電信網絡詐騙疑似涉詐帳戶資金反制預警機制研究及實踐路徑

王夢瑤、單丹 *

摘要：目前我國內地的電信網絡詐騙犯罪猖獗，造成極大的經濟損失。當前的事後資金預警機制存在着公安方面預警啟動困難、降發案降案損作用有限、預警收效不佳、事中柔性干預缺位，銀行方面存在盈利驅動下強管控不力、最新犯罪場景庫補足不及時等現實困境。而以電信網絡詐騙疑似涉詐帳戶為核心的資金反制預警機制，可以作為對現有事後資金預警機制的有益補充。可從促成內外合力、提升監測預警技術、制訂規範性文件等方面切實提升新機制的反制預警實效。

關鍵詞：電信網絡詐騙　疑似涉詐帳戶　預警　反制　模型算法

Research and Practical Pathways for the Anti-Fraud and Early Warning Mechanism Against Suspected Fraudulent Accounts in Telecommunication Fraud

Wang Mengyao；Shan Dan

Abstract: Telecommunication fraud is rampant in Mainland China nowadays, causing great economic losses. For the current post-event funding warning mechanism, it faces practical difficulties including those in initiating public security-related early warnings, the limited effectiveness in reducing occurrences and losses, the poor effectiveness of the warnings, and a lack of flexible intervention during the incident. For the banks, they face practical difficulties including inadequate management and control arising from profit-driven reasons, and late updates to the related crime database. The anti-fraud and early warning mechanism, which targets suspected fraudulent accounts involved in telecommunication fraud, serves as a useful supplement to the existing post-event funding warning mechanism. The anti-fraud and early warning effectiveness of the new mechanism can be effectively enhanced by promoting internal and external cooperation, strengthening the supervision of early warning technology, and formulating regulatory documents, etc.

Keywords: Telecommunication Fraud; Suspected Fraudulent Accounts; Early Warnings; Anti-Fraud; Model Algorithm

* 王夢瑤，中國人民公安大學偵查學院，講師，法學博士。

* 單丹，北京市公安局刑事偵查總隊十支隊，警務技術一級主管，法學博士。

一、前言

電信網絡詐騙屬於侵財類案件，追贓挽損工作直接關係着廣大人民群眾的切身利益，影響着人民群眾對公安工作的認可度，關乎着百姓對黨和國家執政能力的評價。然而，在電信網絡詐騙資金流轉手段不斷迭代的背景下，追贓挽損工作的效果不容樂觀。王小洪部長在 2023 年 5 月的《全國打擊治理電信網絡新型違法犯罪工作電視電話會議》中部署要以“全力減少人民群眾財產損失”為總目標。在這樣的現實背景下，建立與完善電信網絡詐騙疑似涉詐帳戶資金反制預警機制是題中應有之義。

二、問題的提出

與當前內地電信網絡詐騙犯罪高發案、高案損形成鮮明對比的，是資金流預警理論研究成果的不足。筆者以“電信網絡詐騙”與“資金流”為關鍵詞進行模糊複合檢索，僅發現 27 篇學術論文與 2 篇學位論文，其中多以“查控”、“處置”、“整治”、“緊急止付”等為研究方向，而涉及“資金預警機制”的僅在個別文章中佔據極少的篇幅。筆者將其梳理如下：學者賈宇、武曄廷、楊喆認為，銀行機構應在事中環節採用人臉識別、交易延遲、交易阻斷等方式，強化資金風險防控能力，為受害人與警方爭取挽損時間。[1] 學者于龍認為，通過重點涉詐人員數據庫，並依據核查“兩卡”線索等手段進行數據關聯分析，可以實現對電信網絡詐騙行為的資金軌跡進行預警。[2] 學者劉啟剛、陳效棠認為，資金查控分析的深入與否，決定着對潛在被害人進行發現並預警能否成功。[3] 學者陶冶認為，應該建立模型即時監測異常帳戶交易情況，針對異常交易實施帳戶管控。[4] 學者莊華認為資金流預警可通過對被害人資金流的異常變動特徵進行識別，或者對洗錢環節進行監管來實現，但由於資金流數據涉及的數據來源複雜，數據體量大，在實踐中比較難以實現。[5] 學者莊華、廖廣軍認為可以從“供 – 求”兩方面對電詐資金交易進行干預和預警，並提出建立涉詐風險模型，根據交易習慣、金額、時間等要素進行識別。[6] 在域外研究方面，學者多從技術模型構建方面犯罪預警問題。學者羅塞特 (Rosset) 提出了通過特徵進行識別電信網絡詐騙犯罪，如通過交易的行為特徵等來識別電信網絡詐騙犯罪。[7] 愛奧尼塔 (Ionita) 提出了 e3–value 風險分析模型。[8] 迪普 (Deep) 提出神經網絡，模糊邏輯等技術在預警中的應用。[9]

由上述文獻梳理可見：在預警方面，學者們研究方向一致，皆為通過提取資金流的特徵要素，進行識別達到預警目的。然而，學術界鮮有對目前電信網絡詐騙犯罪資金流進行預警的機制進行的研究。

三、對現有電信網絡詐騙資金反制預警機制反思

人們運用科學方法預測犯罪的行為可以追溯到 1829 年的法國，阿德里亞諾·巴爾比和安德烈·米歇爾·古里通過統計分析繪製了一批法國教育水平與暴力和財產犯罪之間關係的地圖。[10] 自此，利用數據統計、數據分析預測犯罪並提前防範成為犯罪治理的重要手段。中辦國辦印發《關於加強打擊治理電信網絡詐騙違法犯罪工作的意見》(以下簡稱：《意見二》) 強調，要堅持“打防結合、防範為先”，並從強化技術反制、

---

[1] 賈宇、武曄廷、楊喆：〈關於個人涉詐帳戶風險治理的調查與思考——以內蒙古烏海市為例〉，《北方金融》，2023 年，第 12 期，第 96–98 頁。

[2] 于龍：〈電信網絡詐騙資金鏈預警查控的困境審視〉，《雲南警官學院學報》，2023 年，第 6 期，第 85–90 頁。

[3] 劉啟剛、陳效棠：〈基於資金查控的電信網絡詐騙犯罪偵查治理〉，《山東警察學院學報》，2023 年，第 35 卷，第 5 期，第 105–113 頁。

[4] 陶冶：〈銀行機構反電信網絡詐騙路徑分析—基於涉案帳戶流水〉，《金融會計》，2023 年，第 7 期，第 68–74 頁。

[5] 莊華：〈電信網絡詐騙犯罪的大數據預警〉，《中國刑警學院學報》，2022 年，第 1 期，第 5–13 頁。

[6] 莊華、廖廣軍：〈“供給 – 需求”視角下電信網絡詐騙犯罪治理框架〉，《公安研究》，2023 年，第 2 期，第 24–28 頁。

[7] Rosset S, Murad U, Neumann E, et al.Discovery of fraud rules for telecommunications–challenges and solutions[C]// Acm SigkddInternational Conference on Knowledge Discovery & Data Mining.ACM,1999.

[8] D Ionita, Koenen S K, Wieringa R J.Modelling telecom fraud with e3value[J]. University of Twente Centre for Telematics&InformationTechnology, 2014.

[9] Deep A, Kaur A, Gill N. Using Data in Telecommunications: Challenges and Solutions. [C]//International Multiconference of Engineers&Computer Scientists. DBLP, 2007.

[10] Linda S T, Elaine H, Dent B.,Atlas of Crime: Mapping the Criminal Landscape. Phoenix, AZ: Oryz Press, 2000, 4–21.

預警勸阻、宣傳教育等三個方面，全面落實“防範為先”理念。[11]《中華人民共和國反電信網絡詐騙法》（以下簡稱《反詐法》）第 18 條對電信網絡詐騙犯罪資金流監測機制做出了規定。[12] 由此可見，建立健全電信網絡詐騙犯罪資金預警機制的法律依據日趨完善。

受制於數據資源等方面的限制，目前電信網絡詐騙犯罪的資金流預警機制是以受害人報案為起點的事後預警機制，該機制的優勢在於由受害人發起，公安機關公權力不過度介入公民私權利，有利於對公民人身、財產權利的保護，然而其局限性也比較突出。

（一）公安機關──事後預警效果不佳

1. 犯罪隱案多造成的機制啟動不及時

電信網絡詐騙犯罪隱案多，嫌疑人利用受害人羞於提起男女關係，或因畏懼參與網絡賭博等違法犯罪被追訴的心理，阻止其報案。如在色情刷單類案件中，嫌疑人通過引流渠道散播可提供上門性服務消息，引誘被害人參與刷單返利任務，聲稱只有完成一定數量的任務，才有機會與異性開展線下互動專案，多數受害人在轉賬多次後才意識到被騙，常因難以啟齒，不願報案。此外，在一些網絡交友類詐騙案件中，部分受害人甚至在見到勸阻民警後，也拒絕承認被騙事實。

另外，事主從被騙醒悟到報案需要時間，也是預警啟動時間節點相對滯後的原因。

2. 事後預警對於降發案、降案損作用有限

如前文所述，目前資金預警模式由受害人報案後被動發起，預警線索產生時多已成案並伴隨受害人大量財產的損失。電信網絡詐騙犯罪的常見形式是，嫌疑人利用固定話術使受害人不斷加深錯誤認識，進而作出一筆接一筆轉賬的錯誤行為，直到受害人餘額不足或無法繼續貸款為止。在此過程中，受害人只能依靠自身認知識破騙局，自主地終止轉賬行為。現有資金預警模式缺乏一種能夠事中干預受害人基於錯誤認識作出的錯誤轉賬行為的“外力”，缺少提前“叫醒”受害人的方法，因而降發案、降案損的作用有限。內地 2016 年曾發生典型案件──徐玉玉案，最高人民法院、公安部、中國人民銀行等六部門聯合發佈的《關於防範和打擊電信網絡詐騙犯罪的通告》提出，自 2016 年 12 月 1 日起，個人通過銀行自助櫃員機向非同名帳戶轉帳，資金 24 小時後到賬。可見，事中干預是相關部門考慮到的作法。只是在運行中，金融機構認為犧牲金融時效而收效不明。

3.“漫灌式”預警收效不佳

當前，電詐洗錢環節前置，利用一級卡直接進行貿易對沖的情形越發普遍。而現有的資金預警模式容易將少數開展合法貿易的小商戶列為預警勸阻對象，不僅浪費了人力、物力，還給部分人民群眾的生產生活造成不良影響。

4. 事中柔性干預缺位，勸阻效果不佳

該資金預警模式中，因銀行及其監管部門的參與度不高，而缺乏事中環節的主動、柔性干預措施。以刑事強制力為背書的公安機關直接接觸受騙群眾，處理關係不當，易引發社會矛盾和輿論炒作。

（二）商業銀行──末端管控興致索然

從上文對現有資金流反制預警機制的梳理中不難看出，該流程的實現需要經歷“受害人 – 公安機關 – 銀行”三重主體的共同參與。銀行作為該機制的最後一環承擔着末端管控效果產出的重要任務。然而，這樣的鏈路設計在實戰工作中暴露出很多問題。

---

[11] 中共中央辦公廳、國務院辦公廳印發《關於加強打擊治理電信網絡詐騙違法犯罪工作的意見》（以下簡稱：《意見》）強調，要堅持以人民為中心，統籌發展和安全，……，堅持打防結合、防範為先，強化預警勸阻，……，堅持科技支撐、強化反制，運用科技信息化手段提升技術反制能力，堅持源頭治理、綜合治理，加強行業監管……《意見》要求，要構建嚴密防範體系。……強化預警勸阻，不斷提升預警信息監測發現能力，及時發現潛在受害群眾，採取勸阻措施。

[12] 《反詐法》第十八條：“銀行業金融機構、非銀行支付機構應當對銀行帳戶、支付帳戶及支付結算服務加強監測，建立完善符合電信網絡詐騙活動特徵的異常帳戶和可疑交易監測機制。”

1. 盈利驅動下管控意願不強

商業銀行在盈利目的的驅動下，缺乏對異常交易行為進行管控的內驅力，因此很難果斷地採取交易掛起、暫停非櫃面業務等強硬管控措施，而多通過刷臉、短信驗證、語音提示等軟性管控措施進行線上實名核驗或提供風險提示，因而無法全面有效地壓降利用銀行卡洗錢的行為。

2. 缺乏對最新犯罪場景的補足

商業銀行具有龐大的基礎數據庫和強大的算力，但對涉案銀行卡犯罪行為的識別與阻斷效果不佳。這是由於在措施管控方面商業銀行的出口直面涉詐帳戶，而在機制設計方面卻與涉詐帳戶操作行為的質性分析脫節。[13] 對於電信網絡新型違法犯罪的最新犯罪手段、發生場景等掌握不足，使銀行難以單獨設計出科學有效的識別、阻斷涉詐風險交易的模型與機制。如當前對涉詐銀行卡的風險管控主要依賴基於實名核驗的反洗錢模型，針對的是過去卡農將銀行卡寄出後由洗錢團夥成員操作使用的場景。而斷卡行動後，犯罪手段發生異化，洗錢團夥通過線上渠道在各地募集、培養卡頭，卡頭在當地招收卡農使用本人銀行卡刷臉洗錢。從“本人銀行卡，由他人異地操作”的洗錢犯罪場景，異化為了“本人銀行卡，由本人在常住地操作”的洗錢場景，反洗錢風控模型自然無法應對最新電詐洗錢模式。

四、電信網絡詐騙資金反制預警機制思路革新

（一）疑似涉詐帳戶資金反制預警模式的提出

通過上述分析，我們發現當前的電信網絡詐騙犯罪資金流預警機制存在着諸多制度性缺陷。實務界亟需探索建立一套由公安機關主導的，聯合銀行機構事中主動干預的疑似涉詐帳戶 [14] 反制預警機制。加快完善“專業 + 機制 + 大數據”新型警務運行模式，在反電詐中充分發揮公安機關發現犯罪活動的能力、算力，借助金融機構資訊系統賦能，從金融機構大數據中發現線索，是公安機關新質戰鬥力生成的重要體現。

（二）對疑似涉詐帳戶資金反制預警模式的評價

疑似涉詐帳戶資金反制模式中，先由公安機關根據最新犯罪規律率先研判出即將用於作案的疑似涉詐帳戶，再聯合商業銀行進行事中干預，最終達到發現、保護並勸阻潛在被騙群眾，減少財產損失，降低成案可能性的目的。

1. 啟動機制更科學

新機制的啟動模式由“人觸發”模式轉變為“問題帳戶觸發”模式。通過公安機關的主動作為，在受害人報案前，提前將具有作案規律特點的“問題帳戶”納入預警視線。一方面可以在成案之前對資金流進行反制預警，最大程度地避免受害人遭受財產損失；另一方面也解決了受害人放棄報案而導致的反制預警機制啟動困難的問題，使得新機制的觸發更加科學有效。

2. 既降發案又降案損

新機制中，銀行機構可對公安機關提供的疑似涉詐帳戶進行有針對性的監測，在感知帳戶異常行為時或案件正在發生時，即時對該帳號進行反制並對疑似被害人進行預警，這一過程都發生在成案之前。因此對於降發案與降案損的效果更加突出。

3. “滴灌式”預警更加精準

相比於“漫灌式”預警，新機制下，銀行機構可以先通過公安機關對可疑帳戶進行初步篩選，之後再發揮自身的模型算力優勢，即時計算涉詐風險交易評分，精準鎖定疑似涉詐帳戶，將“誤傷”的概率降到最低。

---

[13] 涉詐帳戶的異常行為、洗錢資金流的最新動態一般會由公安機關在案件偵查過程中予以發現，而銀行難以直接獲取。

[14] 疑似涉詐帳戶，又稱潛在作案帳戶，指電信網絡犯罪中，被洗錢團夥實際控制的，即將或正在用於接收涉詐資金的銀行帳戶。

4. 發揮部門優勢最大化

新機制融合銀行方面在即時監測、干預涉詐風險交易方面的優勢與公安機關在識別犯罪場景、手段方面的優勢。通過對海量涉詐資金交易行為的整合梳理，提煉出涉詐風險指標參數，利用人工智慧技術，生成能夠精準識別涉詐風險交易的算法模型。

（三）對現有事後資金預警模式與疑似涉詐帳戶資金反制預警模式間關係的檢視

資金預警工作要兼顧矛和盾的屬性，因此，疑似涉詐帳戶資金反制預警模式並不是要替代現有事後資金預警模式，而是作為一種補充形式而存在。即以事後預警為基礎，以疑似涉詐帳戶資金反制預警機制為補充的複合式反制預警機制。二者互為補充，交叉運用，以被動觸發的、不漏一戶式事後資金預警為最後防線，聯合銀行將反詐戰線向前推進，構建精準的事中反制預警網絡。真正做到讓被騙資金“轉不出去”，切實保護好人民群眾的“錢袋子”。

五、疑似涉詐帳戶資金反制預警機制建成的現實要求

隨着數據資源的豐富、數據採集的便捷、硬體算力的提升、算法模型的迭代、體制機制的完善，打破部門資源壁壘，加深警銀聯動協作，實現電信網絡詐騙資金反制預警成為可能，根據複盤後的犯罪情景模式將犯罪要素加工成模型指標，運用人工智慧算法，形成資金預警模型，事前篩選出疑似涉詐帳戶，通過事中監測及時發現涉詐風險交易，干預、阻斷正在實施犯罪的行為，實現犯罪預防功能。

（一）促成內外合力 [15]

電信網絡詐騙犯罪的資金流預警工作依靠公安機關一家力量是遠遠不夠的。當前，聯席辦機制主要是各機構間的“外部協作”，各機構通過“節點部門”合署辦公，實現機構間的協作。公安機關通過節點部門“間接的”與成員單位的具體業務部門（如數據建模團隊）進行交流，使得公安機關對各機構內可調用的反詐資源了解不深、應用效果較差。此外，商業銀行數據資源、風控模型多屬於商業秘密，目前，仍缺少一種數據脫敏、模型產權保護的規則，以及正向激勵機制，致使反詐資金治理各自為戰，無法形成一盤棋，並造成電詐資金流向窪地銀行、短板業務。為此，公安機關應依託聯席辦機制進一步推動警銀深化合作，強化警銀聯防聯控，在信息收集、數據分析、情報成果、應用回饋等方面建立資源融合機制，把間接協作變為直接協作，集合優勢資源，形成齊抓共管、全流程監控處置的開放式的犯罪治理格局。

1. 數據共用：建立雙重激勵機制

依託聯席辦機制通過人民銀行積極推動公安機關與銀行機構、第三方支付機構相關數據的即時共用，依法建立數據加密傳輸網絡，彙集各方反詐情報數據資源。在各銀行機構、第三方支付機構間建立情報數據的流轉市場，並將情報數據資源資產化、價值化，以市場化激勵機制，促進數據資產橫向流動。公安機關根據各銀行機構、第三方支付機構情報數據的貢獻度建立考核體系，定期考核並通報聯席辦，以行政考核激勵反詐情報數據共用，促進數據資產縱向流動。

2. 人才共用：開發共建式模型

反詐工作需要社會各界力量的共同參與，一方面，公安機關專家規則模型已無法適應不斷變化的電詐形勢，需要在銀行方面部署具有自主學習能力的算法模型，並借助銀行機構渠道進行涉詐風險交易的監測和管控，以實現降低發案，預防犯罪的目的。另一方面，在《反詐法》要求銀行機構加強自主反欺詐能力建設的大趨勢下，引入“第三方資源”與“合作開發模型”用於持續提升自身反欺詐能力，也逐漸成為多數銀行機構採用的方法。

[15] 運用《反詐法》以外部強制力填補內驅力，促使銀行轉變站位，使之從末端治理被動管控的角色轉變成為全程參與主動作為的主責部門。新的機制則是為這種共用與融合提供了最重要的制度保障，必將在資金流反制預警方面發揮出 1+1 > 2 的效果。新的機制則是為這種共用與融合提供了最重要的制度保障。

在此背景下，公安機關與銀行機構風控部門進行跨機構、跨部門的直接合作，彙集專業能力共建模型成為反詐工作的必經之路。通過組建電信網絡詐騙資金預警模型實體化專班，吸納公安與銀行模型開發領域的優質人才，以公安機關專家模型疊加商業銀行算法模型的方式，最大限度地發揮主管部門的業務優勢。

3. 過程共用：交叉核驗

為最大程度地發揮反制預警成功率，降低“誤傷率”，在預警情報產出環節，可進行跨行業間嫌疑信息交叉核驗。一方面，由公安將經前期工作或其他渠道發現的預警對象（一般為疑似犯罪嫌疑人和潛在受害人）推送給銀行核驗；另一方面，由銀行將在日常業務工作中發現的異常交易對象推給公安機關進行其他涉案信息核驗，以這種方式來織密金融體系的反欺詐網絡。

（二）提升監測預警技術

1. 建成涉詐風險識別算法模型集

模型建設是資金流反制預警工作的核心與基礎，反詐資金預警模型的設計者需要優先保證在精準度的基礎上，儘量提高模型覆蓋率。

圍繞以往案件建立黑樣本數據庫，結合嫌疑人洗錢行為和主觀供述重建犯罪場景，利用銀行機構多元數據模擬數位化犯罪場景，利用偵查異動思維進行分析，從客戶維度、帳戶維度、交易維度、設備維度、位置維度、操作維度抽取異常特徵，形成可解釋性強的專家規則犯罪模型。[16]

在專家規則犯罪模型的基礎上，運用機器學習、神經網絡、知識圖譜等算法，建立識別涉詐風險指標體系，實現從專家規則到智能算法模型的跨越，在原有專家規則基礎上不斷豐富集群風控維度。

建立覆蓋事前、事中、事後全流程的“專家規則 + 算法模型 + 灰名單庫”涉詐風險交易識別機制。一是通過事前模型主動感知風險隱患，輸出包含高風險客戶、帳戶、商戶、終端、位置等要素的交易信息，初步篩選疑似涉詐帳戶，形成灰名單庫。二是通過事中模型，監測和阻斷疑似涉詐帳戶的高風險交易，防範潛在被害人被騙、阻攔涉詐資金線上轉移。由銀行對模型識別的潛在被害人採取安全頁面提示、人臉識別、短信驗證、電話回撥核實等軟性干預措施，有針對性地進行風險提示和風險阻斷，降低被騙風險；對於模型識別的涉詐風險交易進行攔截，防止涉詐資金流出。通過設備指紋信息採集，加大對黑灰設備的數據挖掘力度，建立灰黑設備名單庫。通過地理位置的網格化管理，將建立高危涉案地點庫。強化與設備名單庫、高危地理名單庫關聯帳戶的風控力度。三是通過事後風險回饋信息回溯，不斷優化模型建設，迭代完善風控規則。以此實現反欺詐防控從樣本到全量、由模糊到精確、由因果到關聯的轉變，提升對欺詐風險的認知能力，將數據收集分析、數據驅動決策運用於反欺詐管理全過程，提升資金方面反詐風險防控能力。

2. 建成實戰一體化資金反制預警平台

相關主管部門應協同建立反制預警實戰一體化平台，以實現全流程閉環處置，有效提升資金流反制預警機制效能。一是即時分析，通過已建成的事前模型集進行全維度篩查分析，精準產出疑似涉詐帳戶。二是即時共用，即時將監測到的疑似涉詐帳戶通過數據共用機制轉遞平台中商業銀行開展佈控。三是即時攔截，由銀行對疑似涉詐帳戶產生的高風險交易第一時間攔截阻斷，並由銀行進行第一輪干預處置，提示潛在被害群眾。四是即時保護，銀行對高危潛在被害群眾採取保護性管控措施，並將信息推送至公安機關，由公安機關進行面對面式勸阻，避免群眾再次轉賬被騙。五是即時救濟。對於經勸阻能夠醒悟的被害人，即時推送銀行方面解除保護性措施。

（三）制定規範性文件

針對多部門協同治理過程中出現工作細則空位、技術方案不統一、標準有待規範導致的機制運行過程中“無章

[16] 犯罪模型是通過犯罪模式中犯罪要素相互關係的抽象化表達，來實現對犯罪機理的描述。構建數位化的犯罪模型的重要價值在於自動化篩查犯罪可能產生的風險點，進而在犯罪預防方面發揮重要作用。

可循”的問題，應當在《反詐法》的規定下，會同人民銀行反詐專班，圍繞目標任務、職責分工、業務規則、系統功能等內容，研究制定相關工作指引性文件，將有益經驗予以固定，並為今後的工作提供標準化、規範化的模式指引。

六、結語

電信網絡詐騙犯罪就是利用網絡的隱蔽性和信息的不對稱性誘導受害人上當，同時利用資金鏈條的複雜性與分拆轉賬的暫態性對抗公安機關的打擊與防範。以事後預警機制為基礎，以疑似涉詐帳戶資金反制預警機制為補充的資金流預警機制，符合當前電信網絡詐騙犯罪打擊治理的總體目標，也符合人民群眾的根本預期，應當成為當前及未來一段時期內對電詐資金流預警工作有益探索。為切實保護好人民群眾的“錢袋子”，最大程度避免人民群眾的經濟損失，貢獻現實路徑。