結構解釋，所謂不正方法，指的就是在電腦或相關設備的程式運作下，符合形式移轉條件，卻違反該交易結構的實質條件之資料或指令輸入行為。以下就從實質的交易結構，逐一審視每個條文所稱的不正方法內容為何，同時也一併思考與特定交易結構關聯的構成要件解釋疑義。

二、自動收費設備詐欺罪

(一)收費設備的交易結構

從字面結構觀察，收費設備的使用者必須先提出給付，由設備審核使用者是否正確地提出符合財產價值的給付，使用者才能取得

⁸¹ 相同看法參見蔡蕙芳，不正利用自動付款設備取財得利罪，月旦法學教室，49期，頁63-64，2006年11月。

設備提供的對待給付，這種結構關係正是收費設備的設置目的⁸²。我們尤其可從立法者預想的飲料自動販賣機交易流程，觀察到這樣的財產流通方式，使用者通常在硬幣投入口擲入10元硬幣（使用者先為給付），接著販賣機審核使用者投入的金額是否正確（收費設備審核給付內容），如果與飲料價額相符，販賣機就會將飲料交給使用者（使用者得到對待給付）。

既然收費設備著重「使用者提出給付vs.設備提供對待給付」的關係，設備程式當然也特別重視使用者是否如實提供正確給付，原則上只要使用者能夠先將給付移轉到收費設備內，對待給付就會實現，從「收費設備」的用語可以認為，該設備並不真切地關心設備使用者（亦即提出初步給付之人）是否為民事關係的真正權利人，只要使用者在收費過程中，確實交付適足、正確的財產給付，設備裝置機制將許可對待給付⁸³。

綜合上述，收費設備只關切使用者給付內容的真實性，但不在乎參與給付活動的人別關係，當收費設備使用者形式上提出給付，並通過收費設備設定的判別程序，該給付卻不具有等值財產價額時，即屬形式上符合交易條件，但又無法符合收費設備提供財物或利益實質條件的行為，即成立第三三九條之一犯罪，本罪不正方法指的正是「貌似已提出合法財產效果的給付行為，但實際上無任何財產給付效果」之行為，常見方法即投入等重鐵塊以取得販賣機中的飲料，等重鐵塊並非通貨，但卻可通過販賣機物理收費設備的判讀程序，致令收費設備誤判為已獲給付，從而下達對待給付指令，

⁸² 由設備自己提供，例如飲料自動販賣機或按摩椅，由設備辨識相對人是否已經提出給付，再授權第三人提供給付，例如公車上的悠遊卡感應扣款機，只要通過扣款，即授權公車司機提供客運服務。

⁸³ 相近見解，見黃常仁，同註2，頁6；蔡蕙芳，同註59，頁57。

此時顯然實現了不合法的財產變動效果，從而構成本罪。

(二)收費設備的定義及範圍

再談收費設備範圍。從字義來看，「收」「費」設備指的是設備使用者提供價金費用，由設備判斷是否已經收到費用，如果確認了，就提供財物或利用作為對待給付，常見的飲料自動販賣機或按摩機，都屬於這類的收費設備，其交易關係單純發生於使用者與設置者之間，原則上都可以納入收費設備範圍⁸⁴。

實務案例中曾出現兌幣機詐欺案例，實務見解傾向肯定兌幣機也算收費設備，對其實施不正方法即能成立第三三九條之一。值得思考的是，兌幣機並不是直接提供特定給付，而用以將面額較大的紙鈔換為面額較小的硬幣，直觀而論，兌幣機只是提供「換錢」服務，使用者不必為這項服務提供任何費用，既然不必付費，那當然沒有任何收費機制與設備可言，基此，我國實務認為兌幣機屬於收費設備的見解，不免有其問題⁸⁵。不過，筆者認為實務見解並無違誤，收費設備是收取使用者一定的給付，以作為對待給付之用，只要使用者必須為了對待給付而先向設備支付一定價金即足，支付後的對待給付內容即便與原給付有完全相等的市場，甚至等同於原來給付，也不會使得該設備不具有「收費」機能，基此，兌幣機仍然可認定為收費設備⁸⁶。

⁸⁴ 一般常見的情況是收費設備本身也提供服務（販賣機、按摩椅），但也有可能由機械收費，再由人提供服務，例如演唱會的驗票機，由於法條並未要求收費設備同時是服務設備，後者原則上也可計入收費設備範圍。就此的討論，參考蔡蕙芳，同註56，頁68-69。

⁸⁵ 學理亦有認為兌幣機屬於付款設備者，見黃常仁，同註2，頁10。

⁸⁶ 同樣的問題也發生在賭博遊戲機，考量其必須付費後才能享受賭博服務的對待給付，筆者原則上認為這也算是收費設備，討論見蔡蕙芳，同註61，頁239-242。

除了上述較為基礎且傳統的收費設備之外，隨著現代交易型態日趨複雜，收費設備的機制已經不再限於一次性給付關係，為了追求更方便的交易環境，現代社會發展出態樣日益繁複的收費機制⁸⁷，我們大概可以將非傳統的收費機制區別為兩種次類型。

第一類可稱為儲值型的收費機制，通常先由買方於實際進行交易之前購買儲值，在交易過程中，買方不再現實性地給付價金，而僅出示買好的儲值內容，賣方確認買方確實有足額儲值後，扣減該儲值金額作為買方的給付內容，接著再提供財物或服務的對待給付。這類具體適例即電話卡或悠遊卡，持卡人必須事先購買儲值，再於嗣後交易時扣減儲值以換得對待給付。根本而論，這類交易關係其實與現金交易無過大差異，只不過必須事前將現金交換成儲值金額，並經由網路連線，藉以確認儲值金額是否還足夠擔負對待給付。依筆者之見，雖然儲值型收費往往動用到連線電腦功能，但實際上並未迥異於傳統收費設備的交易過程，只不過中間多了一道現金轉換為儲值的程序，而實際交易時僅提供效力等同於現金的儲值內容，但交易本質結構並無不同，屬於這類的設備仍可認定為收費設備⁸⁸。

第二類則更為複雜，可稱之為後付型收費設備，這類結構雖然有收費外觀，但實際上付費過程是在交易之後，在交易過程中，設備不收受費用，僅具有身分或連線認證的功能，買方依循身分、連線認證機能確認其為本人後，賣方即透過設備提供交易的財物或服務給買方，完成交易之後，再由賣方向買方請求給付之前的交易對

⁸⁷ 蔡蕙芳教授亦將相關收費設備分為「不涉及資料或程式操縱」及「涉及內部資料或程式操縱」等兩種，參考蔡蕙芳，同註59，頁57。

⁸⁸ 相同見解，參考蔡蕙芳，同註59，頁68-69。主張類似犯罪應以第339條之3處罰者，另見陳子平，偽造支付工具電磁紀錄物罪與相關犯罪，月旦法學教室，111期，頁83-84，2012年1月。

價。常見情況如撥打手機時，用戶並未立即付費，而是由電信公司依費率計算整個月資費後，於月底結帳日向用戶請求支付；又例如使用不需簽名的信用卡，在具有連線功能的讀卡機過卡後，使用者獲得權限而加油。這些交易雖然有收費的形態，但實際上設備裝置者並不即時收受費用，而是先給付財物或利益，同時承擔使用者可能無從清償債務的風險，這一點與傳統型收費設備的交易結構不同，傳統收費設備的服務提供者僅於收到費用後才給付，完全不承擔任何設備使用者嗣後不能清償款項的風險，就此而言，傳統與後付型收費設備的交易結構顯然有相當落差。

我國實務與學說似乎未注意到上述交易結構的差異，幾乎絕大多數的見解，都認為不實質收費而只「計費」的設備，依然可計入「收費設備」⁸⁹，也因此，若行為人不是最終負擔使用費之人，卻盜用他人名義而自計費設備先行享受服務，致使設備裝置者最終必須向本人求償，卻又可能無法如願求償，或成功求償後，使得本人另外支出一筆費用時，我國實務與學說均認為行為人成立第三三九條之一刑責，常見適例即盜用他人信用卡，在無須簽名的自助加油站加油，或以之盜打國際電話，不論加油站或國際電話的信用卡連線機器，均無任何收費機能，設備中計價方式是先行計費功能，未來於每期帳單中向本人請求給付資費；另一種情況則是盜用他人手機通話，該手機連線的電信公司計費系統，同樣也沒有收費功能。我國實務及學說針對上述案例，一向肯定構成第三三九條之一犯罪。

然而本文則有不同見解，判斷人別或資料以決定是否先提供對待給付的設備，並不是嚴格意義的收取費用後再給付對價之「收費設備」，而是用來計算事後向本人索費的「計費設備」，計費設備

⁸⁹ 不同意見，蔡蕙芳，同註59，頁53。

的設置本旨是判斷使用者人別身分，以供事後索費之用，這裡不存在「給付→判斷給付為真→對待給付」的對價支付交易結構。

此外，若再考量交易風險的關係，收費設備的特點在於一手交錢、一手交貨，能夠採用這種直接的給付／對待給付的交易型態，一般而言都以小額給付為多，能引致的損害後果相當受限，再考量到雙方承受的交易風險相對較低，特別是作為被害人的設備提供者，幾乎只負擔「給付是否為真實財產價額」的管控風險，不必負擔未來得向使用者請求償付卻未能實現的風險，也因此，本罪的刑事責任才能大幅度地降低至一年以下有期待刑。相反而論，計費設備的提供者必須負擔極高的受償風險，單純以第三三九條之一的低度罪名論罪，不免有保護不周的疑慮，這類案例的刑事責任判斷重心，其實應該檢討行為人是否構成偽造文書，甚或第三三九條之三的罪名，但基本上無涉於第三三九條之一。

綜上，筆者認為，所謂收費設備僅限於使用者先提出給付，而由機器或電腦判讀其給付內容的財產屬性與價額，待認定符合財產價額後，即為對待給付的設備。倘若設備欠缺領受使用者給付的功能，僅屬計費設備，則與本罪無關。

(三)不正方法的認定

接著討論本罪的不正方法內涵。已如前述，筆者主張考量收費設備特性以確認不正方法的實質定義，收費設備重視「給付／對待給付」的關係，但不關心給付提供者的人別，只要設備設置者可以從被害人處取得價額，即便最終造成被害人的損失，但仍與設備設置者無關。至於收費設備的給付實質條件即為「使用者提出真實財產價額」，任何「形式上符合收費設備程式，卻違反實質條件」的行為，均可認為屬於不正方法。相反地，如果行為人以暴力打壞收

費設備⁹⁰，或是利用人多之便跨越收費柵欄而無費乘車⁹¹，或翻牆潛入收費設備管控入口的遊樂場⁹²，這些行為雖然無權取得利益，但與收費設備交易的詐欺無關，仍不構成不正方法。具體案例的檢討，筆者認為或可從上文提出的幾種收費設備型態分類切入觀察。

1. 傳統收費設備的不正方法

首先是傳統收費設備，典型代表即飲料販賣機與收費式按摩椅，這類型的設備通常採用物理原理建制機械式判讀機制，只要投入的紙鈔或硬幣符合機械判讀流程，設備即給付財物或服務予使用者，對於這類傳統物理式收費設備的不正方法，一般而言又可分為三類。

第一類是投入不具有通貨價值的偽造硬幣或相近外幣，基礎案例即：行為人投入與真幣等重的假幣以換取飲料，形式符合販賣機程式，但實質違反交易條件，構成第三三九條之一的不正方法。如果行為人選擇的侵害方式，是投入假幣後再利用退幣功能而換取真幣，對設置販賣機的交易目的而言，退幣功能也是服務的一部分，讓消費者保有選擇權利，退幣功能仍可認定是交易的從屬結構，該從屬結構仍要求消費者先為給付（投幣），若不滿意販賣機提供的飲料內容，則可選擇全額退費，雖然退費是一種返還原給付，而非另給予新給付，可是設備之所以願意退費，實以使用者先投幣為前提，仍可算是一種特殊形式的對待給付。當行為人先提供的給付是假幣，退幣後卻獲得真幣時，應該認為是本罪的不正方法⁹³。另一

⁹⁰ 林山田，同註16，頁470；甘添貴，同註21，頁330。

⁹¹ Vgl. *Ellbogen*, Strafbarkeit des einfachen „Schwarzfahrens“, JuS 2005, S. 20-21.

⁹² 黃榮堅，同註2，頁316-317。

⁹³ 我國多數見解亦同，參考蔡蕙芳，同註59，頁57。相反而論，如果是兌幣機或相類設備多退錢給行為人，仍與第339條之1無關，參考蔡蕙芳，同註56，頁70-71。

種情況則是行為人投入不能在本國交易，但其重量、形狀卻足以誘發販賣機給付的外國硬幣，這部分的解釋原則上應與假幣相同⁹⁴。

第二類則是投入真幣，但該真幣來源有問題的事例，亦即行為人以竊得、不法侵占或任何違法方式取得的真實硬幣購買飲料，雖然取得硬幣的方式違反法律，只要行為人使用真正通貨投入收費設備，即不違反收費設備的給付實質條件，本文認為不構成不正方法⁹⁵。

除了以硬幣投入收費設備之外，第三類常見的案例則不直接投幣，而是採用投幣以外的其他方法干擾收費設備機械功能的行為，這類案例與保管箱竊盜非常近似，因為後者正是干擾保管箱鑰匙或密碼的保全功能，從而取得內部財物的，兩者間確實有難以區隔的困擾⁹⁶。不過若能更精緻地觀察兩類案例，仍可發現其差異，保管箱的鑰匙或密碼僅能防止行為人開啟，但無任何「附條件給付」機能，收費設備的設置目的則是進行交易，必然附帶特定的給付條件，基此，僅當行為人干擾收費設備機械功能的行為與「誤認消費者已經提出給付（但事實上未有給付）」有關，才能夠納入不正方法的範圍，否則應該屬於竊盜罪的處罰範圍。前文曾提過兩個案例，其中的行為人均干擾機台內部的感應器，使得機台「誤以為行

⁹⁴ 這部分見解為匿名審稿人所指正，筆者敬致謝忱。

⁹⁵ 此亦為我國多數說，參考蔡蕙芳，同註59，頁56；黃榮堅，同註2，頁317；林山田，同註16，頁469-470。

⁹⁶ 此一問題在德國法上尤其有爭議，因為德國法並無我國獨立的「收費設備」規定，較相近的規定僅為其刑法典第265a條的詐領給付罪（*Erschleichung von Leistungen*）以及第263a條的電腦詐欺罪。第265a條重視行為人未真正提出對待給付而取得機器所提供給付，某程度上與第339條之1有相近之處。至於德國刑法典第263a條規定涉及「電腦資料處理」的電腦詐欺罪，此類針對機械式機制的侵害行為，德國實務即認為不成立第263a罪名，vgl. *Biletzki, Anmerkung an OLG Düsseldorf, NJW 2000, 158, NStZ 2000, S. 425.*

為人已經投幣」，而提供夾娃娃的服務或給予飲料，依本文見解，都可認定為本罪的不正方法⁹⁷。

2. 儲值連線型收費設備的不正方法

其次是儲值型收費設備，這一類收費設備通常必須透過連線電腦與中央伺服器連線，才能判斷行為人手邊的儲值額度能否消費，常見侵害方式如行為人無權使用他人的儲值卡提供給付，自動收費設備收到給付訊息後，透過連線電腦系統，研判屬於正確的財產給付後，提供對待給付給使用者。

與前文提到的紙鈔、硬幣問題相同，儲值卡的問題也可分為偽造型與不法取得型，就不法取得型而言，不論行為人以什麼樣的不法管道取得儲值卡（竊盜、侵占遺失物、搶奪或強盜），只要儲值卡為真，收費設備能夠從該真卡扣減儲值，達成給付關係，即無對收費設備實施不正方法可言，因此違法盜用他人悠遊卡搭乘捷運的行為人，仍不成立第三三九條之一犯罪⁹⁸。但若行為人使用偽造卡片扣減儲值，因偽造的卡片無從連結至真實的財產給付內容，構成第三三九條之一的不正方法。

最後，筆者要強調的是，倘若個案中的設備僅具備計費機能，

⁹⁷ 不同見解則認為此僅係行為人鬆弛機器設置者的持有效能後，再取走內容物的竊盜行為，參見蔡蕙芳，同註61，頁242-244。值得強調的是，匿名審稿人對於第三類手法似有不同意見，認為此項手法似乎不符合筆者對第339條之1不正方法的定義，然依筆者之見，只要行為人觸動的機制與收費有關，該手法就可認為是「致令收費設備程式判斷為已得到使用者提出之給付」，從而該當本罪手法，至若行為人觸動機制無關於收費設備時（例如以強暴手法打開集幣箱），則仍非本罪含括的不正方法。

⁹⁸ 至於該行為是否成立耗盡儲值卡價值的竊盜罪，另可參考許恒達，盜用存摺提款與不法所有意圖——評最高法院100年度台上字第3232號判決，月旦裁判時報，16期，頁59-70，2012年8月。Vgl. auch *Schnabel*, *Telefon-, Geld-Prepaid-Karte und Sparcard*, NStZ 2005, S. 18ff.

由於本文認為計費設備不能列入收費設備之列，故此種行為與第三三九條之一無關，其刑事責任應考量其他罪名。

三、付款設備詐欺罪

(一)付款設備的交易結構

有別於收費設備，付款設備的交易結構顯然不同。付款設備並不期待使用者先提出給付，而是要求使用者先出示身分憑證，確認使用者身分後，直接從付款設備交付款項予使用者或指定的第三人。從法律關係來看，設置付款設備的銀行與使用者之間，存有消費寄託的法律關係，銀行事先發給使用者特定的身分認證憑證（金融卡及密碼），並設置能夠辨識使用者身分的付款設備（自動櫃員機），使用者只要向付款設備提示身分認證資料，並經該設備判斷符合之後，付款設備即可核發款項，一般情況下，也將同時扣減銀行戶頭餘額。

在這個意義之下，向付款設備實施不正方法而得到財產利益的行為人，其侵害流程應該是：行為人先向付款設備提出身分認證資料，該身分認證資料足以通過付款設備的檢驗，使得付款設備「誤認」行為人是本人，或獲得本人授權的合法提款者，再將款項支付給行為人，然而行為人卻非真正獲得授權而可合法提款之人，毋寧是無權取款者。

基於上述我們可以認為，付款設備交易結構的重點在於，取款者利用付款設備判讀身分的盲點，假冒為合法取款者而獲得現金款項或移轉帳戶內餘額。相對於收費設備先由使用者提出給付，再由設備提供對待給付，付款關係則須事先有本人與銀行間的金錢寄託，銀行因存款而負返還價金給原所有人的義務，付款設備的交易重心，考量到銀行必須向正確的對象清償債務，整體結構當然特別

重視人別認證機能，在付款設備的交易過程中，雖然只透過卡片及密碼，以確認提款者是否為合法、適格之人，但這不表示銀行不關切取款者的身分；相反地，正因為付款過程涉及能否消滅原先的債權、債務關係，如果取款人不是存戶本人或本人委託之人，而是不正當取得或使用身分憑證者，銀行當然不願付款，這一點可見諸臨櫃取款時，取款人要提示存摺、印鑑（或簽名），還必須輸入取款密碼，而當原存戶以卡片至提款機取款，仍然必須透過密碼來保證存戶及銀行清償對象的同一性，透過這些身分認證手續，銀行在付款交易中，顯然極為重視人別的同一性。

學說上有從交易習慣及清償效果反駁上述看法，認為銀行不在乎自動櫃員機使用者的人別，其理由有二：1. 從交易常態來看，銀行既然授予卡片及密碼，表示銀行已概括同意持有卡片及密碼者皆有權提款，不論提款者是本人、本人授權之人，或是竊取卡片冒名提款者，只要使用真正卡片，並輸入正確密碼，銀行就許可提領款項⁹⁹；2. 若從清償效力觀察，依現行銀行交易實務及官方版定型化契約的規定：「未辦理掛失手續前而遭冒用，存款行已經付款者，視為對存款人已為給付。但存款行或其他自動化服務設備所屬金融機構對資訊系統之控管有未盡善良管理人注意義務，或有其他可歸責之事由，致存款人密碼被冒用或盜用者，仍應由存款行負責」¹⁰⁰，除非銀行行員或付款設備的身分判斷過程，違反了善良管理人的注意義務，否則銀行在本人未掛失卡片之前的付款行為，仍具有清償效力。換言之，卡片未掛失前，只要持有銀行核發的真

⁹⁹ 蔡聖偉，同註71，頁34-35。

¹⁰⁰ 參考新北市政府活期（儲蓄）存款契約附屬金融卡定型化約款範本，http://www.finance.ntpc.gov.tw/_file/1051/SG/42482/D.html，最後瀏覽日：2013年5月4日。

正卡片及正確密碼，就可以從自動櫃員機提款，銀行並不在乎提款者的身分人別¹⁰¹。

上述兩點反駁確實擲地有聲，但筆者容有不同看法。就交易慣習而言，雖然付款設備只依程式決定是否給付，使用者提出正確卡片及密碼後，付款設備就會給付款項，但這不表示付款交易無視本人的授權關係，析言之，如果只在乎身分憑證的正確性，不關切取款者有無合法授權，其實只要控制正確卡片資料，就可以馬上支付款項，之所以要求密碼，無非出於密碼具有極高的私密性，只有存戶本人及得到本人授權之人才能夠知悉，透過密碼可以管控提款者是本人或至少得到本人授權，密碼的存在毋寧表現整個交易結構中，銀行管控提款者身分關係的期待¹⁰²。

至於掛失前銀行除非有過失，否則不負風險一事，主要涉及民事法風險分配，但不能直接推論，銀行完全不在乎人別關係。相反地，在本人掛失前，只要卡片及密碼正確，該行為表示使用者是本人或至少得到本人授權，既然存在這麼一層默示意思表示，所以銀行才願意支付款項給使用者，收受款項者即便不是本人，但仍具有對本人清償同一效力；一旦卡片被掛失，表示本人已經明確告知銀行，他要切斷原卡片及密碼所揭露的身分認證效力，所以銀行接續的付款也不再具有清償效果。從上述關係中可以發現，持用真正卡片與正確密碼前往ATM提款的行為，揭露了付款設備使用者與本人的緊密關係，使用者透過密碼與卡片提示證明了這層緊密的連結屬性之後，付款設備才願意付款，一旦本人直接告知銀行，他要切斷關係，縱或卡片、密碼均為真實，嗣後也無法再從付款設備提取款項。倘依前述學說見解，付款設備不在乎人別，只關心卡片、密

¹⁰¹ 類似見解，參考黃榮堅，同註2，頁319；蔡聖偉，同註71，頁23-25。

¹⁰² Vgl. *Kindhäuser*, aaO. (Fn. 62), S. 301f.

碼的真實性，依本說見解，即便本人向銀行掛失，也不應該直接影響原卡片、密碼的取款效果。從上述對比我們可以注意到，掛失止付制度的存在，正清楚地表現出付款的前提有三：1.真正卡片、2.正確密碼，及3.使用者是存戶本人或得到本人授權，只不過1、2這兩個要素，在自動櫃員機的交易活動中，將以卡片、密碼等「明示」方法表現出來，透過1、2這兩個行為，即可在取款時「默示」表達出該使用者人別與授權關係的3.要素¹⁰³。

綜合上述，筆者認為付款設備與收費設備的交易結構並不相同，收費設備重視使用者與裝置設置者的給付／對待給付關係，但付款設備同時涉及銀行、本人及冒名使用者的三方關係，冒名領取他人存款者的侵害對象，通常不是位居中間角色的銀行，而是最終被領走款項的存戶本人。例如行為人竊得他人寫有密碼的金融卡，持之於銀行領取20,000元現鈔，由於行為人使用真正的卡片及密碼，銀行於審核人別過程並無過失，付款之後，在民法上已經盡了20,000元的清償責任，存戶本人即受到20,000元的財產損害。既然涉及到三方關係，自然必須確認人別身分或有無授權關係，付款設備自然也不是單純接受卡片及密碼資訊的機器而已。

由於付款的三前提中，1.真正卡片與2.正確密碼可以推論：3.

¹⁰³ 匿名審稿人指出：「在一般金融機構中，或許確實會有從業人員額外關注持卡人是否為本人、是否具領取權限，但在操作詐欺近似說時，用來替換自動付款設備的虛擬行員是否也具有這些關注，就會影響到是否該當不正方法。若沒有提出一個清楚的判準，恐會流於恣意。」（原文照刊），筆者的回應如下：審稿人提及的案例，涉及詐欺與付款設備詐欺等不同構成要件，其主要的問題，正是如何介分不處罰的動機錯誤與法益關係錯誤，在詐欺罪時，由於是人與人的交易，因此主要從交易目的觀察，小學生拿班費買玩具，這個目的與老闆的交易無關，是一個動機錯誤，相對於此，如果使用未獲授權的真卡領款，考量卡片用以證明有授權的事實，這就不能當作是付款設備詐欺的動機錯誤了。

使用者是存戶本人或得到本人授權，一般使用者只被要求揭露1.與2.等資訊，不必直接揭露3.，就可以合法地從付款設備領取款項。而要向付款機器進行詐騙，不正方法可能有兩種方式¹⁰⁴：

- (1)行為人使用偽造卡片，並使用正確的密碼。
- (2)行為人使用原卡片及正確密碼，但未得存戶本人授權。

第(1)種方法的行為人使用偽卡，通常未得本人授權，但行為人因為出示能通過身分認證程序的偽卡，又輸入正確密碼，因而默示表達他得到本人授權，可以合法提款，故屬於利用機器漏洞又違反交易結構的類似詐欺行為，屬於第三三九條之二的「不正方法」。

而第(2)種方式的行為人雖然提出1.+2.的真實資訊，符合付款設備程式預定要求，此時也同時默示地表達他符合3.的合法取款權限，但若其欠缺3.之本人授權，即可認定這是對付款設備詐欺的行為，構成第三三九條之二的「不正方法」。

整體而論，本條所稱的「不正方法」，應該從有無本人授權關係觀察，即便行為人提出真正卡片及正確密碼，但只要欠缺合法取款授權，仍屬本罪處罰的「不正方法」範圍。

(二)解釋「不正方法」的理論選擇

值得特別說明的是，解釋付款設備的「不正方法」屬性時，我國學說大多援引德國學理對其刑法第二六三a條第一項第三款的解釋觀點¹⁰⁵，其中共有四種不同看法：處分權人主觀意思說、取得來

¹⁰⁴ 相近見解，參考蔡蕙芳，同註81，頁61-64。

¹⁰⁵ 德國刑法第263a條的電腦詐欺罪第1項第3款，有極為近似的規定：「意圖為自己或第三人不法之所有，無權使用資料影響資料運算之結果，損害他人財產者」，由於行為人必須「無權」透過資料而影響電腦運算，進而造成不正當的財產變動，這樣的結構與第339條之2所謂以「不正方法」輸入卡片上資料至自動櫃員機，而造成不正當的財產變動，兩者的行為結構上幾乎相同，而

源說、設備使用規則說及詐欺近似說¹⁰⁶。其中筆者贊同詐欺近似說，分析理由如下：

1. 處分權人主觀意思說

處分權人主觀意思說從原財產所有人（付款設備的安裝銀行）角度立論，只要行為人擇用手段不符合設備裝置者（銀行）主觀意思，就認定為不正方法¹⁰⁷。本說最大問題正是過度擴張銀行主觀意思的法律效果，當銀行透過設備而建制出一套取款流程，是否不正攻擊，理應從有無濫用流程缺陷的觀點切入分析，本說顯然無視這種形式化且程式化的銀行交易機制，回歸到真正的銀行意思，如此一來，任何不符合銀行期待的付款行為，都會直接納入不正方法的保護範圍，顯然不無處罰過廣的疑慮¹⁰⁸。

此外，採用本說將使得銀行意思成為成罪與否的關鍵，而銀行為了透過銀行迴避損害及風險，必然會採用成罪範圍最大的解釋立場，只要在與存戶的契約中禁止第三人使用卡片提款¹⁰⁹，無論該

描述法定犯行的用語「無權」及「不正方法」，又均屬較為模糊的概念，因此即可從德國學說掌握「無權」的類型及觀點，反思何謂「不正方法」。

Dazu vgl. *Rengier*, aaO. (Fn. 14), § 14 Rn. 10-14; *SK-Hoyer*, 8. Aufl., 2011, § 263a Rn. 14-21; *Kindhäuser*, *Strafrecht Besonderer Teil 2*, 5. Aufl., 2008, § 28 Rn. 23-25; *Scheffler/Dressel*, „Unbefugtes“ Verwenden von Daten beim Computerbetrug, *NJW* 2000, S. 2465f.; *Ranft*, aaO. (Fn. 62), S. 2574ff.

¹⁰⁶ 學說名稱參考蔡聖偉，同註71，頁21-29，另見*Otto*, *Probleme des Computerbetrugs*, *Jura* 1993, S. 613ff.

¹⁰⁷ 我國學說亦有支持者，參見盧映潔，不拿白不拿？，*月旦法學教室*，77期，頁24-25，2009年3月。Vgl. auch *Kindhäuser*, aaO. (Fn. 62), S. 294-297.

¹⁰⁸ 學說上有認為，採取主觀解釋將使得本罪變為一種背信刑責（vgl. *Achenbach*, aaO. (Fn. 63), S. 227），不過誠如蔡聖偉教授所見（蔡聖偉，同註71，頁25-26），這個批評並不到位，因為背信罪以負有特別財產照料義務的行為人為成罪前提，然而違反第339條之2者，倒不必然具有此一身分。

¹⁰⁹ 提款卡使用規則有幾種常見要求，整理見蔡蕙芳，同註81，頁56。

第三人與存戶間有無合法授權，任何非本人的提款行為都可能成立刑事責任，這顯然不是自動櫃員機提供方便金融交易的初衷¹¹⁰，也將第三三九條之二理解為銀行交易安全的保障條文，筆者認為並不適合。

2. 取得來源說

取得來源說則認為，只有取得過程合法的卡片才能合法使用，倘若取得過程違法，事後的使用取款行為也必然屬於不正方法¹¹¹。此說以提款的前行為作基準，決定取款本身的合法性，雖然不法取得的卡片幾乎不可能合法使用，本說某程度上可以得到尚稱合理的結論，但實則忽視了一個重點，倘若行為人合法取得卡片、密碼，是否一定有合法取款權限？常見適例即有管理卡片權限的行為人，未得公司或本人授權而盜領其存戶金額。論者或許認為，這類行為人僅違反內部授權，不應動用刑法處罰，不過依筆者之見，第三三九條之二正是利用電腦程式的設計漏洞而詐領款項，不論偷他人卡片而取款，以及越權使用卡片取款的行為人，都是利用電腦程序無法判讀其授權關係的既有缺陷，縱然兩者的前行為有明確差別，但後行為利用電腦程序瑕疵而盜領的舉措，不論是無權或越權使用卡片，都實現了同樣結構的財產侵犯¹¹²，既然前、後兩行為可以切割，不論合法或非法的前行為，均無關於後行為的侵害後果，本說即不可採。

3. 設備使用規則說

另一見解是我國學說上獲得相當支持的設備使用規則說

¹¹⁰ 相同意見，參考蔡聖偉，同註71，頁26。

¹¹¹ 支持本說見解，參考Cramer/Perron, in: Schönke-Schröder, 28. Aufl., 2010 § 263a Rn. 10. (不過該註釋條文認為自己持詐欺近似說)。另有關於本說的詳細討論，vgl. NK-StGB-Kindhäuser, § 263a Rn. 23.

¹¹² 參考蔡聖偉，同註71，頁28-29。

(Computerspezifische Auslegung)¹¹³，本說認為使用銀行發行的合法卡片取款，即非不正方法，越權使用或不法取得卡片後的使用行為，均非不正方法，僅當使用非銀行授權的偽造卡片，方屬不正方法¹¹⁴。

設備使用規則說是最符合電腦特質的見解，僅當行為人使用偽造資料，使電腦誤為以是真正資料時，才構成不正方法，然而，筆者認為仍有若干解釋問題。從成罪範圍而言，本說見解必然使得本罪大幅限縮，僅當使用偽造卡片才有可能成立刑責，這個解釋勢必將本罪理解為行使偽造文書的特別規定，卻完全忽視本罪的財產犯罪特質。

此外，當行為人先以不法前行為取得他人真正的卡片及密碼後，再持之取款，其前行為只侵害卡片本身的所有利益，但後階段取款行為卻損害了卡片對應的帳戶款項，已經造成新的法益損害，採用本說解釋，後階段的行為將完全不罰，這顯然是一個處罰機制的漏洞¹¹⁵。

本說核心論點認為，銀行只在乎卡片、密碼是否為真，不關切使用者與存戶之間的內部關係，上述觀點的問題是：使用偽造卡片及密碼，而能夠拿到付款設備使用而領取款項的前提，仍須卡片足以對應到某存戶帳號，否則仍然不可能提款或轉出餘額，之所以要處罰持用偽卡取款的行為，恐怕不是因為銀行不許可偽卡本身的使用，而是因為偽卡連結特定帳戶，使用偽卡盜領款項，將致令帳戶所有人在不知情的狀況下，因被盜領款項而蒙受財產損害；既然重

¹¹³ 黃榮堅，同註2，頁318-319；李聖傑，溢領借款的詐欺——評台北地院92年度自字第17號判決，月旦法學雜誌，120期，頁224-225，2005年5月；蔡聖偉，同註71，頁31。

¹¹⁴ Neumann, aaO. (Fn. 62), S. 537.

¹¹⁵ 相似批評，林東茂，同註59，頁2-160，auch vgl. Otto, aaO. (Fn. 106), S. 614.

心是偽卡連結的帳戶關係，卡片是否為偽造即非重點，關鍵毋寧是帳戶所有人未許可他人使用其取款渠道，卻被盜用而受到損害的過程與結果。

本說能夠解釋真正／偽造提款卡的問題，但本說無法解決所有盜用帳戶的問題，倘若銀行不透過卡片，而以帳號、密碼實行身分確認機制（例如現行實務上的網路銀行），因為密碼只有正確與否，沒有偽造、變造的問題，若採本說必然導出所有無權使用帳號、密碼者都是第三三九條之二有權之人，這種結果顯然不能完全接受。

綜上討論，設備使用規則說過度從形式角度立論，因為銀行提供ATM的取款服務，正是讓存戶更加方便管控其帳戶，即使卡片、密碼類似管理帳戶的鑰匙功能，但不代表任何持有正確鑰匙者，就可以管控帳戶，舉例而言，假設小偷拾獲被害住家的真正鑰匙，持有而進入被害人家中，我們不會因為小偷拿的是「真正鑰匙」，就排除第三〇六條侵入住居的刑事責任。質言之，本說無異過度緊縮成罪界限，使得無權盜用他人卡片而取款者不受刑事制裁，這樣的結果似乎悖離了本罪規範目的。

4. 詐欺近似說

依筆者之見，較合理的見解其實是詐欺近似說（*täuschungsäquivalente od. -nahe Auslegung*），本說認為，應該本於第三三九條之二的詐欺屬性解釋不正方法，實際操作重心在於將電腦設備代換為行員，只要行員同樣因行為人出示的身分認證資料而陷於錯誤，即可認為是不正方法¹¹⁶，更精確地說，行為人默示意思表示才是不正方法的判定關鍵，只要行為人出示能使用的卡片及正確密碼，

¹¹⁶ Lackner, aaO. (Fn. 13), S. 52; Ranft, aaO. (Fn. 62), S. 2574; Lackner/Kühl, aaO. (Fn. 66), § 263a Rn. 13.

就表達了他得到本人授權而可以合法取款的默示意思，礙於電腦（或假設代換的銀行行員）無從檢證行為人表達的默示意思是否存在，屬於交易技術上無法克服的瓶頸，行為人利用該項技術瓶頸而取款，即屬本罪的不正方法¹¹⁷。

不過，學理上也對本說提出若干質疑，主要批評有二：首先，電腦詐欺其實是利用設備及程序的設計瑕疵而取得不法利益，既然是利用設備瑕疵而不是利用相對人認知錯誤，先天上本來就不可能構成詐欺，又如何能夠以「類似詐欺」的角度來理解構成要件行為？¹¹⁸甚而，設備只依程式運作，不可能理解默示意思表示，從違反默示意思表示而說明存在類似詐欺的關係，不免是過度強加詐欺罪的解釋於電腦犯罪之上¹¹⁹。最後，針對越權提款的案例型態，本說主張者也往往有不同結論，其理論構成的一致性難保無誤¹²⁰。

對於上述批評，我們或可先從政策角度思考，現代經濟交易不再以人際關係的信賴為前提，而是建立在交易者提出有用的憑證，證明自己的人格、信用或給付能力，這些憑證只能擔保在絕大多數情況下，交易者滿足其所宣稱的交易條件，但不可能百分之百管控條件是否滿足，如果要求交易絕對符合所有宣稱條件，絕對無任何風險，我們只能回歸至早期建立在人際信賴的交易形態，然而這已經不再可能。自動櫃員機正是現代交易的適例，透過銀行發出的卡片與密碼，存戶不再需要直接臨櫃交易，固然卡片與密碼無從百分

¹¹⁷ NK-Kindhäuser, § 263a Rn. 25.

¹¹⁸ Ranft, aaO. (Fn. 62), S. 2574-2575; Mitsch, aaO. (Fn. 13), § 3 Rn. 22.

¹¹⁹ 批評參考NK-Kindhäuser, § 263a Rn. 26; Neumann, aaO. (Fn. 62), S. 537; Hilgendorf, Scheckkartenmissbrauch und Computerbetrug – OLG Düsseldorf, NStZ-RR 1998, 137, JuS 1999, S. 543.

¹²⁰ 尤見蔡聖偉，同註71，頁24。

之百保證存戶本人意思，但透過卡片的持有與個人設定的密碼，基本上已經能夠管控絕大多數情況，至於那些無法完全控管的少數情況，則是刑法必須介入管制的範疇，倘若有人利用這種交易上無法究極確認的缺點獲利，刑法即須介入干預，質言之，正因付款設備只能判讀「憑證所揭露交易條件」，在交易過程中，我們必須接受該條件滿足時，即可推定「真正交易條件」也已滿足，如果行為人利用兩者間的落差犯罪而取得財產，自應由刑法介入干預、處罰。

至於釋義學層次，筆者認為尚未能全面地推翻詐欺近似說。固然設備或機器不會陷於類似詐欺的錯誤，但這不表示我們不能採用詐欺觀點來進行解釋，正因為機器只有技術缺陷，所以我們才說這是「類似」詐欺，而不是真正的詐欺；而所謂機器不能接受默示意思表示的看法，接收使用者提出默示表示的對象是銀行而不是機器，只不過銀行不派行員在中間督查並接收該默示表示，毋寧透過特定程式，依據程序提供的形式功能接收憑證，以及憑證揭露的默示意思，此一批評並未打到痛處；最後是標準浮動的問題，筆者認為，只要能夠從交易結構清楚地分析默示意思的內容，就可以穩定其判斷標準。綜言之，上述批評似乎不足以成為反對類似詐欺說的理由，故筆者仍認同本說見解。

(三)付款設備的定義及範圍

接著討論付款設備的範圍。相對於收費設備態樣繁雜，付款設備涉及金融機構與存戶間的關係，銀行能夠提供的付款機制受有相當限制，態樣上較不多樣化。

從條文文字觀察，立法者設計第三三九條之二時，應該只想像了設置在公開場所的實體櫃員機，以及透過實體櫃員機進行的取款（第一項）、轉帳（第二項）等金融交易，都可以認為是付款設備的服務範圍，而一般狀況下，實體櫃員機提供取款服務時，取款者

是消費寄託契約的債權人，取款乃基於該契約向銀行請求返還寄放於銀行戶頭的款項。

不過隨著金融市場高度發展，資金活用的需求增加，銀行逐步開放讓未在銀行存放款項的客戶，也可以使用現金卡或信用卡，透過自動櫃員機向銀行借款，這類交易雖然不是典型實現消費寄託債權的取款行為，使用者不是「實現債權」，而是利用自動櫃員機向銀行借用款項而負擔債務，但民事法律關係的差異，仍不妨害使用者從自動櫃員機「取款」的事實，我國實務也採取同樣看法，使用者縱然屬於現金卡或信用卡借款，只要經由實體的自動櫃員機，均可納入本條所稱的付款設備範圍，此說可茲贊同。

同樣的道理，在網路及電信時代來臨後，付款設備已經不僅是裝設於重要場所的實體型付款設備，我們可以想像到的可能包括早期發展的電話語音轉帳設備，以及近期廣受使用的網路ATM與網路銀行，這些非實體性的金融服務機制，都與實體的自動櫃員機功能雷同，問題是：若行為人透過不需使用卡片的網路銀行，無權輸入密碼或資料，從而轉帳至自己或第三人的帳戶時，或是盜用他人卡片並輸入他人密碼，利用網路ATM將他人帳戶內餘額轉給自己，行為人是否構成第三三九條之二的犯罪？

從第三三九條之二的條文看來，其實未將成罪範圍限於「實體」櫃員機，毋寧有付款機能的設備或連線電腦，都屬於該條規範對象。事實上，實體櫃員機僅專為處理個人消費金融業務而設計、安裝於特定場所的連線電腦，該設備與網路上的連線設備，幾乎沒有什麼不同之處，甚而，第三三九條之二也未限制一定要有卡片，行為人同樣可以使用密碼或銀行規定的認證方式登入銀行系統，辦理金融業務，與卡片相同，這些認證方式設計的目的，也是判斷是否具有給付對象的同一性，只要行為人形式上能提出通過認證的密碼或資料，但實質上卻非銀行預期的給付對象，就可以認定為該罪

的不正方法。

基於上述，就語音轉帳系統而論，其特點是行為人撥電話到銀行，輸入預先設定或由銀行亂數指定號碼表中的密碼，之後就可以透過電話委託銀行將銀行存款轉至他人戶頭，交易過程中並無真正的行員協助代辦，而是全由電話撥碼下指令給銀行伺服器。如果行為人先無權取得他人語音密碼，再透過語音轉帳機制，將他人存款轉至自己戶頭時，因為案例中並未出現付款設備的實機，整個轉帳流程是建構在電信機制上時，就有能否成立第三三九條之二的爭議，實務若干見解支持第三三九條之二，但也有部分見解主張不成立第三三九條之二，只能構成第三三九條之三。依本文之見，上述電話交易的過程，其實與實體櫃員機的交易機制差異不大，同樣都先辨別身分，再提供轉帳的金融服務，不能僅因使用者看不到安裝在銀行中心伺服器中的大型實機，而採取否定說，我們實無任何理由否認語音轉帳屬於付款設備。

此外，今日流行的網路銀行及網路ATM交易建制，同樣只是沒有實體的自動櫃員機，也沒有辦法直接領取現款，其交易機制與實機完全相同，使用者必須透過自己的網路連絡至銀行中央伺服器，待確認人別關係後，再進行轉帳交易，這些形態的交易媒介沒有理由外於第三三九條之二的管制範圍。

綜上討論，筆者認為電話語音銀行、網路ATM及網路銀行均為本條規定的付款設備。

(四) 檢討具體案例

前文已經提過，筆者主張從類似詐欺說理解第三三九條之二的
不正方法內容，接著就以實務及學理上曾出現過的具體案例，說明

對不正方法的理解方向¹²¹。

1. 使用偽造卡片提款

第一類案例最沒爭議，行為人先偽造內容與真正卡片相同的偽卡，再持之前往銀行取款，由於偽卡的使用未得本人或銀行同意，卻又能通過付款設備的審核機制，符合本文對不正方法的定義，行為人成立本罪¹²²。

不過，這一類可能出現較為一種特殊的想像案例，此即帳戶所有人遺失卡片後，卻未向銀行掛失，而是自行偽造卡片，持用至自動櫃員機領取款項。姑且不論帳戶所有人可能成立偽造文書的罪名，單就第三三九條之二的「不正方法」而言，行為人使用雖未得銀行授權，但本身是帳戶所有人而領取其所有款項，行為人使用卡片與密碼，同時默示表達出「本人取款」的真正意思，依本文見解屬於完全合乎帳戶使用規則的作法，並非不正方法，故不成立第三三九條之二刑責¹²³。

2. 不法取得他人卡片提款

第二類案例則是不法前行為後的盜領行為，例如行為人竊盜、搶奪、強盜、侵占卡片後，再使用該不法取得的真卡，並輸入正確密碼取款，依本文之見，雖然行為人提出的卡片及密碼均屬實，但該行為的默示意示牴觸了帳戶所有人意思，故應認為是不正方法¹²⁴，我國實務均採此一見解，可茲贊同¹²⁵。

¹²¹ 類型化的討論方條，亦可參考蔡蕙芳，同註1，頁55-64。

¹²² 此為我國通說見解，參見黃榮堅，同註2，頁317-319；蔡聖偉，同註71，頁31；蔡蕙芳，同註81，頁63；甘添貴，自動付款設備詐欺罪之不正方法，月旦法學教室，39期，頁23，2006年1月。

¹²³ 此一案例依處分人主觀說、取得來源說或設備規則說，均為不正方法，僅依詐欺類似說不構成不正方法。

¹²⁴ 本例依處分人主觀意思說、取得來源說及詐欺類似說，均為不正方法，但依

3. 卡片保管者越權提款

第三類是違反內部授權溢領款項的事例，通常情況是行為人受帳戶所有人之託保管卡片及密碼，卻違反所託，未獲許可自帳戶提領款項，或越權溢領款項，行為人本來就是合法的卡片、密碼持有者，其盜領行為屬於違反內部授權。依本文見解，縱然行為人持用真正卡片及密碼取款，但其盜領行為揭示已獲本人授權的默示意思，但實際上卻未獲本人授權，屬於利用付款設備無從判斷的設計缺陷而取款的行為，故應認定為不正方法¹²⁶。

4. 利用設備故障溢領款項

第四類則是利用機器發生錯誤而取款的特別事例，例如行為人一開始使用自己所有的真正卡片，於自動櫃員機領取1,000元，未料機器吐出5,000元，行為人食髓知味後，繼續以同一方法五次溢領現金共20,000元¹²⁷。這個案例中要分幾個階段觀察，行為人第一次多領得4,000元，是付款設備單純溢付款項，與行為人無關，不成立第三三九條之二刑責¹²⁸，不過之後五次的溢領行為，行為人

設備使用規則說分析此類型案例，則行為人盜用真卡，仍不成立第339條之2罪名。但本文認為此一結論並不合理，詳參前文討論。

¹²⁵ 我國實務見解的整理，參見陳子平，自動付款設備詐欺罪，月旦法學教室，53期，頁68-73，2007年3月。

¹²⁶ 本例依處分人主觀意思說屬於不正方法，依據詐欺類似說則有爭議，但設備使用規則說及取得來源說則非不正方法，不成立刑責。

¹²⁷ 相關案例討論，參考盧映潔，同註107，頁24。

¹²⁸ 至於行為人自行取走溢付的4,000元，是否另行構成刑責？向來學說均主張構成刑法第337條的侵占遺失物罪（例如盧映潔，同註107，頁25），不過筆者對此一結論容有不同看法，自動櫃員機本身的設置目的即在符合條件下交付現款，任何透過機器程式而交付的款項，即已移轉所有權予使用者，如果可以接受此一結論，我們沒有理由認為行為人不是民法上的所有權人，換言之，這4,000元已然透過ATM的交付而移轉所有權了，行為人縱然花掉，也只是消費自己所有的金錢，稱不上侵占他人所有財物，故可考慮認為行為人不

則已完全知悉付款設備瑕疵，卻仍利用既有瑕疵而溢領款項，該行為是否成立第三三九條之二即有待檢討。

認為行為人後階段行為成立第三三九條之二不正方法的理由在於：行為人明知系統缺陷，卻又利用該缺陷溢領款項，該行為違反銀行設置提款機的用意¹²⁹。然而筆者有不同的看法，以銀行的最終意願判斷不正方法，此即前文提過的處分權人主觀意思說，此一見解過度擴大銀行最終意願的刑法機能，使用者之所以能溢領款項，完全因為銀行自己設置提款機時的重大瑕疵，如果還要苛責行為人，顯然讓設備出問題的銀行完全不負責風險，而從一般交易過程來看，這種重大瑕疵已然超出一般銀行不必承擔風險的範圍，理應由銀行自負其責，不能怪罪使用者，以銀行最終局意願決定不正方法，只不過抬出一個未曾在交易結構中真正出現的銀行意思，甚而滿足銀行想要營利又想要卸責的不合理期待而已。

至於行為人明知的問題，筆者認為主觀上的明確認知，仍不足以作為改變客觀構成要件行為認定標準的理由，即便行為人在後階段明知付款設備的重大瑕疵，但從行為人本來就是合法存戶，也提出正確密碼，更在提款時表明只提領自己戶頭內的1,000元餘額，行為人的取款行為的默示意思表示，並未違反實情，客觀上屬於完全合法的行為，理論上非不正行為，如果僅因其主觀知悉設備已經故障，就要轉認為不正方法，不免過度強化主觀惡性。基此筆者主張，行為人尚無類似詐欺的不法侵害行為，不構成第三三九條之二

成立任何刑責，但銀行仍然對行為人有民事請求權。此一問題仍須對於侵占罪與所有權的關係進行更深入的研究，遠非本文所能完成，未來將另撰文討論。

¹²⁹ 參考盧映潔，同註107，頁25。本案似為真實個案，但因被告之一為未成年人，未予公開，僅能見諸媒體報導：<http://www.libertytimes.com.tw/2008/new/nov/14/today-so5.htm>，最後瀏覽日：2013年5月3日。

的不正方法¹³⁰。

5. 利用現金卡溢借款項

第五類案例是現金卡，現金卡的持卡人可以使用卡片，在自動櫃員機依銀行授權額度借款，不過近期以來，因銀行緊縮授信而較少出現與現金卡有關的溢借問題。具體案例則是：行為人先合法取得預借額度僅50,000元的現金卡，使用現金卡於自動櫃員機借款50,000元，嗣後恰巧發現銀行連線系統故障，該預借額度失準，行為人遂再使用現金卡預借數次，總額合計250萬餘元，借得金錢後即予消費，而因行為人無資力返還而被銀行提出告訴¹³¹。

此一案例中，行為人自始使用銀行核發的真正現金卡，沒有偽造文書的問題，行為人又是現金卡的持卡人，可依卡片享受銀行提供的金融服務，而行為人又無任何管照、監護義務，唯一能討論的罪名只有刑法第三三九條之二，問題即在明知無資力償還卻又使用現金卡預借款項的行為，是否算是不正方法？實務很快地認為，明知無資力而仍預借款項算是不正方法，但學說則有引用設備規則說的見解，認為本案應不成立不正方法而無罪¹³²。就這兩說而言，本文贊同學說意見的結論，不過理由構成上，筆者則有不同意見。

銀行發行現金卡，鼓勵客戶向銀行小額貸款，無非為了賺取利息收入，這是銀行商業行為，但以授信方式投資以獲利，銀行也要承擔可能無法收回借款的風險，當銀行許可特定客戶使用現金卡，

¹³⁰ 前文提到的四說中，只有依最寬泛的處分人主觀意思說才能認定本案滿足不正方法，另外三說均不成立不正方法。

¹³¹ 本案為臺北地方法院92年度自字第17號判決，相關評釋參見李聖傑，同註113，頁219-228。德國學說雖無完全相同的案例，但就越權溢領或溢借款項的問題，亦有持設置者主觀說而成立電腦詐欺的見解，vgl. *Kindhäuser*, aaO. (Fn. 62), S. 303f.

¹³² 參見李聖傑，同註113，頁224-227。

已經表示在該現金卡的借款上限額度內，銀行願意自行擔負客戶欠款致無法追償的風險，即使客戶明知未來可能無力償還，仍使用現金卡透過自動櫃員機借款，考量整個交易過程中，銀行明知其授信風險，即便客戶預期自己無從償還，也應該由銀行在授信之前進行風險評估，不應由客戶承擔其管控責任，該使用現金卡在ATM預借額度內現金，卻因可歸責銀行瑕疵而溢借的客戶，仍非不正方法。

除此之外，上例還涉及與第四種案例型類似的問題，此即行為人已知付款設備故障，故意利用設備瑕疵而溢借款項，與前例相同，當銀行自行安裝的付款設備本身出現瑕疵，使用者因而可以取得超出原定額度內的款項，一來使用者自始輸入符合授權且內容真實的人身憑證，二來這理應是銀行自負的設備風險瑕疵，即便行為人明知，但考量這種主觀明知顯然不同於濫用設備的客觀瑕疵，故仍不足以作為行為人構成不正方法的實質理由。綜上，筆者認為本例行為人不構成第三三九條之二不正方法，本案僅涉及民事關係。

6. 盜用帳戶密碼使用網路銀行或語音銀行

另一類常見的案例與卡片無關，主要涉及無權使用他人帳號密碼，而在網路或語音銀行進行轉帳交易，從而損害原有帳戶所有人的財產利益。

就此類型案例，近期實務逐漸傾向認為網路或語音銀行不是付款設備，因此轉以第三三九條之三論斷刑責，這一點已如前文所述，付款設備不必以實體機器為前提，即便透過電信或網路連線達成的轉帳機制，也可以認為是付款設備；此外，當使用者透過語音或連線輸入密碼時，其實默示表達他是合法使用者，只要實際上未得本人授權，依本文主張見解，自屬不正方法。

四、不正使用電腦詐欺罪

(一)變更財產權紀錄的交易結構？

前文已經檢討過第三三九條之一及之二等規定，兩則條文均明確限制行為客體（收費或付款功能）屬性，雖然法定犯行語焉不詳，但至少侵害客體的交易結構提供了考量基點，也因此筆者才強調，第三三九條之一重在使用者提供真實的財產給付，而第三三九條之二則關切使用者與存戶本人的同一或授權關係，只要使用者提出的給付或資料符合這些「形式」標準，就可推定「實質」符合交易條件，設備即許可交付財物或利益予使用者，但設備有其先天缺點，只能從形式條件推定實質條件的滿足，但無從確認實質給付或資料真實性的固有障礙，當行為人利用設備對交易條件的審查缺陷而取得財產，此即第三三九條之一及第三三九條之二的「不正方法」。

雖然是同期立法產物，也規定在同一罪章，但第三三九條之三則與前兩條有極多差異，最主要的區別有二：第一，依第三三九條之三的規定，行為人必須先在電腦或相關設備上，輸入內容不實或干擾正常功能的資料或指令，造成電腦資料處理過程不符合實際的民事財產秩序，並出現錯誤財產權紀錄的中間結果，最後引起財產關係不合理變動的財產損害¹³³，與前兩條比對，第三三九條之三只規定損害流程的進展方式，卻未明確規定侵害客體，任何符合第三三九條之三所定流程的事實，均可納入規範範圍，問題是：與電腦相關的財產權紀錄種類繁多（銀行存款紀錄、以電腦記載的買賣紀錄），只要稍微與財產關係沾上邊，甚而間接地影響他人現有或未來財產，某程度上均可認為是關涉財產權紀錄的電腦資料。舉例來說，假設房屋租約並無紙本，僅有電腦的word檔，當出租人趁承

¹³³ 就此參考蔡蕙芳，同註41，頁72-74。

租人不注意，篡改word檔上的租金數額，雖然不會馬上發生現有財產的變動，但勢必影響未來財產的分配關係，理論上也可算是財產權的電腦紀錄；此外，條文規定了輸入虛偽資料與不正指令兩種侵害手法，所謂虛偽資料顯然指「記載內容」不符事實的資料，但這種從內容定性的取徑，勢必導出任何未獲授權的輸入行為，都可以認定為虛偽資料，而不正指令更無從其文字描述掌握「不正」的界限，而再考量現代科技的發展，影響財產權紀錄正確的輸入資料或指令手法不勝枚舉，舉凡經理故意變更存戶餘額、駭客侵入銀行電腦變更餘額、使用者輸入假資料等行為，這些不同法律意義的侵害手法¹³⁴，都可算是輸入虛偽資料或不正指令，立法者選用這一類的規範取向，其結果必然是無從明確限定可罰行為。立法文字的模糊，再加上侵害方式與侵害中間結果的多樣性，必然難以定性第三三九條之三的成罪界限¹³⁵。

其次，第三三九條之三也沒有明確的交易結構可供參酌。不同於前兩條，行為人須向設備提供符合交易結構的財產對價或人別訊息，作為電腦處分財產的判斷憑據。然而，第三三九條之三只強調行為人必須輸入電腦資料或指令，藉以影響紀錄正確性，但其輸入資料並非電腦處分財物或利益的對價或給付前提，而中間結果的財產權紀錄變動，其本身對於設備作成的財產處分有何機能，也無法從法條中得知。正因為條文欠缺交易結構的預想，倘若行為人先侵入銀行伺服器，在伺服器中植入扣減存戶餘額尾款，並轉移至行為人指定帳戶的木馬程式，致使行為人帳戶餘額增加，本案行為人縱

¹³⁴ 經理利用內部授權機會變更存戶額款，類似透過電腦實行的背信行為；侵入電腦後修改他人帳戶餘額，則是侵入電腦罪的後階段損害；使用者輸入虛偽資料，則又與第339條之1及之2相似。這些罪質有明顯差異的犯行方法，都可以透過第339條之3的文字共同含括於處罰界限之內。

¹³⁵ 不同見解，參考蔡蕙芳，同註41，頁77-78。

然輸入電腦的資訊是木馬程式，該程式只可影響伺服器運作正確性，是一種介入電腦機能的干擾行為，並非任何財產交易的前提，也與轉帳給行為人的對待給付或交易結構無關，但仍可以成立本罪；相反於此，當便利商店的店長透過電腦程式，提供虛偽的信用卡繳費紀錄，藉以賺取交易手續費時，店長的虛偽資料卻又與銀行的手續費給付具有對價關係，其犯行又涉及交易結構上的詐欺。從這兩宗案例可以發現，第三三九條之三可以涉及電腦系統的交易結構，但同時又一併處罰無關交易結構的案例，這也使得我們在解釋第三三九條之三時，不能援用前述條文以交易結構為中心的解釋策略。

綜合上述，第三三九條之三既無特定侵害對象與侵害流程，又不存在獨立受到管制的交易結構，我們無從透過交易結構的解釋技法，明確劃清條文期待的可罰與不可罰界限。因此，筆者認為要解釋第三三九條之三，只能依循三重解釋策略：

第一，本罪是唯一將「電腦或其相關設備」寫入條文的罪名，涉及本罪的行為，原則上必須是濫用電腦處理資料的特性，但不包括對於機械式設備的侵害手法，亦即，行為人僅限利用電腦處理資料特性而侵害財產。

第二，既然交易結構與明確的侵害流程難以掌握，解釋上，只能透過因果關聯性的具體操作限定成罪範圍，要求每一個構成要件要素之間，具有前後的明確因果連結，當行為人不正輸入資料或指令後，必須直接製作財產權得喪變更的紀錄，該紀錄一旦作成，將直接透過電腦程式傳導與連結，作成不正當財產給付，實現財產損害，原則上這個過程必須完全由電腦運作，不得有人為介入審查、核可的空間。

第三，即便第三三九條之三條文極為空泛且一般，但這不代表完全無法建立處罰的明確類型，相反地，正因為條文空泛，設法統

整各種成罪型態的共通點，才能歸納出可能成罪的方式。前文曾經提過，實務在第三三九條之三大致處罰三種不同態樣：管理權限濫用型、侵入電腦型及資料操縱型，筆者認為透過這三種不同的成罪態樣，或可歸納出第三三九條之三的類型譜，從而畫出本罪適用準線。

以下討論，就接續著本文提出的三重解釋策略進行分析，首先分析第三三九條之三的構成要件個別要素，說明如何判定其具體內容，以及如何確認各要素間的因果關聯，接著再以三種類型為中心，具體探討各類成罪形態。

(二)構成要件的解釋與因果連結

1. 法定犯行的定性

先談本罪的構成要件行為，立法者要求行為人必須以不正方法，輸入虛偽資料或不正指令才能成立犯罪，單從文字而言，「不正方法」及「輸入虛偽資料或不正指令」同時描述了犯罪行為，然而「輸入虛偽資料或不正指令」本來就是不正方法，甚而更具體、明確地限定成立侵害方式，不正方法反而沒有什麼直接的定性功能，如果要認為兩者不同，也難以想像有什麼是「輸入虛偽資料，但非不正方法」而不成立犯罪的情況，我國多數見解因此認為，本罪關鍵性犯行內容其實是「輸入虛偽資料或不正指令」，或者可以統括為不正輸入資料的行為¹³⁶，此說應可贊同。

換言之，第三三九條之三的不正方法，指的就是接續的「輸入虛偽資料或不正指令」，本罪的解釋重點應非不正方法的定性，而是什麼是條文所稱的「資料」與「指令」，以及什麼樣的資料稱得

¹³⁶ 黃榮堅，同註2，頁320；林東茂，同註59，頁2-160；蔡蕙芳，同註41，頁71-79。

上「虛偽」，什麼樣的指令才算是「不正」？

在討論「虛偽」與「不正」的概念前，筆者要先強調，由於虛偽資料或不正指令是輸入到電腦或相關設備，因此這裡所稱的資料或指令，必須與電腦處理資料的特性有關，不能是單純文書資料；至於資料與指令兩者有無區別。依我國多數意見，原則上應該認為資料是直接與人別、財產所有關係，或債權債務相關的電腦資訊，例如存戶姓名、帳戶金錢餘額，或有無特定的財產請求權等，而指令則是其他與程序或執行網路平臺有關係的電腦訊息¹³⁷，此說應該贊同。

至於資料的「虛偽性」，學理曾有借鏡德國刑法第二六三a條第二種行為方法的解釋，認為所謂虛偽資料即德國條文的「不正確之資料」（*unrichtige Daten*），該資料指其內容違反客觀事實¹³⁸，依上述德國學說解釋，倘若行為人無權使用他人密碼，因密碼是正確資料，但被行為人無權使用（*unbefugte Verwendung*），仍不算是「不正確之資料」。此項見解雖然源自德國法，同時也與我國條文有相當契合關係，不過筆者認為第三三九條之三不適合此一解釋，此因德國刑法第二六三a條同時規定兩種不同行為手段：「使用不正確資料」（*Verwendung unrichtiger Daten*）及「無權使用資料」（*unbefugte Verwendung von Daten*），上述所謂無權使用他人資料的行為方法，必須擇納至另一種構成要件行為，所以德國學理才會認為，無權使用他人資料不算是「不正確資料」¹³⁹，然而我國並

¹³⁷ 蔡蕙芳教授正確指出，虛偽資料涉及「資料操縱」，而不正指令與「程式操縱」有關，參見蔡蕙芳，同註41，頁75、78。

¹³⁸ *Kindhäuser*, aaO. (Fn. 105), § 28 Rn. 13; *Maurch/Schroeder/Maiwald*, aaO. (Fn. 14), § 41 Rn. 237.

¹³⁹ Vgl. *Kratz*, aaO. (Fn. 13), S. 40f.

未有此一區別，德國學說似乎不能直接用以解釋我國法¹⁴⁰。

依筆者之見，資料「虛偽性」仍應從資料內容是否與財產交易及分配秩序相同觀察，只要輸入電腦資料不符合財產客觀狀況，就應該認為是虛偽資料，想像上可能有兩種情況：(1)資料本身純粹反應既已實現的交易狀態，而間接與行為人想要侵害的財產有關，例如便利商店店長提供虛偽的卡費繳納紀錄，向銀行申請手續費，銀行給付手續費是以已經存在的繳費交易為前提，當客觀不存在任何繳費交易時，但行為人提出的電腦資料卻又顯示有繳費交易，此時即屬不符合客觀既生實情的虛偽資料¹⁴¹；(2)資料本身關涉未來交易，而行為人未得本人授權，假冒本人之名提出交易請求，這一類虛偽資料特點在於，行為人提出資料後，將使得本人或交易相對人現有的財產狀態產生貶損，由於本人未曾許諾特定的財產交易，雖然必須於未來完成交易後，才可能出現財產，但行為人無權使用資料的同時，也將立即改變「本人或相對人現在應有財產狀態」，筆者主張這類行為，也應同時納入虛偽資料的範圍¹⁴²，具體適例即行為人盜用本人信用卡，在網路上未經實體店員審核直接購物，客觀上本人未有此項交易意思，而行為人卻實現了此項交易，可認為是不符本人交易意思的虛偽資料。

至於「不正」指令的定義，筆者認為這與程式的干擾方式有

¹⁴⁰ 德國學理亦有認為此一爭議無足輕重，vgl. *Kindhäuser*, aaO. (Fn. 105), § 28 Rn. 14.

¹⁴¹ 這一類型本來就是德國法所謂的「不正確資料」(unrichtige Daten)。德國法多數見解採客觀說(內容不符合客觀事實)解釋其定義，vgl. *Cramer/Perron*, in: *Schönke-Schröder*, § 263a Rn. 5; *SK-Hoyer*, § 263a Rn. 26.

¹⁴² 不過從德國法的客觀說看來，此一形態似乎不能納入不正確資料的範圍，vgl. *Kraatz*, aaO. (Fn. 13), S. 40-41. 不過亦有認為屬之者，vgl. *Arzt/Weber/Heinrich/Hilgendorf*, aaO. (Fn. 14), § 21 Rn. 32.

關，指令連結的干擾手法是影響電腦程式運作，而電腦程式的運作機制是由系統設置者決定，在這個意義下，只要違反系統設置者主觀意思的干擾指令，原則上即屬不正指令¹⁴³，即便行為人是系統的有權使用者，但若在系統中安裝不合原交易目的的程式，也屬於不正指令。舉例而論，銀行部門負責經理可以合法登入銀行系統，檢視並調取存戶資料，但這不代表該經理可以在銀行伺服器內安裝扣除存款尾數的非法程式，其行為自屬輸入不正指令。

綜上，對於第三三九條之三的構成要件行為意義，筆者主張：(1)構成要件行為限於與電腦機能相關的輸入資料或指令行為；(2)不正方法實為贅詞，並無特別意義；(3)輸入的資料不符合客觀實情，即屬虛偽，包括不符合過去財產及交易情狀，或是以該資料創造不符合應有財產分配等兩類；(4)輸入的指令不符合電腦系統設置者意思，即屬不正。當行為人採用上述手法之一而輸入資料或指令時，表示他具有合法授權，可以變動儲存於電腦系統內的財產權資料，但實際上卻無相關權限，此即本罪的詐欺屬性¹⁴⁴。

2. 中間結果：製作財產權資料的得喪變更

緊接著構成要件行為，第三三九條之三還規範了「製作財產權之得喪、變更紀錄」中間結果。就字面看來，第三三九條之三所稱的財產權資料，並不限於電磁紀錄，理論上也包括紙本資料。問題在於：一旦採取了這種解釋方式，在現代電腦化的社會中，任何紙本資料都可以改用電磁紀錄保存，行為人只要透過因果連結，即可

¹⁴³ 此解釋參考德國法輸入不正指令的通說，以設備設置者的主觀意思為準，不過學說上另有反對見解認為應從客觀事實為準認定，vgl. *Cramer/Perron*, in: *Schönke/Schröder*, § 263a Rn. 5; *SK-Hoyer*, § 263a Rn. 23; *Mitsch*, aaO. (Fn. 13), § 3 Rn. 16-17. 針對此一爭議，本文主張指令既然與系統相關，並無不依系統設置意思決定的必要性，故接受設置者意思主觀說。

¹⁴⁴ Vgl. *Arzt/Weber/Heinrich/Hilgendorf*, aaO. (Fn. 14), § 21 Rn. 33.

能因修正紙本資料後，又改以電腦儲存，從而成立第三三九條之三罪名。舉例來說，行為人並無展店計畫而向被害人借款，被害人陷入錯誤後，前往銀行取款，在取款過程中，因帳戶資料都已電磁資訊化，銀行遂依行為人提供的資料，作成被害人轉帳給行為人的電腦資料紀錄，致生財產損害。依第三三九條之三判斷上例刑責，雖然行為人不是自己輸入虛偽資料，但仍然算是提供虛偽資料，利用被害人及行員間的臨櫃提款行為，使得行員將提款紀錄輸入於銀行的電腦系統，製造財產權變更紀錄，造成被害人損害，直觀看來，完全符合第三三九條之三各項要素，但實際上本案應該是第三三九條普通詐欺罪，根本與電腦詐欺無關。如果不具體限制條文所稱財產權資料的屬性，本罪成立範圍已無任何界限可言。

礙於第三三九條之三對中間結果並無進一步的文字定性，刑責界限勢必極度浮動，解釋上顯然有必要參酌法定犯行與財產關聯性，對於第三三九條之三所稱得喪變更的「財產權紀錄」予以限定。依筆者之見，既然法定犯行限於「輸入」訊息及指令到電腦系統，最後造成不合法的財產變動，行為人當然得透過「輸入」行為，直接「製作」儲存於電腦系統的財產權變動資料，換言之，中間結果的實現必須附加三個條件：(1)該變動的財產權資料必須儲存於電腦系統¹⁴⁵；(2)該財產權紀錄違反真實¹⁴⁶；(3)行為人透過輸入電腦資料或指令，自行依電腦系統的運作方法，直接製作系爭變更紀錄，該變更紀錄完全由電腦依程式完成，不得透過有實質審查權限的第三人作成¹⁴⁷，如果製作財產權紀錄的過程中，還必須經過第三人

¹⁴⁵ 即便如此，本罪保護法益仍是財產而非電腦安全，vgl. *Kindhäuser*, aaO. (Fn. 105), § 28 Rn. 30.

¹⁴⁶ 此一要求亦見於蔡蕙芳，同註1，頁84。

¹⁴⁷ Vgl. *Mitsch*, aaO. (Fn. 62), S. 314. 另外必須強調，雖然要求行為人自行製作變更紀錄，但這不代表本罪屬於親手犯 (*Eigenhändiges Delikt*)，行為人仍可利

審核，財產權的紀錄才能變更，原則上即排除本罪的成立¹⁴⁸。

如果可以接受上述看法，再回頭審視前文案例，行為人向被害人借款，同時造成財產紀錄的不正確記載，但銀行存款紀錄的變動並非行為人直接作成，而是由有權決定的被害人及行員共同完成，中間欠缺直接的製作紀錄屬性，故非本罪處罰範圍¹⁴⁹。

3. 中間結果與最終財產交易的因果關聯

最後討論財產損害的認定與因果關聯性。第三三九條之三屬於財產犯罪的電腦詐欺，即使條文未寫，成罪結果仍須致生財產損害，損害判定標準，原則上同於第三三九條之一及之二的規定。除此以外，由於法條明文要求「製作財產權之得喪、變更紀錄，『而取得』他人財產者」，財產紀錄變更的中間結果必須與電腦系統給付財物或利益，從而致生財產損害之間，具有直接因果連結性，亦即，財產交付的風險實現後果，必須發自財產紀錄的變更所致¹⁵⁰，行為人透過其犯行發動的干擾效果，直接讓電腦下達實現特定給付的指令，該給付行為一旦作成，財產損害也將隨之實現，當關涉財產關係的電腦紀錄被變更後，不可以有任何人為審查介入，只需要依憑電腦系統運作即足¹⁵¹。相反而論，倘若財產資料變動與財產交付損害間，還有第三人審查的介入空間，甚而還必須

用不知情第三者代為輸入，只不過被利用人必須時是輸入資料者及製作變更紀錄者。不同見解，參見黃榮堅，同註2，頁321。

¹⁴⁸ 雖然排除人為審核權，但不排除電腦系統的審核權限，事實上，當行為人提供虛偽資料時，正是利用電腦審核權限的盲點才能成功詐取財物。

¹⁴⁹ 相近見解，vgl. *Kindhäuser*, aaO. (Fn. 105), § 28 Rn. 33. 學說上另有認為如果都可能成立時，應優先適用原詐欺罪規定，vgl. *Mitsch*, aaO. (Fn. 13), § 3 Rn. 9.

¹⁵⁰ 參考蔡蕙芳，同註41，頁80-81。Vgl. *Kraatz*, aaO. (Fn. 13), S. 38; *Arzt/Weber/Heinrich/Hilgendorf*, aaO. (Fn. 14), § 21 Rn. 34.

¹⁵¹ 向實體店員提供他人信用卡而取得對價，因過程中有店員介入，仍不成立第339條之3罪名，參見黃榮堅，同註2，頁322。

得到該人認許才能給付，此時就不再是直接由電腦程式運作所作出的電腦詐欺，而是存在相對人的一般詐欺或奪取型罪名¹⁵²。

舉例而言，倘若銀行行員登入系統後，冒用存戶名義，在銀行電腦系統中將存戶的定存解約，如果依據銀行內控機制，還必須由銀行經理審核，待審核完成後，才可領出解約後的本息，此時應該認為經理的介入，將使得電腦系統不是直接的給付源頭，行為人仍不成立第三三九條之三罪名。

(三)類型化的觀察取徑

以上大致討論了第三三九條之三成罪要素的個別解釋，最後則是本罪可能成立的三種類型。就此筆者認為，既然立法者未在條文之內明訂具體的成罪限制，只要能符合本文強調因果關聯性的解釋，即應認為成立本罪，三種不同形態的成罪方式，原則上都可基於這些判斷標準認定。

首先是管理權限濫用型，這類行為人通常有系統後端登入權限，而合法接近財產權資料，行為人利用該機會改變財產資料，實現他人財產損害。改變資料內容的具體方法，除了直接篡改存戶資料外（輸入虛偽資料），也可以是安裝電腦病毒或木馬程式，干擾系統的正常運作，而作出不合理的給付關係¹⁵³。

以前文提過事例來談，銀行行員在電腦系統變更客戶定存資

¹⁵² 此解釋參考詐欺罪要求「相對人處分行爲」與「財產損害」間，不得有行為人的介入，相關討論，vgl. *Jäger*, Die drei Unmittelbarkeitsprinzipien beim Betrug, JuS 2010, S. 761-765; *Kindhäuser*, aaO. (Fn. 105), § 28 Rn. 32; *Maurach/Schroeder/Maiwald*, aaO. (Fn. 14), § 41 Rn. 237.

¹⁵³ 這類犯罪通常伴隨著背信罪，就第339條之3的成立，通常問題發生在財產資料變更與財產給付的關係，雖然行為人可以登入後台，但不代表資料變動後，一定可以拿得到錢，依本文之見，只要有第三者的審查介入，原則上應認為已經脫逸電腦詐欺的處罰範圍，不成立本罪。

料，倘若返還定存本金須經行員審查，則該行為即非第三三九條之三罪名；又例如捷運站員工直接以其權限，塗銷同事的乘車紀錄，已然輸入虛偽資料而製作付費乘車的不正財產紀錄變更，該同事因而不需要繳費，該過程可由捷運公司的電腦系統直接判讀，故屬本罪的可罰範圍¹⁵⁴。

其次是侵入電腦型，這類行為技術門檻較高，必須先無權侵入中央伺服器，我國實務案例並不多見，亦較少受到關注。

最後則是本條解釋關鍵的資料操縱型，這種侵害形態確實是整個電腦詐欺罪最根本的規定，德國電腦詐欺罪正沿循著此種方式規範，只不過我國除了本罪之外，另外還多規定了第三三九條之一及之二的構成要件，其中的自動付款設備詐欺罪又把應由電腦詐欺概括條款處罰的關鍵案例，完全排除於第三三九條之三的處罰範圍，這勢必使得第三三九條之三只能用來處理之一及之二兩條未能處理的類型。

這類型案例的典型情況，應是便利商店店長偽造繳費紀錄，依循連線系統向銀行申請手續費，只要店長自行輸入偽造繳費紀錄至電腦系統，而銀行信賴便利商店，不再有任何人為審查介入手續費發給程序，完全委由電腦執行，即可成立本罪。又例如行為人趁彩票行老闆不注意，自行列印特定號碼彩票，該行為人盜用原屬老闆的登入權限，未付對價，直接在系統中製作特定號碼的投注紀錄，從而取得未來向彩票公司請求彩金的期待權，可認為是輸入虛偽資料而不法製作財產權紀錄，而系統在未有第三人審查時，即許可列印出紙本彩票，該過程雖然僅只實現期待權，但仍完全成立第三三九條之三的罪名。

以上探討成罪的基礎類型，最後附加檢討若干有相當爭議的案

¹⁵⁴ 另參考蔡蕙芳，同註41，頁76。

例類型：

1. 實務上曾出現趁其他電玩玩家上洗手間的機會，盜用其帳號，將他人帳號內供遊戲使用的虛擬寶物移轉至行為人個人帳號之下，依本文見解，行為人非帳號的合法使用者，輸入轉移寶物的電腦資料，製作了財產資料變更，只要虛擬寶物可以在現實世界中具有市價行情，即可成立第三三九條之三第二項犯罪¹⁵⁵。

2. 此外，我國實務近期判決，逐漸主張網路ATM、網路銀行，及語音銀行均適用第三三九條之三，但本文認為這種限縮第三三九條之二於實體櫃員機的見解並不正確，相類的行為應構成第三三九條之二罪名，理由已於前述¹⁵⁶。

3. 設若行為人盜用他人名義，使得本人或相對人負擔不應有的支出，從而使得收費設備誤信為真，進而給付財產，實務向來認為這些案例構成第三三九條之一，不過本文主張這些只是計費設備，行為人盜用他人名義，屬於輸入虛偽資料，而計費設備的費用紀錄，可以認為是財產權的不實資料，最後取得財產，這些案例實應成立第三三九條之三。例如，行為人提示信用卡，而於網路上鍵入數字購物，或於無人管理的加油站自助加油，又或行為人盜打他人名下手機，這些案例都應構成第三三九條之三¹⁵⁷。

¹⁵⁵ 進一步討論，參考甘添貴，同註51，頁179-183。

¹⁵⁶ 匿名審查人指出：「作者[……]反對實務上將針對網路ATM、網路銀行的行為歸入第339條之3，而主張應成立第339條之2，是否認為這兩個條文的適用係屬互斥排他？若否，則兩罪間的競合關係為何？」（原文照刊），筆者看法認為，第339條之2應該屬於第339條之3的特別規定，兩者間具互斥適用關係，因為付款機制必須以連線方式計算款項及餘額，這些行為其實都已構成第339條之3的犯罪，只不過因為立法者獨立出「付款設備」的特別規定，任何「輸入人別資料而提領或轉發款項」的近似侵害手法，都應該歸入第339條之2的處罰範圍，而不再是第339條之3。

¹⁵⁷ 值得注意的是，德國學說上亦有主張依詐欺類似說，無權盜打他人行動電話

4. 又若電動遊戲場店員在應繳回公司的作廢會員卡上加值，之後再販賣給他人謀利，法院認為行為人構成第三三九條之三。但對此見解筆者則有不同意見，會員卡儲值其實是預收費用，該預收費用在每一次顧客使用遊樂設備時，會被收費機制扣除點數，行為人偽造能夠讓買受顧客使用的卡片儲值，其實與第三三九條之一比較接近，因此買受行為人偽造儲值的卡片，而通過機器驗證並享受服務的會員，構成第三三九條之一的不正方法，至於修改儲值後予以轉賣會員卡，但未直接對收費設備實施不正方法的行為人，不可能構成第三三九條之一的正犯，至多構成之一罪名的共犯¹⁵⁸。至於在無人使用會員卡之前，行為人能否單因偽造儲值數字而成立第三三九條之三？基本上必須考慮增值行為的屬性，如果行為人單獨於卡片上加值，而該違法增值紀錄未連線至公司的中央伺服器，則僅屬電磁紀錄的偽造文書行為，與第三三九條之三虛入不正資料而造成錯誤財產紀錄無關，不過倘若公司的儲值系統是透過中央伺服器控制，行為人的增值必須連線修改伺服器內的儲值資料，這已然是前文提到的管理權限濫用型，應可成立第三三九條之三刑責。

5. 實務另有案例，行為人打電話給電信公司，謊報他是本人並通過身分認證後，變更本人原有的資費費率。本案法院認為變更資費費率並非財產權紀錄，故不成立第三三九條之三。筆者贊同法院結論，但理由不同：電信資費的費率本身關涉未來繳付價額，雖然看似不直接與財產有關，但其關涉如何計算繳付金額，可以認為是一種財產權的紀錄，這一點法院見解似乎有誤。然而，本案之所以

仍不算電腦詐欺，但應注意其電腦詐欺的規定與我國不同，vgl. *Kretschmer, Der erfolglose Literat, Jura 2006, S. 227.*

¹⁵⁸ 基於共犯從屬性，行為人成立共犯（特別是幫助犯）的前提，當然是已有會員使用該會員卡而構成正犯。

不成罪，主因第三三九條之三的犯行，必須由行為人以電腦方式輸入，但該案行為人僅告知電信公司服務人員，再由服務人員代為改變費率，應無法認為屬於「輸入虛偽訊息至電腦」。此外，第三三九條之三是典型的財產犯罪，行為人必須有不法得利意圖，但該案的行為人僅出於損害本人利益而變更費率，無不法得利意圖而不成罪。

肆、結 論

最後總結本文研究成果如下：

一、第三三九條之一至之三等三個罪名都有不正方法，但其定義不同，判定其內容時應實質探求個別構成要件涉及的交易結構，再予以認定其定義；至若條文中無法抽繹出明確的交易結構時，只能轉從個別要素間的因果關聯性與電腦特性，實質地掌握成罪界限。

二、第三三九條之一交易結構是「財產給付／財物或利益的對待給付」，不正方法指的是行為人提出欠缺財產意義的虛假給付，但形式上卻可通過設備判讀，從而享有設備提供的對待給付。此外，第三三九條之一只處理收費設備，計費設備不屬於條文所稱的收費設備。

三、第三三九條之二交易結構在於「人別認證／付款」，不正方法指的是行為人使用偽造的認證資料，或是提出形式上真實但欠缺實質授權的認證資料，原則上只要是未得本人授權，不論是外部侵害（竊取卡片）或內部侵害（越權提款），均可認定為不正方法。

四、第三三九條之三的條文中，立法者只規定損害流程，但無明確的侵害對象及交易結構，不能採用解釋前兩條的作法，成立第

三三九條之三罪名的判斷重心，應是行為人輸入不符合本人或設置者意思的資料或指令，使得系統誤判行為人具有合法權限，而放任行為人直接製作財產權變更的電腦紀錄，直接引發電腦給付財產的指令，實現財產損害，這些要素之間必須具備明確的因果關聯性，否則仍不成立本罪。

參考文獻

一、中 文

1. 甘添貴，虛擬遊戲與盜取寶物，台灣本土法學雜誌，50期，頁179-187，2003年9月。
2. 甘添貴，自動付款設備詐欺罪之不正方法，月旦法學教室，39期，頁22-23，2006年1月。
3. 甘添貴，刑法各論（上），2009年6月。
4. 李茂生，資本、資訊與電腦犯罪，載：權力、主體與刑事法，頁165-300，1998年5月。
5. 李聖傑，溢領借款的詐欺——評台北地院92年度自字第17號判決，月旦法學雜誌，120期，頁219-228，2005年5月。
6. 李聖傑，靜靜都有事？，月旦法學教室，104期，頁28-29，2011年6月。
7. 林山田，電腦犯罪之研究，載：刑事法論叢(一)，頁135-169，1987年5月。
8. 林山田，評詐欺罪章中之新增三罪，月旦法學雜誌，49期，頁85-89，1999年6月。
9. 林山田，刑法各罪論（上），5版，2006年11月。
10. 林東茂，詐欺罪的財產損害，警大法學論集，3期，頁199-209，1998年3月。
11. 林東茂，刑法綜覽，7版，2012年8月。
12. 吳耀宗，詐欺罪詐術行使之解析，月旦法學雜誌，163期，頁50-64，2008年12月。
13. 許恒達，盜用存摺提款與不法所有意圖——評最高法院100年度台上字第3232號判決，月旦裁判時報，16期，頁59-70，2012年8月。
14. 陳子平，自動付款設備詐欺罪，月旦法學教室，53期，頁68-73，2007年3月。
15. 陳子平，偽造支付工具電磁紀錄物罪與相關犯罪，月旦法學教室，111期，頁78-92，2012年1月。
16. 張麗卿，機器與詐欺，載：新刑法探索，頁321-332，2006年8月。

17. 黃常仁，「困頓新法」——論刑法第三三九條之一、第三三九條之二與第三三九條之三，台灣本土法學雜誌，27期，頁1-12，2001年10月。
18. 黃榮堅，刑法解題——關於詐欺等財產犯罪，載：刑法問題與利益思考，頁79-98，1995年6月。
19. 黃榮堅，電腦的心事，月旦法學教室，37期，頁20-21，1998年6月。
20. 黃榮堅，刑法增修後的電腦犯罪問題，載：刑罰的極限，頁301-344，1999年4月。
21. 黃榮堅，電腦犯罪的刑法問題，載：刑罰的極限，頁167-210，1999年4月。
22. 蔡蕙芳，電腦犯罪與刑事立法的課題，月旦法學雜誌，0期（試刊號），頁103-107，1995年4月。
23. 蔡蕙芳，電腦詐欺行為之刑法規範，東海大學法學研究，18期，頁29-50，2003年6月。
24. 蔡蕙芳，自動化設備濫用行為之刑法規範，中原財經法學，11期，頁43-77，2003年12月。
25. 蔡蕙芳，不正利用收費設備取財得利罪，月旦法學教室，44期，頁64-73，2006年6月。
26. 蔡蕙芳，不正利用電腦取財得利罪，月旦法學教室，46期，頁70-81，2006年8月。
27. 蔡蕙芳，不正利用自動付款設備取財得利罪，月旦法學教室，49期，頁55-67，2006年11月。
28. 蔡蕙芳，刑法第339條之1不正利用收費設備取財得利罪之適用問題——四則地方法院判決之檢討，月旦法學雜誌，138期，頁233-244，2006年11月。
29. 蔡聖偉，論盜用他人提款卡的刑事責任，月旦法學雜誌，144期，頁20-40，2007年5月。
30. 盧映潔，不拿白不拿？，月旦法學教室，77期，頁24-25，2009年3月。
31. 盧映潔，刑法分則新論，5版，2012年9月。

二、外 文

1. *Achenbach, Hans*, Die „kleine Münze“ des sog. Computer-Strafrechts – Zur Strafbarkeit des Leerspielens von Geldspielautomaten, *Jura* 1991, S. 225ff.
2. *Arzt, Gunter/Weber, Ulrich/Heinrich, Bernd/Hilgendorf, Eric*, Strafrecht Besonderer Teil, 2. Aufl., 2009.
3. *Biletzki, Gregor*, Anmerkung an OLG Düsseldorf, *NJW* 2000, 158, *NStZ* 2000, S. 424ff.
4. *Duttge, Gunnar*, Vorbereitung eines Computerbetrug: Auf dem Weg zu einem „Grenzlosen“ Strafrecht, in: *Ulrich Weber-FS*, 2004, S. 285ff.
5. *Ellbogen, Klaus*, Strafbarkeit des einfachen „Schwarzfahrens“, *JuS* 2005, S. 20ff.
6. *Hilgendorf, Eric*, Scheckkartenmissbrauch und Computerbetrug – OLG Düsseldorf, *NStZ-RR* 1998, 137, *JuS* 1999, S. 542ff.
7. *Jäger, Christian*, Die drei Unmittelbarkeitsprinzipien beim Betrug, *JuS* 2010, S. 761ff.
8. *Kindhäuser, Urs*, Der Computerbetrug (§ 263a StGB) – ein Betrug?, in: *Gerald Grünwald-FS*, 1999, S. 285ff.
9. *Kindhäuser, Urs*, Strafrecht Besonderer Teil 2, 5. Aufl., 2008.
10. *Kindhäuser, Urs/Neumann, Ulfrid/Paeffgen, Hans-Ullrich*, *NomosKommentar zum Strafgesetzbuch*, 3. Aufl., 2010.
11. *Kraatz, Erik*, Der Computerbetrug (§ 263a StGB), *Jura* 2010, S. 36ff.
12. *Kretschmer, Bernhard*, Der erfolglose Literat, *Jura* 2006, S. 219ff.
13. *Lackner, Karl*, Zum Stellenwert der Gesetzestechnik, in: *Herbert Tröndle-FS*, 1989, S. 41ff.
14. *Lackner, Karl/Kühl, Kristian*, *Strafgesetzbuch Kommentar*, 26. Aufl., 2007.
15. *Lenckner, Theodor*, *Computerkriminalität und Vermögensdelikte*, 1981.
16. *Maurach, Reinhart/Schroeder, Friedrich-Christian/Maiwald, Manfred*, *Strafrecht Besonderer Teil*, Bd. 1, 10. Aufl., 2009.
17. *Mitsch, Wolfgang*, Strafbare Überlistung eines Geldspielautomaten – OLG Celle, *NJW* 1997, 1518, *JuS* 1998, S. 307ff.

18. *Mitsch, Wolfgang*, Strafrecht Besonderer Teil 2, Teilband 2, 2001.
19. *Neumann, Ulfrid*, Unfares Spielen an Geldspielautomaten – OLG Celle, NStZ 1989, 367, JuS 1990, S. 535ff.
20. *Otto, Harro*, Probleme des Computerbetrugs, Jura 1993, S. 612ff.
21. *Ranft, Otfried*, Zur „betrugsnahen“ Auslegung des § 263a StGB, NJW 1994, S. 2574ff.
22. *Rengier, Rudolf*, Strafrecht Besonderer Teilband 1, 11. Aufl., 2009.
23. *Rudolphi, Hans (et al.)*, Systematischer Kommentar zum Strafgesetzbuch, 8. Aufl., 2011.
24. *Scheffler, Hauke/Dressel, Christian*, „Unbefugtes“ Verwenden von Daten beim Computerbetrug, NJW 2000, S. 2465ff.
25. *Schnabel, Falk*, Telefon-, Geld- Prepaid-Karte und Sparcard, NStZ 2005, S. 18ff.
26. *Schönke, Adolf/Schröder, Horst*, Strafgesetzbuch, 28. Aufl., 2010.
27. *Sieber, Ulrich*, Computerkriminalität und Strafrecht, 2. Aufl., 1980.
28. *Wessels, Johannes/Hillenkamp, Thomas*, Strafrecht Besonderer Teil/2, 30. Aufl., 2007.

Computer Fraud and Unlawful Means

Heng-Da Hsu^{*}

Abstract

This study explores the present interpretation of liability for computer fraud which was enacted in Taiwan's Criminal Code in 1997. The relevant paragraphs (§§ 339-1, 339-2 and 339-3) aimed to deal with computer fraud which caused a significant amount of property damage at that time. However, since the legislature adopted many unclear concepts such as unlawful means, data processing, fees-collecting apparatus, and automated teller machine, et al., how to interpret these offensive conditions remains a difficult issue for criminal justice specialists and academic circles up to the present. The author finds that the resolution of these problems could stem from the investigation of the trading structure in each paragraph, e.g. §§ 339-1 and 339-2. In addition, as no trading structure can be established in § 339-3, the key to interpreting it should be the causal relation between all elements of § 339-3.

Keywords: Computer Fraud, Trading Structure, Unlawful Means, Data Processing, Fees-Collecting Apparatus, Automated Teller Machine

* Associate Professor, College of Law, National Chengchi University; Dr. iur. Frankfurt University, Germany.

Received: May 15, 2013; accepted: July 12, 2013