● 연구 보고서

전화금융사기 유형에 따른 제도적 대응방안의 검토

정 순 채*

Ⅰ. 문제의 제기

오늘날 인터넷 사용이 보편화[1] 되면서 각 개인의 인터넷상 금융거래정보를 노리는 범죄자들이 늘고 있다. 금융정보 등 타인의 개인정보를 절취하는 방법에는 종래 '해킹'이 널리 쓰였으나, 최근에는 피해자의 방심을 틈타 직접 피해자로부터 금융정보를 얻는 피싱(Phishing) 수법이 사용되고 있다.[2] 피싱이란 "피싱 공격자가 위장된 금융기관 등의 웹사이트나 전자메일로 고객을 현혹하게 하여 이들로부터 인증번호나 신용카드번호, 계좌번호 등 금융정보를 취득한 후, 이를 불법적으로 이용하여 피해자에게 재산상의 손해를 입히는 신종 인터넷 사기를 말한다.[3] 그런데 인터넷을

* 서울동대문경찰서 사이버범죄수사팀장, 경희대 국제법무대학원 인터넷법무학과 재학 중.

1) 한국인터넷진흥원(2010년 인터넷 이용실태조사보고서, 2010.09.29)의 자료에 의하면 2010년 5월 말 현재 인터넷 이용인구는 전체인구의 77.8%인 3,701만명으로 나타났다.

2) 피싱사기 및 이와 유사한 피망사기의 개요에 대하여는 정 완, "인터넷사기의 신종유형과 법제도적 방안", 경희법학 제40권 제1호(2005.6), 59~62면 참조.

3) 한국의 피싱사례는 외국에 비해 크지 않은데, 그 이유는 전자금융거래에 공인인증서를 사용할 뿐더러 비밀번호와 보안카드 사용 등 여러 장치가 복합적으로 사용되어 다른 나라보다 안전하기 때

이용한 피싱 수법에서 한 걸음 더 나아가 아예 피해자에게 전화를 걸어 금융기관, 수사기관 등을 사칭한 뒤 직접 개인정보를 물어보거나 송금하게 하는 이른바 보이스피싱(Voice Phishing)[4]이 늘어나 크게 사회문제화 되고 있다.[5]

보이스피싱이라고 하는 전화금융사기는 주로 중국 등 해외의 본거지에서 범행이 시도되는 특징이 있다. 전화라는 통신수단과 은행업무자동화기기[6]라는 금융수단을 이용하여 자금이체를 요구하거나, 금융정보를 탈취하는 수법의 선진국형·국제형의 신종사기 범죄이다.

이러한 전화금융사기는 최초에는 국세청의 세금환급을 빙자한 문자메시지 발송 형태의 전화사기에서 수사기관·금융기관·우체국 등 각종 기관을 사칭하거나, 또는 자녀납치 빙자 유형으로 변모하였다. 최근에는 위와 같은 수법을 혼합하여 활용하는 등 다양한 형태로 진화·발전하고 있다.[7]

2006년 중반부터 현재까지 발생되고 있는 전화금융사기는 국내의 수많은 피해자들에게 막대한 금전적인 피해를 주고 있다. 위와 같은 전화금융사기는 2010년 까지 전국적으로 2만건 이상이 발생되었으며, 그 피해금액도 2,000억원 이상에 이르는 것으로 집계되었다. 이와 같은 피해자는 대부분 정보가 빈곤한 부녀자, 노인 등 정보취약계층에서 전 국민으로 확대되고 있다.

또한 전화금융사기 피해자는 피해금이 인출되지 않았을 경우에는 금융기관의 지급정지 조치 후, 가환부[8]를 청구하거나 부당이득금 반환 청구소송[9]을 통해서 피해

문이다. 정 완, "인터넷사기의 최근 동향", 형사정책연구소식 95호(2006.6) 36면. 독일에서는 인터넷 뱅킹을 할 때 계좌번호, 비밀번호, 송금번호만 알면 계좌이체에 아무런 지장이 없다고 한다.

4) "귀하의 우편물이 반송되었으니…" 등의 전화녹음 멘트로 시작되는 보이스피싱은 음성(vioce)+개인정보(personal data)+낚시(fishing)의 합성어로 인터넷 전화 등을 이용하여 해커(Hacker)가 사용자에게 직접 전화를 걸어 음성으로 피해자들로부터 신용카드 번호나 신분도용에 사용될 다른 정보들을 받아서 이를 범죄에 사용하는 것을 일컫는다. 우리나라는 해커가 피해자로부터 직접 계좌이체를 하도록 하는 '전화금융사기'와 혼용하여 사용하고 있다. 최근에는 메신저(Messenger)를 이용하여 지인을 사칭하고서 금원 차용을 요구하는 방법의 메신저 사기도 빈번하게 발생되고 있으며, 접속지는 주로 중국으로 나타나고 있다.

5) 정 완, 「인터넷법 연구」, 한국형사정책연구원, 2009, 131면.

6) 은행업무자동화기기(Automatic Teller Machine : ATM)는 이용자가 비밀번호와 거래내용을 입력하면 은행 창구 직원이 맡고 있는 입금, 지급, 통장정리 등의 업무를 자동 처리해주는 기계를 말한다.

7) 금융 및 수사기관 직원 등을 사칭한 다수가 피해자에게 순차적으로 전화를 하여 피해자의 은행계좌번호, 비밀번호, 보안카드번호, 신용카드번호, 주민등록번호, CVC(Card Validation Code. 카드유효성 검사 코드) 등을 알아낸 후, 이를 이용하여 카드이지론 대출 및 현금 서비스를 받아 이체하거나, 검찰청 등 홈페이지를 가장한 피싱사이트를 이용하는 신종 수법이다.

8) 형사소송법 제133조 제1항에 근거하여 진행사건 종결 전에 압수의 효력을 존속시키면서 소유자·소지자 또는 보관자 등에게 잠정적으로 환부하는 제도를 말한다.

금을 반환받을 수 있다. 이는 지급이체를 지시하는 지급인이 착오로 송금하는 경우와 사기에 의한 의사표시로 입금한 경우가 유사하기 때문이다. 그러나 전화금융사기는 금융계좌 간 전자자금이체제도[10]를 악용하는 자들에 의해 피해자가 사기에 의한 의사표시로 지급지시를 한 것이라는 특수성에 비추어 현행법상의 구조제도는 피해자의 보호가 미흡한 것이 사실이다. 민사상 부당이득금 반환 청구소송은 소송제기에 반드시 필요한 사기계좌 명의인의 성명 및 주소 등 인적사항을 확보하기란 쉽지 않다. 또한 복잡한 소송절차에 많은 시간과 노력 및 비용이 수반되어 피해금액이 소액인 경우에는 소송제기를 포기하는 경우가 많은 실정이다.[11]

본고에서는 전화금융사기의 실체 및 수법, 전화금융사기의 원인 및 특징, 전화금융사기의 주요 유형, 전화금융사기 피해예방 요령, 주요 기관의 대책, 제도적 대응방안의 순으로 검토하고자 한다.

Ⅱ. 전화금융사기의 실체 및 수법

1. 전화금융사기범의 실체

가. 전화금융사기의 피해 사례

국내 전화금융사기 최초 피해사례는 2006년 5월 18일 피해자가 국세청을 사칭한 세금 환급금 관련 사기전화를 받고서 이에 속아 금 800만원을 송금한 사건이다.[12] 이후 위와 같은 전화금융사기는 지속적으로 발생하여 2010년까지 총 26,098건이 신고되었으며, 그 피해금도 2,591억으로 상당히 많은 금액의 피해가 발생하였다.[13] 하지만 이는 피해자가 경찰에 신고한 건수에 한하므로 실제로 발생된 건수는 더 많

9) 민법 제741조 (부당이득의 내용) 법률상 원인 없이 타인의 재산 또는 노무로 인하여 이익을 얻고, 이로 인하여 타인에게 손해를 가한 자는 그 이익을 반환하여야 한다.

10) '전자자금이체제도'는 은행권, 어음 등 종이에 의한 수단을 사용하지 않고, 컴퓨터와 데이터통신을 응용해서 전자신호에 의한 지불지시(전형적으로는 지불인·수취인 명의 계좌간의 이동)에 의하여 송금이나 결재 등의 자금이동을 행하는 시스템을 말한다.

11) 김수희·한영찬, "전화금융사기(Voice Phishing) 지급인 보호를 위한 금융법적 개선안 검토", 은행법연구 제3권 2호(2010.11), 은행법학회, 271면.

12) 2007년 4월 4일 경찰청에서 주최한 「보이스피싱 관계기관 실무협의회」 자료에 의하면 국내 최초의 전화금융사기 피해는 2006년 5월 18일 우리은행 인천 간석동 지점에서 피해자가 국세청을 사칭한 사기전화를 받고 800만원을 이체한 사건이었다.

13) 경찰청 보도자료, 2011.1.6.<www.police.go.kr>

을 것으로 생각된다. 피해자가 느끼는 자책감이나 체념, 사법당국에 대한 불신 등으로 인해 신고되지 않은 경우가 상당수에 이른다고 본다면, 실제 발생건수와 피해액은 이보다 훨씬 더 클 것으로 추정된다.[14]

2009년 3월 31일에는 경남 김해의 한 여대생이 아르바이트 등으로 모은 대학 등록금 640만원을 사기당하여 아파트 15층에서 뛰어 내려 투신자살하기도 하였다. 이 여대생의 죽음은 개인의 비극일 뿐 아니라 우리사회가 전화금융사기로 인한 고질병의 피해가 어느 정도인지를 보여주는 상징적인 사건이다. 이 같은 보이스피싱 범죄의 심각성은 금전적 측면을 넘어서 사람의 생명까지 위협한 것으로 피해를 당한 당사자가 죽음을 선택하게 할 정도의 극심한 고통을 안겨주고 있다.[15]

그러다보니 엉뚱한 피해가 속출하고 있다. 정상적인 업무상의 전화조차도 수신자가 불신하는 등 금융기관이나 관공서가 그들을 사칭한 보이스피싱의 역풍을 맞고 있는 것이다.

나. 전화사기 조직의 실체와 역할

전화를 이용한 전화금융사기 범죄는 조직적으로 이루어진다. 국경을 초월한 다국적 범죄의 실행을 위해서는 일반 범죄조직과 달리 철저한 비밀에 의한 위계구조를 갖춘 조직을 필요로 한다. 그래야만 각자의 역할 분담으로 나름대로 담당한 사기임무를 완수할 수 있기 때문으로 판단된다.

일반적으로 전화금융범죄 사기집단은 잠재적 피해자들에 대한 정보를 수집하고, 이들에게 사기전화를 거는 실행단계의 중국 소재 '콜센터'와 국내의 피해자로부터 계좌이체 받은 돈의 인출과 중국으로의 송금을 담당하는 '국내조직'으로 구성된다. 피해자의 돈을 인출하고, 이를 중국으로 운반하는 역할을 담당하는 '국내조직'은 '계좌모집조직-인출조직-환전·송금조직'으로 이루어진다. 각 하위조직들은 별개의 조직이나 서로의 이익을 위해 상호간에 긴밀하게 협조한다.[16] 이들 국내 조직은 점조직화된 행동대원들이다.

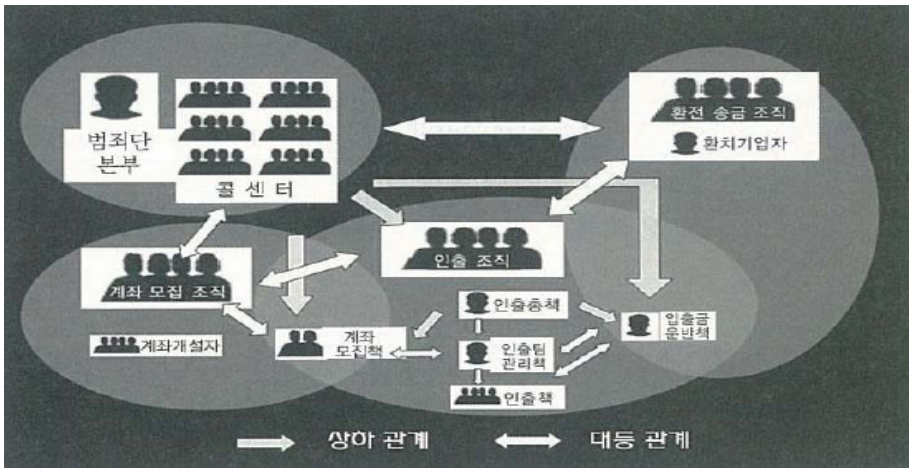
---

14) 권성언·양영진. "전화금융사기 범죄의 진화 : 보이스피싱(Voice Phising)의 피해구조 분석과 대응", 한국공안행정학회보-제32호(2008), 105면.

15) 현재까지 전화금융사기로 인한 자살 사례는 3건으로 나타났다. 2007년 2월에는 대전의 한 빌라에서 전화금융사기로 수백만원을 사기 당한 40대 여성이 스스로 목숨을 끊는가 하면, 2007년 7월에는 충북 청주에 사는 70대 노인이 금융기관 직원을 사칭한 전화를 받고 560만원을 사기당한 뒤 괴로워 자살하기도 하였다.

16) 권성언·양영진. 앞의 논문 124면.

<그림 1> 전화금융사기 범죄조직 네트워크 구성도



출처: 대한민국 국회입법조사처, "전화금융사기(보이스피싱) 대응책의 현황 및 개선방안", 현안보고서 제34호(2009.8.21), 4면.

전화금융사기의 총책은 중국 및 대만의 폭력조직(삼합회 산하의 신의안파[17], 대만 죽련방[18]) 등으로 국제전화 및 인터넷 전화 등 자국 및 해외의 전화망을 이용하여 경찰·검찰·금융기관·우체국 등 직원을 사칭하여 범행하고 있다.[19]

국내 수사기관에서 현금 인출책 등 행동대원을 검거하더라도 그 뿌리를 검거하기 어려운 실정이다. 국내에서 활동하는 인출책이나 송금책, 또는 은행통장 등 접근매체를 모집하는 모집책 등 국내하부 조직은 중국이나 대만에서 지시를 하는 사기범들에 대한 실체를 알 수 없다. 또한 현지에 거주하는 가족들의 살해 위협 등으로 실체를 안다고 하여도 쉽게 수사기관에 협조를 하지 못하고 있다. 전화금융사기와 같

17) 삼합회(三合會)는 홍콩을 거점으로 한 중국의 범죄 조직 중 하나로 청나라 말 유명한 반청복명(反淸復明) 조직인 천지회(天地會)에서 변질하였다. 이들은 마약밀매, 청부살인, 돈세탁, 도박, 매춘 등 흉악범죄를 일삼고 있다.
<http://ko.wikipedia.org/wiki/%EC%82%BC%ED%95%A9%ED%9A%8C> [2010.12.25. 방문]

18) 죽련방(竹聯幇)은 1만여 명의 조직원이 있는 것으로 알려져 있으며, 홍콩과 미국 등에 거점을 둔 거대 폭력조직이다. 이 조직은 지난 1997년 중국, 대만, 홍콩, 필리핀 등 6개국 거점 국제마약조직 수사당시 국내 폭력조직과 연계하여 히로뽕을 밀조한 사실이 알려지기도 하였다.
<http://kin.naver.com/pna/detail.nhn?d1di=6&dirld=613&dirld> [2010.12.25. 방문]

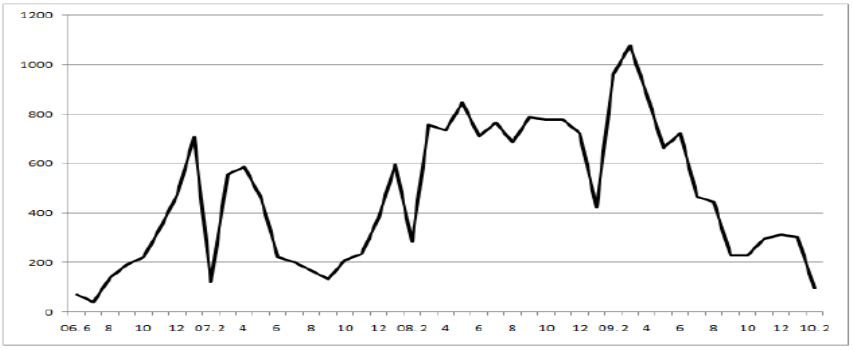
19) 전화금융사기 조직은 외국에 총책·지령책·센터를 두고, 국내의 조직도 현금인출책·관리책·송금책 등 체계적으로 구성하여 운영하고 있다.

은 형태의 다국적 범죄수사는 국가간의 상호 협조가 필수이나, 수사공조에 대한 한계가 발생한다. 인터폴 등을 통한 한국 경찰과 중국 공안과의 적극적이고 유기적인 협조가 잘 안되며, 그 조직들은 상대적으로 중국 공안의 힘이 적게 미치는 내륙지방으로 이동하여 활동을 하기 때문으로 판단된다.

다. 전화금융사기 발생 비교

위와 같은 전화금융사기는 최초 발생 이후 2008년까지 범죄발생이 증가하다가 2009년부터 감소추세에 접어들어 2010년은 2008년 대비 범죄발생이 35.4% 감소하였다.[20] 또한 각 년도의 월 발생건수를 비교해 보면 2월의 발생건수가 다른 달에 비해 현저하게 낮다는 것이다. 이 시기가 중국 최대명절인 춘절의 휴가기간과 겹치는 점으로 미뤄보아 일시적으로 중국의 '콜센터'도 휴가를 위해 활동을 중단한 때문이 아닌가 한다.[21]

<그림 2> 한국의 월별 전화금융사기 발생건수 및 피해액 추이

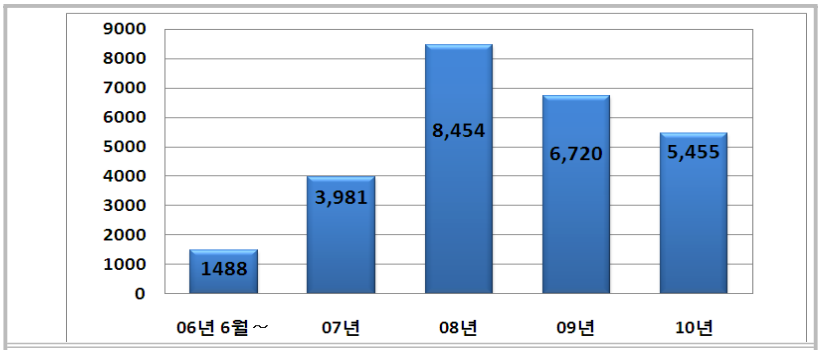


출처: 경찰청 보도자료, 2010.3.

그리고 우리나라 여름 휴가기간인 7~9월에는 발생빈도가 감소하는 경향이 있고, 그 후 연말까지 상승했다가 다시 감소하는 패턴이 나타난다. 이러한 경향은 범죄 피해자가 피해자의 직업이나 여가활동과 같은 일상성과 밀접한 관련이 있다는 일상활동이론[22]의 가설과 어느 정도 부합된다.[23]

20) 앞의 경찰청 보도자료 2면.
21) 권성언·양영진. 앞의 논문 116면.

<그림 3> 연도별 전화금융사기범죄 발생 현황



▸ 다각적인 대응결과 2008년을 정점으로 전화금융사기 발생건수 감소 추세

출처: 경찰청 보도자료, 2010.3.

이러한 전화금융사기는 2008년을 정점으로 발생건수가 감소 추세를 보이고 있다. 그 이유는 한국과 중국 경찰간의 상호 공조수사로 중국 현지 범죄조직의 활동이 크게 위축되었고, 국제전화 발신 표시[24] 등의 통신제도 개선과 ATM기 이체한도 제한 및 지급정지 등 금융권의 노력, 공익광고 등 각종 홍보활동의 영향으로 평가할 수 있다. 그러나 현재는 정보통신의 발달에 편승한 범죄수법의 발전으로 인하여 이동통신사의 발신번호 변경서비스를 이용 국내 경찰청 등 수사기관 및 국내은행 등 각 기관의 실제 전화번호를 표시하여 발신함으로써 전화수신자들을 더욱 혼란스럽게 하고 있다.[25] 사기단은 중국 인터넷망에 접속하여 070 인터넷폰을 이용하여 조작번호를 발신하거나, 발신번호 변경서비스를 하는 국내인터넷 전화업체를 이용하여 발신하게 되면 피해자는 관공서 등의 전화번호로 변경된 발신자 번호를 수신하게 된다.

22) '일상활동이론'은 대표적인 범죄피해에 관한 이론으로 일상활동의 요소와 범죄피해간의 관계를 설명하기 위하여 많은 수정과 확장과정을 격어오고 있으며, 특히 경험적 연구에서 더욱 두드러지게 나타난다.

23) 권성언·양영진. 앞의 논문 116면.

24) 2009년 5월 1일부터는 국제전화를 최초 접수한 통신사에서 식별번호('001'...'005' 등)가 표시되고 있다. 발신자 표시 서비스가 보편적 서비스가 아닌 사용자가 비용을 부담해야 하는 서비스임을 고려할 때, 발신자 표시 서비스를 받지 않는 사용자에 대한 정책적 고려로 2009년 10월 1일부터는 국제전화가 올 경우 이동전화 화면에 "국제전화입니다"라는 문구를 표시하고 있다.

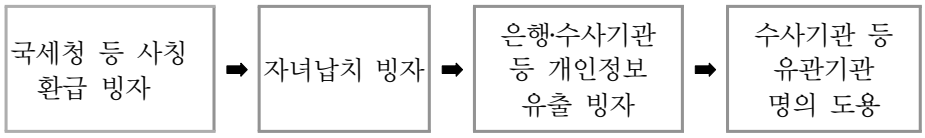
25) 금융사기 조직 중 콜센타에서 발신자 번호를 국내 경찰 및 검찰, 금융기관 등 유관기관에서 현재 사용하고 있는 번호를 표시하여 발신하고 있다.

2. 전화금융사기 수법

가. 전화금융사기 수법의 진화

전화금융사기 수법은 날로 진화하고 있다. 전화금융사기범은 일정 기간 금융기관 등 특정기관 직원을 집중 사칭하다가 대국민 홍보가 강화되자 사칭기관을 바꿔가면서 범죄행위를 계속하고 있다. 종전에는 환급금 지급 등 금전적 이득을 제공하는 것으로 하였으나 최근에는 "계좌보호 조치를 위한 것이다"라고 유인하고 있다. 이는 환급금 지급에서 신용카드연체로, 신용카드연체에서 납치협박으로, 납치협박에서 사건연루로, 사건연루에서 전화요금 연체로, 전화요금 연체에서 우체국 택배 반송 등의 방법으로 진행되었다.

<그림 4> 사칭유형 변화 현황



이러한 전화금융사기 수법의 유형을 파악해 두는 것은 동일 유형의 전화금융사기를 예방할 수 있기 때문이다. 최근에는 경찰·검찰 및 금융감독원 등 유관기관 명의로 전화를 거는 등 그 수법이 계속 진화하고 있음을 유의해야 한다.

사회현상에 편승하여 구제역 보상금 지급을 위해 계좌번호 등 정보를 요구하기도 한다. 검찰청 등 '공공기관'이나 '○○캐피탈' 등 금융회사 홈페이지를 가장한 피싱사이트[26]를 개설해 보이스피싱에 이용하는 방법의 신종 금융사기도 발생하고 있다.[27]

---

26) 범죄조직이 검찰청 등 수사기관 직원을 사칭하여 피해자에게 전화해 예금통장이 범죄에 연루되었다며, 피싱사이트로 위장된 검찰청 등 수사기관 홈페이지로 유도한 뒤, 피해자가 입력한 통장 계좌번호와 비밀번호 등의 금융정보를 이용해 돈을 인출한다. 또한 ○○캐피탈 등 금융기관과 비슷한 이름의 피싱사이트를 열어 놓은 후, 문자로 '대출을 해 준다'고 피해자들을 유인하여 계좌번호, 보안카드번호를 입력하게 하고서 대출금에 필요한 선이자를 입금하면 이를 편취하고서 바로 홈페이지를 폐쇄하는 방법이다. 접속 IP는 해외로 나타나는 것이 보통이다.

27) 경향신문(2011.01.20. 보도자료). 필자도 같은 내용의 피해로 인한 사건을 수사 중이다.
<http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201101190951571&code=940301> [2011.1.20. 방문]

나. 전화금융사기의 주요 유형[28)]

날로 진화하는 전화금융사기 주요 유형을 세분화하면 다음과 같이 4가지 유형으로 크게 나누어 볼 수 있다.

첫째는 '보호형'으로 경찰·검찰·법원을 사칭하여 사기사건에 피해자의 예금계좌가 연루되었다면서 예금보호 명목으로 피해자의 계좌번호 등 개인정보를 요구한다. 또한 은행·카드사·금융감독원 직원을 사칭하여 카드대금 연체 및 명의도용 등을 빙자하거나, 해당기관에 신고를 해주겠다면서 현금지급기 조작을 유도한다. 그리고 우체국을 사칭하여 우편물 및 택배, 카드 반송 등의 수법을 이용하여 개인정보가 유출되었다면서 현금지급기를 이용 이체하게 하는 방법이다.

둘째는 '보상제공형'으로 연금관리공단·국민건강보험공단·국세청·학교 교직원 등을 사칭하여 과납한 보험금, 세금, 등록금 등 환급금을 돌려준다면서 현금지급기 조작을 유도하는 수법이다.

셋째는 '협박형'으로 폭력조직을 사칭하여 자녀납치 및 가족 상해 협박 등의 수단을 이용하여 피해자의 예금계좌를 이체하게 하는 방법이다.

넷째는 '의무부과형'으로 동창회·종친회·대학교 등을 사칭하여 동창회비나 종친회비, 또는 대학 추가 합격자 등록금 납부 등의 방법으로 계좌를 이체하게 하는 방법 등으로 그 수법도 다양하다.

다. 최근에 발생하는 유형

여론조사기관, 고객 감사 이벤트 당첨, 또는 농업 직불금·보조금 지급 등의 방식으로 유인하는 등 그 방법도 다양하게 지속적으로 발생되고 있다. 또한 최근에는 피해자가 공신력 있는 기관을 사칭하면 쉽게 믿는 점을 이용한다. 금융회사와 경찰, 금융감독원 등 공공기관의 발신번호를 조작해서 범죄조직 각자의 사전 각본에 의해 순차적으로 피해자에게 전화를 건다. 피해자의 은행 계좌번호, 비밀번호, 보안카드 번호, CVC 등의 개인정보를 알아낸 후, 이를 이용하여 피해자 명의로 카드이지론 대출을 받거나 현금 서비스를 받아 이체하는 신종수법도 등장했다.[29)]

그리고 다른 사람의 인터넷 메신저 아이디를 도용하고서 지인을 가장해 송금을

28) '전화금융사기 주요 유형' 구분은 경찰청·금융감독원, "주요 불법금융거래 유형 및 해설", 2009.9. 133면 '도표'를 참조하여 구분하였다.

29) 각주 7) 참조.

요청하는 메신저 이용사기도 자주 발생하고 있다. 메신저 이용사기는 타인의 메신저를 해킹하여 친구로 등록된 지인들에게 돈을 차용하거나,[30] 메신저를 이용하여 피해자들에게 소액결재를 유도한다. 메신저를 이용한 대화 중 '금전, 비용, 차용' 등의 단어가 입력이 되면 이를 경고하는 내용의 문구가 나타남에도 불구하고, 이를 무시하고 송금을 하므로 피해가 발생한다.[31]

이 같은 메신저이용 사기는 범행 3~4일전에 소셜네트워크서비스(SNS) 아이디를 해킹해 가족, 친구, 친척 목록까지 알아낸 다음 메신저에 접속한다. 일부 SNS는 포털과 자동 연계되어 해킹되면 일촌 목록이나 쪽지까지 해커에게 노출된다. 해커들은 이 정보를 이용, 말투를 흉내 내고, 개인적인 사건을 언급해 피해자의 의심을 막는다. 이런 범죄 형태는 무작위로 전화를 거는 보이스피싱과는 다른 유형으로 트위터 등 SNS를 이용한 보이스피싱의 진화이다.[32]

<그림 5> 대검찰청 홈페이지 도용 피싱사이트

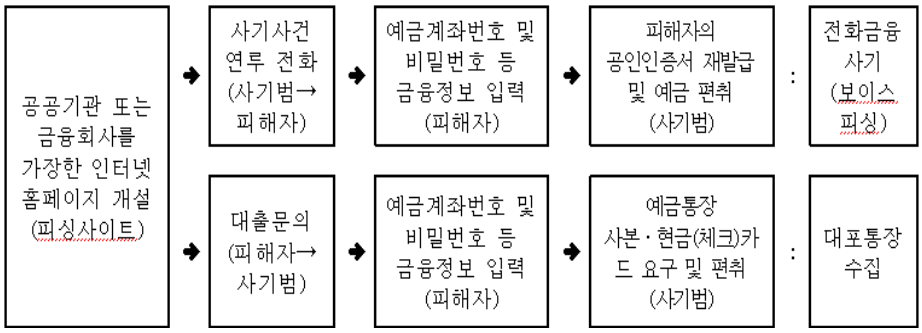
또한 금융사기범이 공공기관 또는 금융회사의 인터넷 홈페이지를 가장한 피싱사이트를 개설하여 전화금융사기에 이용하는 신종 사기수법도 발생되었다. 이 수법은 사기범이 검찰청 직원을 사칭하고 피해자에게 전화하여 피해자 명의의 예금 통장이 사기사건에 연루되었다면서 검찰청 출석을 요구한다. 피해자가 이를 의심하면 개인

30) 타인의 메신저를 해킹하여 등록된 친구들이나 지인들에게 "급하게 병원비가 필요하다. 가족이 교통사고가 났다"라고 피해자를 기망하여 송금을 유도한다.
31) 대화시 "지인을 사칭하거나 급박한 상황을 빙자한 금전 피해 사례가 빈번하게 발생되고 있으니, 금전 요구시 전화로 반드시 대화 상대를 확인하십시요"라는 적색 경고 문자가 표기된다.
32) 경향신문(2011.01.20. 보도자료), <http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201101201057145&code=940202. [2011.01.20 방문]

정보가 유출된 것 같다며, 검찰청 홈페이지를 가장한 피싱사이트로 유인하여 피해자의 금융정보를 동 피싱사이트에 직접 입력하도록 유도한다.[33] 그 후 피해자가 입력한 금융정보로 공인인증서를 재발급 받아 인터넷 뱅킹을 통해 피해자의 계좌에서 사기계좌로 예금을 이체하여 편취한다.[34]

사기범은 대출광고를 휴대전화 문자메시지로 발송해 이를 보고 연락한 대출희망자를 '△△캐피탈' 등 금융 대출회사 상호와 유사한 명칭의 피싱사이트로 유인한다. 피해자가 해당 피싱사이트에 접속하면 "대출금을 수령 받을 계좌를 확인 하겠다"는 명목으로 피싱사이트에 예금계좌번호 및 비밀번호 등 금융정보를 입력하도록 유도한다. 그 후 해당 계좌의 예금통장 사본과 현금(체크)카드를 택배 등을 통해 받은 후 이를 전화금융사기 등에 이용하는 것으로 보인다.[35]

<그림 6> 신종 사기수법 흐름도



Ⅲ. 전화금융사기의 원인 및 특징

1. 전화금융사기의 원인

2009년에 한국형사정책연구원이 실시한 범죄피해 조사에 의하면 만 14세 이상의 응답자 10,671명중 71.5%가 2008년 한 해 동안 누군가로부터 송금이나 금융정보

33) 인터넷뱅킹 이용자 ID, 주민등록번호, 예금계좌번호 및 비밀번호, 보안카드번호 등을 입력하도록 한다.
34) 금융감독원 보도자료(2011.01.20).
35) 위의 금융감독원 보도자료.

를 요구하는 '보이스피싱' 전화나 이메일, 문자 메시지를 받은 적이 있었던 것으로 나타났다.[36] 이 조사에서 응답자의 1.3%가 피싱 전화인지 모르고, 실제로 송금(0.2%)을 하거나 개인정보·금융정보 등(1.1%)을 알려줬던 것으로 밝혀졌다.[37] 즉 최소 100명 중 1명에게 실질적인 피해가 발생되었던 것으로 집계되었다. 일반사람들이 공공기관에 대해 갖는 신뢰감을 이용한 새로운 유형의 범죄는 피해자들에게 직접적인 경제적 피해를 야기하고 있을 뿐만 아니라 공적신뢰의 훼손, 타인에 대한 불신, 낯선 전화번호에 대한 두려움의 유발이라는 사회비용을 초래하고 있다.[38]

대만에서는 2000년대 초반부터 전화를 이용한 사기가 사회문제로 급부상하였다. 대만 정부의 강력한 대응조치가 취해지면서 2005년 이후 상황이 다소 진정되었다. 그러나 그 시기에 즈음하여 한국, 일본[39], 홍콩, 싱가포르 등 이웃 국가들은 새로운 사기 범죄로 인해 큰 혼란을 겪게 된다. 이는 전화나 다른 통신매체들을 이용하는 새로운 유형의 범죄가 공간적으로 전이되었음을 짐작하게 하는 부분이다.[40]

우리나라는 정보통신망의 발달로 인하여 이동전화의 보급과 편의점 등 주변에 설치된 금융기관 자동화기기의 보급이 잘 되어 있다. 그리고 중국·대만 등 현지에서 우리언어를 능숙하게 구사할 수 있는 조선족을 쉽게 고용할 수 있어 언어문제 해결이 쉬워 전화금융사기의 표적이 된 원인 중의 하나이다. 또한 은행에서 통장 및 현금카드의 발급이 쉽고, 은행자동화기기의 계좌이체 및 인출한도가 고액인 점 등이 주요 원인으로 타나난다.

한편 국민의 공공기관에 대한 신뢰감이 높은 상황에서 사기범들이 이동통신요금 인하, 우편물(카드) 반송, 자녀납치 협박 등 사회적 이슈가 될 만한 사기수법을 계속 개발하고 있다. 그리고 각 기관의 홍보효과도 상당히 제한적이어서 노인 및 주부 등 정보 소외계층이 존재하기 때문에 향후 상당기간 전화금융사기는 계속 될 것으로 전망된다.

---

36) 김은경·최수형·박정선, "2008년 한국의 범죄피해에 관한 조사연구(Ⅵ)", 한국형사정책연구원, 2009. 163면.
37) 위 논문 166면.
38) 권성언, "전화금융사기 범죄의 대한 한국 사회의 대응 : 대만과의 비교 분석", 형사정책 제22권 제1호(2010. 7), 10면.
39) 김범수, "일본도 '보이스 피싱'과의 전쟁", 한국일보, 2008.10.13. 이윤주, 국회입법조사처, 앞의 방안 17면.
40) 권성언, 앞의 논문 10면.

2. 전화를 이용한 금융사기의 특징

가. 전화를 이용한 금융사기

전화금융사기 범죄는 일반사기 범죄와 마찬가지로 피해자를 기망하여 이에 속은 피해자가 착오로 계좌이체를 하는 형태이다. 위와 같이 착오에 빠지는 것은 사기범들의 기망행위가 공적 혹은 사적 '신뢰'에 의존하고 있기 때문이다. 특히 사기행위가 비대면적 상황에서 발생하기 때문에 피해자들은 오직 사기범들이 전달 또는 지시하는 내용의 진위여부만을 판단할 수 있을 뿐이다. 사기범들이 사칭하는 대상은 대개 공공기관이거나 사적으로 친분이 있는 집단, 혹은 인물들이다. 피해자들에게 공공기관은 권위와 전문성의 상징으로 다가오며, 그들의 견해나 지시는 피해자들을 쉽게 움직이게 한다. 사적인 친분과 친밀성에의 호소는 어려움에 처한 가족, 친척, 친구 집단에 의한 사회적 지지(social suport)의 감정을 이끌어냄으로써 피해자들의 인지착오를 유발하는 원인으로 작용한다.[41]

전화금융사기 범죄의 수법은 끊임없이 진화하는 특성을 보인다. 자신들의 수법이 널리 알려졌다고 판단되면 사기범들은 사칭기관이나 유인방법을 달리하면서 당시의 주변 상황에 맞게 새로운 수법으로 옮겨간다. 이는 범죄의 전술적 전이(tactical displacement)에 해당한다.[42]

국내 전화금융사기 범죄의 유형 변화는 초기에는 국세청 및 국민건강보험공단을 사칭한 '환급금 빙자'에서 금융감독원 또는 금융회사를 사칭한 '신용카드 연체빙자'로 변하였다. 그리고 자녀들을 납치하였다는 형태의 '납치협박 빙자'에서 법원·경찰·검찰을 사칭한 '수사기관 사칭' 형태로 변하였다. 그 후 통신회사를 사칭한 '전화요금 연체 빙자'에서 우체국 또는 택배회사를 사칭한 '택배사칭'의 순서로 주요 전술적 기법들이 계속 진화한 것이다.

전화금융사기범들이 사칭하는 기관이나 유인방법들은 당시의 사회상황 및 정치적·사회적 현안과도 밀접한 관련이 있다. 2008년도에는 증권회사를 사칭한 전화금융사기가 발생하였다.[43] 최근에는 이동전화를 이용 문자메시지를 발송하는 수법도 늘어나고 있다.[44]

---

41) 권성언, 위의 논문 16면.

42) Reppetto, T. A., "Crime prevention and displacement phenomenon," Crime and Delinquency 22, 1976.

43) 금융감독원, "증권회사를 사칭한 전화금융사기 주의 요망", 보도자료, 2008.3.12.

전화금융사기의 주요특징은 해외로부터 ARS 등을 이용하여 전화를 하기 때문에 통화 감도가 떨어지는 경우가 많으며, 조선족 등을 고용하여 어눌한 우리말을 사용하고 있다. 그리고 조목조목 되묻거나 강경하게 대처하면 전화를 도중에 끊으며, 발신자 번호를 조작하여 전화하므로 실제로 발신자 번호로 전화를 해보면 통화가 불가능 하는 등의 특징이 있다.

끝으로 피해자와 사기조직의 특징을 살펴보면 전화 금융사기의 피해자는 무방비 상태이고, 혼자 고립되어 계좌이체를 한다. 반면에 사기범들은 다수가 조직적으로 연결되어 있고, 사전에 치밀하게 준비를 하여 역할 분담을 한다는 것은 쉽게 추측할 수 있다. 피해자도 지역적 한계는 있으나 경남창원중부경찰서의 자료에 의하면 대부분 서민층에 속하는 사람들로 보고 있다.[45] 이들의 평균 피해액이 803만원으로 금융기관에 투자한 예금이나 자산이 많은 사람들은 금융기관에서도 특별고객으로 관리를 하고 있는 경우가 많다. 때문에 사기전화를 받더라도 금융기관 직원에게 바로 전화를 하여 문의할 가능성이 많은 것으로 추정되기 때문이다.[46]

나. 메신저를 이용한 금융사기

국내에서 전화금융사기에 대한 예방과 단속활동이 강화되자 해킹 등을 통해 타인의 메신저 아이디를 도용하여 지인으로 등록되어 있는 사람인 것처럼 속여 금원을 요구하는 소위 '메신저피싱'이 새롭게 등장하였다.

2010년 1월의 발생건수는 109건이었으나 8월에는 810건으로 크게 증가하였으며, 피해금액 역시 같은 기간 9,400만원에서 14억 6,900만원으로 급증하였다. 여기서 흥미로운 사실은 2009년도 3월에서 8월까지 월별 전화금융사기의 감소 추세와

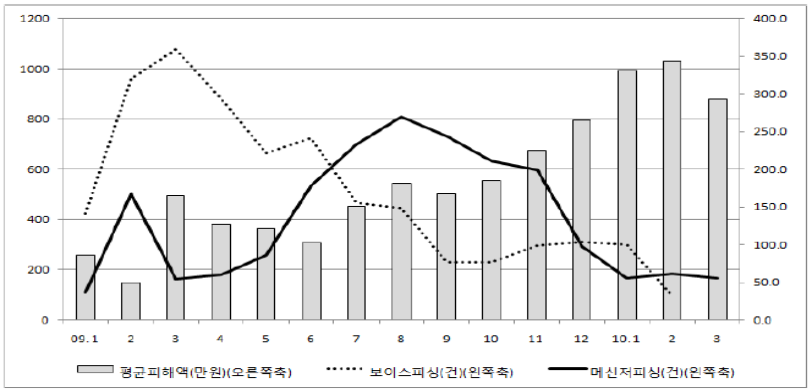
---

44) 이동전화 문자 메시지의 구체적 형태는 ① 동창회나 종친회 등의 연락처를 입수하여 회원들에게 회비 납부를 요구하거나, 또는 돈을 빌려 달라는 문자 메시지를 발송하여 자금이체를 유도한다. ② 이동전화 문자 메시지를 이용하여 해외 및 국내 백화점 등에서 신용카드가 결재되었다는 문자 메시지를 무작위로 전송한다. 그 후 사용 내역을 확인하려는 피해자들로부터 카드번호나 유효기간 등 필요한 정보를 입수하여 획득한 개인정보로 인터넷이나 전화로 물건을 구입하고, 이를 되팔아 현금화하는 방법 등이 있다. 특히 ② 항의 유형은 신용카드가 보편화됨에 따라 신용카드 사고를 예방하고자 하는 카드 이용자들의 심리와 행동을 역이용한 수법이라는 데서 우려할 만 하다.

45) 2006.11.~2008.3.까지 경남창원중부경찰서 관내에서 발생한 136건의 사건을 분석한 자료이다. 이봉한. "전화금융사기범죄의 유형과 전망", 수사연구, 2008.8. 13면. 양영진, "보이스피싱 범죄의 근절 방안에 관한 연구", 경남대 석사논문, 2008, 40~41면.

46) 정 완, 앞의 글 139면.

<그림 7> 2009년 월별 메신저피싱 발생건수 및 건당 피해 금액 추이



출처: 경찰청 자료, 2010.4.

메신저피싱 사기범죄의 증가 추세가 맞물리고 있다는 점이다.

메신저를 이용한 사기범죄는 2009년 8월 최대치에 이른 이후 점차 감소하는 추세이다. 그렇지만 2009년 말까지 메신저피싱의 월별 발생빈도는 전화금융사기보다 훨씬 높다. 이러한 결과는 전화를 이용한 금융사기에서 메신저를 이용한 금융사기로의 전이가 일어나고 있음을 짐작하게 한다.[47] 2009년 8월 이후로 메신저피싱의 발생건수는 감소하고 있지만, 월평균 피해액은 오히려 증가하고 있어 향후 추이를 지켜봐야 한다.[48]

다. 일반사기 범죄와의 비교

형법상 사기범죄의 구성요건은 "사람을 기망하여 재물의 교부를 받거나 재산상의 이익을 취득한 자"이다.[49] 일반적으로 사기범죄의 개념은 법률상 타인에게서 금전적으로 유가치한 재물 등을 빼앗을 목적으로 행한 고의의 허위표시행위이다.[50]

47) 경찰청 c었던 자가 다수 포함되어 있다고 한다.

48) 권성언, 앞의 논문 18면.

49) 형법 제347조(사기) 제1항은 사기행위에 대하여 10년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. 제2항은 제1항의 방법으로 제삼자로 하여금 재물의 교부를 받게 하거나 재산상의 이익을 취득하게 한 때에도 전항의 형과 같다. 그리고 제347조의2(컴퓨터등 사용사기)는 컴퓨터등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력·변경하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 한 자는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

50) 허위표시란 우리 민법상의 개념으로 표의자가 상대방과 통정하여 행하는 진의 아닌 의사표시를

사기는 그 자체로서 하나의 범죄를 구성하기도 하지만, 대개는 허위의 표시나 연기를 통해 금전을 편취하는 경우와 같이 범죄의 한 요소를 이룬다.

사기만큼 유형이 다양한 범죄를 발견하기도 어려울 것이다. 외형상 비슷하게 보이는 사건들도 수법이 서로 다르고, 피해대상이나 피해자의 특성에 차이가 많기 때문이다. 그러므로 사기범죄는 유형을 구분하기가 매우 어렵게 보일 수도 있으나 유형분류가 불가능한 것은 아니다. 각양각색의 사건마다 고유성을 지니면서도 원리가 비슷한 경우가 많기 때문이다.[51]

사기범죄도 국제화 및 개방화로 전이되고, 첨단화 되었다. 정보통신기술의 발달은 사기범죄의 국제화에 결정적 영향을 미쳤다. 사기범죄의 지능화, 첨단화 추세는 컴퓨터와 정보통신기술이 조성하는 사이버공간의 피해사례를 통해 극명하게 확인된다. 인터넷이 가진 강력한 전파력과 저비용, 익명성 환경이 신종사기를 속출시키는 것이다. 전자상거래가 급성장하면서 '인터넷사기' 피해가 속출하고 있다.[52]

반면에 전화금융사기는 앞에서 서술한바와 같이 피해자가 전혀 인식이 없는 상태에서 어느 순간 전화 등 정보통신에 의한 원인으로 인하여 피해가 발생된다. 피해대상도 오프라인 범죄와 달리 피해자가 특정되지 않은 상태에서 무작위로 발생한다. 피해 금액 또한 피해자의 금융환경에 의하여 결정되는 지능형 신종범죄이다. 이는 정보통신환경의 발달로 인한 범행용이성, 자료 절취 및 위변조의 용이성 등의 특징이 있다.

전화금융사기는 음성에 의하므로 표정이나 범인의 정체를 확인하기 어렵고, 피해가 비교적 단기간에 이루어진다. 범행을 위해서는 세련된 연기력이 필요한 것은 일반 사기와 마찬가지이다. 과거에 보이던 초보적 형태의 전화사기와 달리 최근에는 범죄조직이 치밀하고, 국내 및 국제 통신망을 이용한다는 특징이 있다. 그리고 피해 규모가 크다는 점을 보면 상당히 교묘하게 진화된 신종사기 유형에 속한다고 볼 수 있다. 그렇지만 사기범죄의 기본 구성요건인 기망이 크게 유인(enticement)과 위

말한다. 허위표시가 성립하려면 의사표시가 있어야 하며, 의사와 표시가 일치하지 않아야 한다. 표의자 스스로가 그 불일치를 알고 있어야 하며, 진의와 다른 의사표시를 하는데 상대방과 서로 통정을 해야 한다. 이때 허위표시의 이유나 동기는 상관없다.

51) 사기범죄는 시장영역별로는 ▷국민경제부문(신용카드 사기 등 금융거래 차원 및 토지관련 사기 등 부동산거래 차원) ▷상품판매 및 구매사기 등 기업경제부문 ▷월부 및 할부 사기 등 소비자 및 일반인의 경제활동부문과, 생활세계 일반영역으로는 ▷차용사기 등 개인 간의 비공식적 금융거래부문과 ▷동업사기 등 일상사부문으로 크게 나눠볼 수 있다.

52) 경찰청 보도자료(2011.1.17)에 의하면 최근 3개월 동안 인터넷 사기를 집중단속 한 결과 사기 쇼핑몰과 온라인 게임 사기 등 인터넷 사기로만 5,519명을 검거하여, 그 중 105명을 구속하였다.

하(scare) 전술을 통해 이루어지는 것은 전화금융사기에서도 예외는 아니다.[53]

Ⅳ. 전화금융사기의 유형 및 대처 요령

1. 전화금융사기의 주요 유형

전화금융사기 수법은 범행 방법 및 수법 등 형태에 따라 환급빙자형(세금형), 수사기관 사칭형(사건연루 등), 납치빙자 협박형, 통신회사 사칭형, 우체국 직원 사칭형 등으로 크게 분류할 수 있다.[54] 이렇게 유형을 나눠보는 이유는 전화금융사기임을 용이하게 식별하고 그에 대한 대책을 마련하기 위함이다.

가. 환급빙자형(세금 등)

'환급빙자형'은 전화로 "국세청 징수과입니다. 고객님의 과납세금 00만원을 환급해 드리고자 하니 문의사항이 있으시면 9번을 눌러주세요"라는 녹음된 멘트를 발송한다. 피해자가 이를 듣고 '9'번을 누르면 전화를 받는 사기조직은 "국세청 징수과 직원"이라고 사칭한다. 피해자의 이름과 주민등록번호를 물어보고, 과납된 세금 등에 대한 환급서류를 작성하여 정산과에 통보한 후, 다시 연락하겠다며 이동전화 번호를 물어보고 전화를 끊는다.

잠시 후 "국세청 정산과 직원"이라면서 피해자의 휴대폰으로 전화를 하여 자주 이용하는 은행 카드나 통장을 휴대하고, 가까운 현금지급기로 가서 환급을 받아야 한다며 현금지급기로 유인하고서 전화를 끊는다. 피해자가 현금지급기에 가면 이동전화로 다시 전화를 걸어 입금 받을 은행카드를 넣고, "이체"를 누르게 한 뒤, "환급인증 절차"를 빙자하는 방법으로 현금지급기를 조작하게 하여 자금을 이체 받아 편취한다.

---

53) 이봉한, "전화금융사기의 유형과 피해자 분석-한국과 일본의 비교", 한국범죄심리연구 제4권 제2호(2008), 169면.

54) '전화금융사기의 주요 유형'은 경찰청·금융감독원, 앞의 글 135~137면.

나. 수사기관 사칭형(사건연루 등)

‘수사기관 사칭형’은 일반전화로 “검찰청(법원)입니다. 법정출두 일시에 출두하지 않아서 2차 기한까지 출석을 요청합니다. 상담을 원하시면 ‘9’번을 누르세요”라는 녹음된 멘트를 발송한다. 피해자가 이를 듣고 ‘9’번을 누르면 “검찰청(법원) 직원”이라며, “사기사범을 검거했는데, 피해자 명의의 계좌번호를 사용하고 있으니, 담당 형사에게 통보해 주겠다”며, 이동전화 번호를 물어보고서 전화를 끊는다.

잠시 후, “경찰관을 사칭”한 사기조직이 전화를 걸어 사기사건에 연루되었다면서 신분증 분실 여부, 주민등록번호 등 개인정보 및 계좌번호 등을 물어본 후, “계좌정보가 노출된 것 같다. 금융감독원에서 계좌안전조치를 해줄 것”이라고 속여 현금지급기에 가서 기다리도록 한다. 피해자가 이를 진실로 믿고 현금지급기에 가면, 또다시 “금융감독원 직원”을 사칭하여 전화를 걸어 피해자 사용의 은행계좌에 ‘안전코드’를 설정해 주겠다며, 현금지급기를 조작하게 하는 방법으로 자금을 이체 받아 이를 편취한다.

다. 납치빙자 협박형

‘납치빙자 협박형’은 아들 등 사전에 자녀의 휴대폰 번호와 집 전화번호를 파악하여 아들 휴대폰으로 계속 전화를 걸어서 욕을 하는 등 귀찮게 하여 전화를 끄게 한다.[55] 위와 같이 전화가 꺼짐을 확인하고서 피해자의 집으로 전화를 하여, “당신 아들과 아들 친구를 납치했는데 아들 친구는 돈을 줘서 풀어줬으니, 0천만원을 입금하라, 입금하지 않으면 옥상에서 떨어뜨려 죽이겠다”고 협박하여 자금을 이체 받아 편취한다.[56]

라. 통신회사 사칭형

‘통신회사 사칭형’은 피해자의 일반전화로 전화를 걸어 “안녕하십니까. ○○텔레콤입니다. 고객님이 과다하게 사용하신 통신요금 00만원을 징수하고자 하오니 문의사항이 있으시면 ‘9’번을 눌러주세요”라는 녹음된 안내 멘트가 나온다. 이를 듣고

55) 피해자가 자녀에게 전화를 하여도 자녀의 이동전화가 꺼져 있기 때문에 통화가 안된다. 때문에 피해자는 심리적으로 불안하여 사기전화의 내용을 진실로 믿게 된다.

56) 전화로 폭행을 가하는 소리와 아이들 울음소리를 들려주며, 피해자로 하여금 공포분위기를 느낄 수 있도록 한다.

피해자가 '9'번을 누르면 사기조직이 "○○텔레콤 직원"이라며 전화를 받는다. 이름과 주민등록번호를 물어보고서 "징수서류를 작성하여 징수과에 통보한 후 다시 연락주겠다"면서 이동전화 번호를 물어보고 전화를 끊는다.

그리고 피해자가 사용하는 이동전화로 전화를 하여 "○○징수과 직원"이라며 자주 이용하는 은행카드나 통장을 휴대하고 가까운 현금지급기로 가서 입금처리를 해야 한다면서 현금지급기로 유도를 하고서 도착시간을 확인한 후, 전화를 끊는다. 피해자가 현금지급기에 가면 이동전화로 다시 전화를 하여 입금 받을 은행 카드를 현금지급기에 넣고 '이체'를 누르게 한 뒤, "입금 인증 절차"를 빙자하여 현금지급기를 조작하게 하는 방법으로 자금을 이체 받아 편취한다.

마. 우체국 직원 사칭형

'우체국 직원 사칭형'은 위의 '환급빙자형' 유형과 유사한 형태로서 일반전화로 전화를 하여 "안녕하십니까, 우체국 직원 ○○○입니다. 고객님에게 발송된 카드가 반송되었습니다. 상담을 원하시면 9번을 누르세요"라고 ARS 메시지를 발송한다. 이를 듣고 피해자가 9번을 누르면 전화를 받는 사기조직원이 "우체국 직원"이라며, 이름과 주민등록번호를 물어보는 등 개인정보를 파악하여 빼내가거나, 개인정보가 노출되었으니 경찰에 신고해 주겠다고 하고 전화를 끊는다.

그 후에 경찰을 사칭하는 자가 전화를 하여 "피해 접수를 해 주겠다"고 하면서 "금융거래 안전을 위해 금융감독원 직원을 연결해 준다"고 하고서 전화를 끊는다. 이후 금융감독원 직원을 사칭하는 자가 다시 피해자에게 전화를 하여 계좌안전조치를 위해 현금지급기로 가라고 하면서 계좌이체를 유도하여 자금을 편취하는 방법이다. 위의 각 사기 유형은 각각의 사기집단 조직원들이 역활 분담을 하는 형태이다.

위의 주요 유형은 또한 보호 형태에 따라 '환급빙자형, 수사기관 사칭형' 등은 '보상제공형'이나 '보호형'으로 재 구분할 수 있다. '보상제공형'이나 '보호형'의 경우 범행은 대개 "기망에 의해 인지적 착오가 발생한 피해자를 현금인출기로 유인한다. 전화로 불러주는 해당기관의 인증코드나 보안설정번호를 입력하라고 속이고 계좌이체를 하게 한 다음, 이를 인출하여 편취하는 방식으로 범행이 진행된다. 이때 피해자는 자신의 계좌에서 사기조직이 사용하는 계좌로 돈이 이체된다는 사실, 즉 사기조직에게 돈을 직접적으로 교부했다는 사실을 전혀 인식하지 못하는 상태에서 피해를 당한다.

반면 '납치빙자 협박형'이나 동창회비 등을 납부하도록 하는 '의무부과형'과 같은 전화금융사기 형태는 피해자가 인식을 한 상태에서 피해가 발생된다는 것이 '보상제공형'과 차이가 있다. 사기조직들이 미리 타인 명의로 계좌가 개설된 일명 '대포통장'[57]의 계좌번호를 불러주면서 피해자로 하여금 강제로 돈을 이체하게 하는 방법이다. 피해자는 기망에 빠져 사기조직에게 스스로 직접 돈을 교부하는 것이다.[58]

2. 전화금융사기의 대처요령

가. 무대응의 원칙

전화를 이용하여 계좌번호, 신용카드번호, 주민등록번호 등 개인정보를 요구하는 경우에는 일체 대응할 필요가 없다. 금융회사나 수사기관, 또는 감독기관에서는 전화를 이용하여 개인정보나 금융거래정보를 요구하는 경우는 없으므로 이러한 경우는 모두 전화금융사기 전화이다.[59] 현금지급기(CD/ATM)를 이용하여 세금 또는 보험료 환급, 등록금 납부 등을 해준다는 안내에도 일체 대응하지 말아야 한다. 이는 금융기관, 국세청, 법원 등에서는 현금지급기를 이용하여 환급을 해주는 경우는 없기 때문이다.[60]

우체국에서는 자동응답시스템전화(ARS)를 이용하여 카드 또는 소포 등의 도착 및 반송에 대하여 안내를 하지 않는다. 때문에 ARS전화를 이용하여 우체국 카드 또는 소포(택배) 등의 도착 및 반송에 대해 안내하는 경우에는 반드시 가까운 수사기관에 신고할 필요가 있다. ARS를 이용한 사기 전화이기 때문이다. 전화나 문자메시지로 은행직원 등이라 기망하여 카드대금 연체, 카드부정발급 등에 대한 조사를 위하여 필요하다면서 자동응답시스템으로 통화를 유도한다.[61] 그 후에 계좌번호, 카

57) 대포통장은 금융실명제를 위반하고, 제3자의 명의를 도용해서 만든다. 통장의 실사용자와 명의자가 각각 다른 통장을 지칭하는 것으로 주로 탈세 및 금융사기 등의 범죄에 이용될 가능성이 높다.

58) 권성언·양영진, 앞의 논문 122면.

59) 국민연금관리공단 및 국민건강보험공단을 사칭 세금 환급, 은행·카드사·통신회사를 사칭 카드 대금 및 서비스 이용요금 연체, 경찰 및 검찰 등 수사기관을 사칭 출석요구 및 범죄연루를 빙자한 개인정보 및 금융거래 정보를 요구한다.

60) 피해자로 하여금 세금 환급, 대학 등록금 환급, 장학금 지급을 위해 ATM 기기로 유도하여 기기 조작을 요청하거나, 범죄 연루 및 카드 도용 등으로 인해 계좌 정지가 필요하니 이를 위해 ATM 기기 조작을 요청한다.

61) 은행직원 뿐만 아니라 카드사, 금융감독원, 경찰, 검찰 등을 사칭하는 경우도 많다.

드번호 등을 입력하라고 하여 금융정보를 빼가는 경우도 있으니 특히 이를 주의하여야 한다.

나. 수사기관 등 관계기관 신고

전화금융사기에 속아서 전화금융사기범들이 지정한 은행계좌에 자금을 이체한 경우에는 즉시 해당 은행에 지급정지를 요청하여야 한다. 전화사기범들은 이체된 자금을 바로 인출해가므로 거래은행 직원 또는 거래은행 콜센터에 신속히 '계좌지급정지'를 요청하여 사기범들이 자금을 인출하지 못하도록 조치를 한다.[62] 그 후에 반드시 수사기관에 피해사실을 신고하므로 해당 금융계좌에 대하여 2차 피해가 발생되지 않도록 수사기관 및 은행 등 금융기관에서 해당 계좌에 대하여 「부정계좌 등록」 조치를 하여야 한다.[63]

다. 개인정보보호 철저

무심코 전화사기범들에게 주민등록번호 등 개인정보를 알려준 경우 즉시 금융감독원 또는 해당 거래은행을 통하여 「개인정보노출자 사고예방시스템」[64]에 등록하여 추가적인 피해를 최소화하여야 한다. 미니홈피, 블로그 등 1인 미디어 내에 전화 번호 등 자신 및 가족의 개인정보를 게시하지 않는다. 미니홈피 및 블로그에 올려진 전화번호 등 개인 및 가족의 연락처 정보가 범죄에 악용되기도 한다.[65]

따라서 미니홈피 및 블로그에는 범죄에 악용될 수 있는 이동전화 번호 등의 개인정보를 게시하지 않거나, 가까운 사람들만이 볼 수 있도록 콘텐츠 접근 권한을 제한

62) 자금을 송금한 전화사기범 사용의 은행계좌는 해당은행 콜센터 및 창구를 통해 할 수 있다.

63) 경찰 등 수사기관에서는 신고 접수 즉시 피해자로부터 수취계좌 명의인과 계좌번호를 확인한 후 수취계좌 개설지점에 피해금이 인출되지 않도록 요청한다. 피해자에게 해당 은행에 계좌지급정지 요청을 하도록 하고 경찰 전산망에 등록한다. 피해 신고 접수 즉시 사기범 조직이 피해금을 통상 20분 이내에 인출하므로 신속히 지급정지 요청 및 부정계좌로 등록을 하여야만 현금 인출 시 검거할 수 있다.

64) 피해자의 개인정보가 노출되어 「개인정보노출자 사고예방시스템」에 등록하면 전 금융회사가 대상자의 정보를 공유하여 신규예금 계좌개설, 대출 신청, 신용카드 발급 등 금융 거래시 철저한 본인확인을 요구하게 된다.(단 우체국, 새마을금고 등은 관할기관이 다르므로 별도로 신청을 해야 한다.)

65) 가족관계 및 피해자 자녀 이동전화 번호를 입수하여 자녀에게 지속적인 욕설 전화를 하여 이동전화전원 차단을 유도하거나, 학교 홈페이지 내 행사 및 시험일정 파악 후, 전화 받지 못하는 상황을 악용 자녀 납치를 빌미로 금전을 요구한다.

한다. 또한 스마트폰 SNS 앱 이용자가 늘면서 트위터 SNS의 아이디를 해킹한 뒤, 이를 이용 트위터 등에 올린 글을 토대로 개인 신변 내용을 알아내어 이를 메신저 피싱에 악용하는 사례가 늘고 있다. 이를 예방하기 위해서는 메신저 비밀번호는 주기적으로 변경하고, 사용하지 않은 메신저 계정이나 버디 리스트는 삭제한다. 단기적으로 가입한 사이트는 사용 후 탈퇴하고, 각 웹사이트의 아이디와 비밀번호는 다르게 설정 및 관리한다.[66]

납치빙자 협박형의 사기범죄를 당하지 않기 위해서는 자녀 등 가족에 대한 비상시 연락을 위해 친구나 교사 등의 연락처를 확보한다. 전화 사기범은 상대방의 전화로 욕설전화 등을 계속 걸어 전화기 전원을 끄도록 유도한 후, 연락이 되지 않은 틈을 타서 가족에게 전화를 걸어 납치한 것처럼 위장하여 송금을 요구한다. 따라서 자녀의 친구나, 교사 등 가족의 휴대폰 전원이 꺼져 있는 경우에 연락가능 한 추가적인 연락처를 확보할 필요가 있다.

종친회, 동창회, 동호회 사이트 등에 주소록 및 비상연락처 파일을 게시하지 않는다. 전화사기범은 종친회, 동창회, 동호회 사이트에 올려진 주소록이나 비상연락처 파일을 범죄에 이용하기도 한다.[67] 따라서 이와 같은 개인정보가 포함된 파일은 홈페이지에 게시하지 않고, 개인 메일로 전송하거나 오프라인에서 배포하여야 한다. 자동응답시스템이나 문자메시지를 이용 계좌번호, 카드번호 등을 입력하게 하여 금융정보를 빼가는 경우가 있으므로 주의한다. 계좌이체, 신용카드 사용내역 등 본인의 계좌에서 돈이 빠져나가는 것을 바로 인지할 수 있도록 이동전화 문자서비스(SMS)를 적극 이용하고, 발신자 번호를 확인한다.[68]

라. 사실관계 확인

공공기관은 어떠한 경우에도 전화 또는 인터넷 홈페이지를 통해 예금계좌 비밀번호 및 보안카드 번호 등을 요구하지 않는다. 공공기관 직원을 사칭하는 사람으로부터 이러한 전화를 받은 경우에는 개인정보 및 금융정보를 등을 알려주거나 인터넷

66) 경향신문, 2011.1.20자.
67) 종친회 및 동창회 명부 입수 후, 동창회비 및 교통사고 보상금 등을 빙자하여 송금을 요구한다.
68) 발신자 전화번호 표시가 001, 002, .. 005 등으로 시작하는 것은 국제전화이므로 공공기관 직원을 사칭하는 경우에는 주의한다. 또한 전화 사기범들이 사용하는 전화는 수사기관의 추적을 피하기 위해 발신자표시가 없거나, 001, 008, 030, 086 등 처음 보는 국제전화번호를 사용하므로 반드시 발신자 전화번호를 확인하여야 한다.

홈페이지에 입력하지 말고, 반드시 해당기관에 직접 사실여부를 확인한다. 또한 대출업체의 홈페이지를 통해 대출을 신청하는 경우에는 사전에 서민금융포털인 「서민금융 119서비스」[69]를 방문하여 해당 업체가 제도권 내에 있는 금융회사 또는 지방자치단체에 등록한 업체인지를 확인한다. 이러한 대출업체에서 대출을 명목으로 예금계좌 비밀번호 및 현금·체크카드를 요구하는 것은 100% 사기이므로 이에 속지 않도록 각별한 주의가 필요하다.[70]

종친회비 납부 등의 '의무부과형'에 대한 피해를 당하지 않기 위해서는 이런 내용의 문자를 수신하면 반드시 종친회 등을 상대로 사실관계를 확인하여야만 피해를 당하지 않는다.

V. 관계당국의 피해예방 대책

1. 금융감독원

금융감독원에서는 전화금융사기 피해자가 해당 송금은행 등에 전화로 지급정지를 요청하면 해당 은행에서는 전산등록을 통해 즉시 지급을 정지하는 제도를 시행하고 있다. 이 제도는 은행간 '금융사고자금 지급정지 시스템'[71]의 협약에 의거 운영되는 「전화금융사기자금 지급정지제도」[72]이다. 또한 전화금융사기에 의한 개인정보노출 시에도 사고예방시스템에 등록하도록 「개인정보노출자 사고예방시스템」을 개선하였다.

1일 이체한도를 5천만원에서 3천만원으로, 1회 이체 및 1일 인출한도를 1천만원

69) '서민금융 119서비스<http://s119.fss.or.kr>'는 금융감독원에서 운영하는 서민금융서비스로 금융회사 선택 서비스부터 신용회복에 이르기까지 다양한 서비스를 제공하고, 금융감독원뿐만 아니라 한국이지론 등 10여개의 금융정보를 제공하는 금융포털 사이트이다.

70) 앞의 금융감독원 보도자료.

71) 금융사고 발생시 사고발생 은행에서 금융결재원을 통하여 각 은행에 사고자금이 이체된 경로를 실시간으로 추적 확인하여 일괄 지급 정지하는 시스템이다.

72) 전화금융사기 피해예방대책의 하나로 피해자가 사기범에게 속아 돈을 송금한 경우 인지 즉시 긴급하게 입금된 상대은행에 피해자금의 지급정지를 요청할 수 있도록 하는 제도이다. 전화금융사기로 자금을 이체한 경우 피해자 또는 송금은행이 자금이 입금된 상대은행에 전화로 피해자금의 지급정지를 요청할 경우 상대은행은 우선 지급정지 조치를 이행한 후 24시간 이내에 서면으로 지급정지 요청서를 징구하여 보완하도록 하고 있다. 이 제도는 사기범들이 짧은 시간 내에 이체된 자금을 출금해가고, 수사기관에서도 추적이 어려운 상황을 감안하여 도입된 것이다.

에서 6백만원으로 하향 조정하는 등 CD/ATM기 거래한도를 축소하고[73] '주의문구'를 삽입하였다.[74] 외국인을 통해 계좌를 개설하고 이를 전화사기에 이용함에 따라 단기체류 외국인 등에 대한 계좌개설 요건을 강화하였다.[75]

또한 전화금유사기에 이용되어 지급정지 된 계좌의 예금주 명의로 다른 은행에 개설된 계좌[76]에 대해서도 비대면 인출거래를 제한하는 「전화금융사기자금 지급정지제도」를 보완하였다. 전화금융사기의 경각심 제고를 위하여 일부 은행에서 실시하고 있는 CD/ATM기의 음성경고음을 모든 은행 및 위탁운영사까지 확대하고,[77] 소액 입출금이 빈번한 계좌 등 전화금융사기에 많이 이용되고 있는 유형의 계좌에 대한 은행 자체 모니터링을 강화하고 있다.

금융감독원에서는 전화금융사기를 근절하기 위해 2010년 12월 23일부터 17개 국내은행, 신용협동조합, 우체국, 새마을금고 등 금융회사와 공동으로 사기에 이용될 모든 금융계좌에 대한 집중단속을 실시하고 있다.[78] 사기범이 주로 신규 계좌를 사기에 이용하였으나 '단기간 다수계좌 개설목적 확인 제도'[79]로 금융사기에 이용할 신규 계좌의 확보가 여의치 않게 되었다. 그래서 최근에는 대출을 빙자하여 기존 거래계좌[80]를 수취하여 사기에 사용하는 등 신종 사기수법을 이용하고 있는 것으로 파악된다. 이에 따라 금융감독원은 단속 대상을 신규 계좌뿐만 아니라 기존 거래계좌[81]까지 확대하고, 금융회사와의 정보공유를 활성화하는 한편 관련 전산시스템

73) 전화금융사기에 취약한 노인 및 주부 등은 CD/ATM기를 이용한 계좌이체 실적이 거의 없는 점을 감안하여 최근 이체실적이 없는 계좌의 1회 이체한도를 600만원에서 70만원으로 계좌이체 한도를 대폭 축소하였다. 다만 고객의 불편해소를 위하여 본인이 창구에서 이체한도 증액을 요청하는 경우에는 종전 한도까지 이체를 허용하고 있다. 참고로 전화금융사기 피해자 120명을 상대로 조사한 결과 53명(44.2%)이 최근 1년간 CD/AMT기 이체 실적이 없었다.

74) '"전화사기 주의" 고객님의 계좌에서 000원이 인출됩니다, 계속 하시겠습니까?'라는 메시지가 뜬다.

75) 외국인 등록증, 재직증명서 등 신원을 확인할 수 있는 증명서를 제시하는 경우에 한하여 계좌개설을 허용하며, 여권만 제시하는 경우에는 원칙적으로 계좌개설을 불허하고 있다.

76) 경찰청 조사 결과 사기범은 동일인에게서 개설은행이 다른 8개의 대포통장을 매입한 것으로 나타나 전화금융사기에 이용된 대포통장은 대부분 은행에서 개설되었다.

77) "공공기관에서는 전화를 통해 환급하지 않습니다. 전화사기에 주의하시기 바랍니다"라는 경고음이다.

78) 금융감독원 보도자료(2010.12.22).

79) 이는 2010년 3월 29일부터 시행되는 제도로 전 금융회사는 최근 1개월간 2개 이상 예금계좌(보통·저축예금)를 개설하는 고객에 대해 개설 목적을 확인하고 그 목적이 불분명한 경우 계좌개설을 거부할 수 있다.

80) 개설된 지 1개월이 지나 정상적으로 사용 중인 계좌를 말한다.

81) 현금지급기(CD/ATM) 또는 폰뱅킹을 통해 자금이 입금된 계좌(신규 및 기존거래계좌)에서 일정시간 이내 인출거래가 발생하는 계좌 등을 중점 점검한다.

을 확충하였다.

2. 경찰청

가. 범죄단속·제도개선·예방홍보 대책 추진

경찰은 조직·인력·장비 등 경찰수사역량을 총동원하여 2006년 최초발생 후 현재까지 전화사기범 총 18,659건에 27,149명을 검거하고 2,075명을 구속하였다. 범죄유형별로는 대포통장 제공자 23,834명 외에 송금책 362명, 인출책 2,072명, 모집책 881명을 검거하여 범죄분위기 차단에 주력하였다. 특히 2010년 7월에는 서울지방경찰청 등 8개 지방경찰청에 설치된 「금융범죄수사팀」을 활용하여 2회에 걸친 특별단속을 추진하는 등 범죄분위기 제압에 소기의 성과가 나타난 것으로 보인다.[82]

<그림 8> 2010년 특별단속 추진성과

❖ 2010. 7. 서울지방경찰청 등 지방 8개 경찰청에 「금융범죄수사팀(62명)」 설치
❖ 2010. 3. 1 ~ 5. 31 전화금융사기 단속강화 실시 692건에 1,090명 검거
❖ 2010. 8. 1 ~ 10. 31 전화사기 등 금융범죄 특별단속으로 1,179건에 1,785명 검거

또한 전화금융사기는 금융수단인 현금자동지급기(ATM)와 통신수단인 해외 인터넷전화(VoIP)[83]를 범죄수단으로 이용하는 점에 착안하여, 「휴대폰 국제전화표시서비스」, 「예금계좌 개설정보 조회시스템」 등 전화금융사기 근절을 위한 제도개선의 노력을 기울여 왔다.

경찰의 주요 제도개선 현황을 살펴보면 2010년 3월 29일 대포통장 개설 방지을 위한 「예금계좌 개설정보 조회 시스템」[84]을 구축하였다. 2010년 5월 6일부터는 '대한법률구조공단'[85]의 협조[86] 아래 전화금융사기 피해자를 위한 무료 소송 지원

82) 앞의 경찰청 보도자료.
83) VoIP는 인터넷망을 통해 음성신호를 실어나르는 기술이다. 기존 회선교환 방식의 일반전화와는 달리 인터넷의 근간인 IP네트워크를 통해 음성을 패킷형태로 전송한다.
84) 시스템 개요는 단기간에 여러 계좌개설 희망자의 개설목적을 확인하여, 목적이 의심스러울 경우 계좌개설을 거부할 수 있다.
85) 대한법률구조공단은 1987년 9월 1일 설립되었으며, 서울에 본부가 있고 18개 지부, 39개 출장소, 15개 지소로 조직되어 있다. 변호사 50명, 공익법무관 131명, 전문상담원 350명 등 총 7백

절차인 전화금융사기 One-Stop 구조절차[87]를 시행하고 있다.

현재 피해회복을 위해서는 통장명의자 등 접근매체 당사자에게 부당이득반환청구소송을 제기하여 이체된 피해금을 회수하여야 한다. 그러나 전화금융사기' 민사소송을 제기하면 약 3개월에서 8개월이 소요된다. 그리고 경찰에서는 압수수색 영장을 집행하여 상대방 계좌 압수 후 가환부가 가능하나, 일부 지검 및 법원에서는 채권(예금반환청구권)은 압수대상이 아니라며 영장을 기각하는 사례도 발생하고 있다. 이 제도는 피해자의 빠른 피해회복을 위한 것으로 법원에서는 수사 중인 경찰서에 사실조회를 하면 경찰서에서는 수령 즉시 조회결과를 통보하는 등 소송기간을 단축시키고 있다.[88]

전화금융사기 피해회복을 위해 피해금액을 압수하여 가환부를 실시하고 있으며,[89] 통신사와 협조하여 국제전화를 최초 접수한 통신업체를 파악할 수 있는 식별번호 등을 부여하여 피해를 예방하고 있다.[90] 또한 이동전화로 국제전화 수신시 "국제전화입니다"라는 문자를 표시하여 수신자가 전화 내용을 의심할 수 있도록 하였다.[91]

2009년 7월부터는 피해자가 ATM기 계좌이체 단계에서 전화금융사기 경고화면 표시 및 경고음성 방송으로 피해자의 경각심을 유도하였다. 2009년 8월부터는 금융감독원과 협조하여 1년간 이체실적이 없는 금융계좌의 ATM기 계좌이체 및 현금인출한도를 하향 조정하였다.[92] 또한 2009. 10월부터는 경찰서에서 전화금융사기로 인한 피해신고 접수

여 명이 저소득층, 범죄피해자 등에 대한 소송대리, 무료변호, 합의중재 등을 위해 일하고 있다.

86) 2009년 11월 13일 전화금융사기를 당한 서민층의 범죄피해구조를 위해 '경찰청-대한법률구조공단' 간 업무협약을 체결하고, 이를 기초로 서민피해자 구제를 위한 다양한 협조방안을 모색하고 있다.

87) 전화금융사기 One-Stop 구조절차는 경찰에서 전화금융사기 신고 접수 시 수사착수와 동시 피해구조 절차를 피해자에게 설명해준다. 그리고 무료로 소송을 도와주는 대한법률구조공단 담당자에게 협조차원에서 피해내용을 설명해 준다. 그 후 상담일을 정하여 피해자가 신속히 구조 받을 수 있도록 피해사실 확인원 및 범죄에 이용된 계좌번호, 거래내역 등 자료를 피해자에게 건네준다. 그러면 법률구조공단 소송담당 변호사가 송금 받은 자의 인적사항, 거주지 등을 명백히 하기 위해 법원에 사실조회를 신청하면 수사 중인 경찰서에서 사실조회 내용을 통지하는 등의 조치를 신속히 진행하는 절차이다.

88) 민사소송법 제294조(조사의 촉탁) 법원은 공공기관·학교 그 밖의 단체·개인 또는 외국의 공공기관에게 그 업무에 속하는 사항에 관하여 필요한 조사 또는 보관중인 문서의 등본·사본의 송부를 촉탁할 수 있다.

89) 2009. 5.22(최초 실시일)~2010.12월까지 47건에 2억6천만원을 가환부하였다.

90) 이 제도는 2009년 5월 1일부터 현재까지 시행하고 있으며, 기간통신 5개사, 별정통신 7개사가 참여하고 있다.

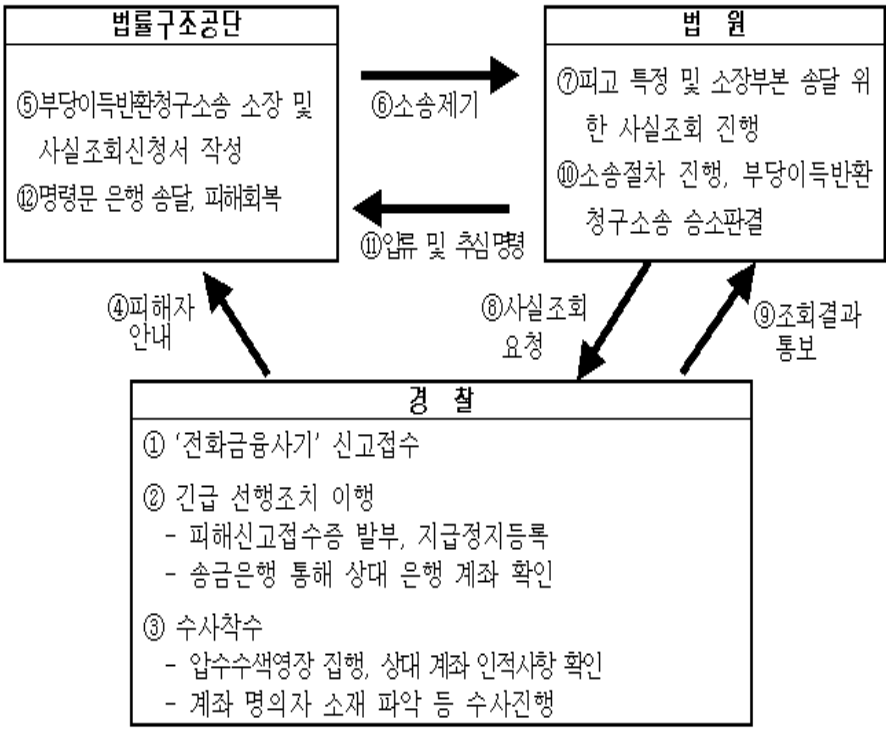
91) 이 제도는 2009.09.01부터 시행을 하고 있으며, SKT, KTF, LGT 등 이동통신 3개사가 참여하고 있다.

92) 1년간 이체실적이 없는 경우 1일 이체금액을 3000만원에서 70만원으로, 1회 이체한도를 600만

시 소송절차 및 소장 작성요령 등 안내장을 교부하여 피해에 적극 대처하고 있다.

아울러 범죄피해 예방을 위해서는 홍보가 무엇보다도 중요하다고 보고 경각심 고취를 위해 TV·신문 등 방송매체를 통해 범죄유형 및 피해예방 방법을 적극 홍보하였다. 특히 한국방송광고공사와 협조하여 공익광고를 통해 가시성 높은 홍보활동을 전개하였다.[93] 기타 방송매체로 부족한 경우를 위해 반상회, 부녀회, 노인정, 주민자치단체 등 현장 진출 및 현수막 등을 통해 전화사기 수법 및 피해예방책을 집중 홍보하였다.

〈그림 9〉 전화금융사기 피해자 One-Stop 구조절차



전화금융사기의 배후에 중국 및 대만의 폭력조직이 있는 점을 감안하여 근본적으로 범죄를 뿌리 뽑기 위하여 2007년 2월 2일 환급사기와 관련하여 중국공안, 대만

원에서 70만원으로 각 하향조정하였다.

93) 2009.7. 28부터 같은해 9.03까지 한국방송광고공사와 협조하여 대국민 홍보를 적극 실시하였다.

대표부와의 업무협의를 하였다. 이후 2010년 10월 25일까지 도합 10회에 걸쳐 중국 및 대만, 일본과 국제공조협력을 강화하여[94] 사기조직을 검거한 바 있다.[95]

나. 지속적인 수사 활동의 전개

경찰은 전화금융사기 근절을 친서민정책의 최우선 과제로 지정하고, 2010년 10월 18일부터 추진 중인 「서민생활 위해사범 단속」과 연계하여 2011년 연중 내내 강도 높은 단속을 지속할 계획이다. 또한 전화금융사기 피해의 심각성에도 불구하고, 복잡한 소송절차로 인해 피해구제가 어려운 상황임을 감안하여 신속한 피해구제를 위한 「전기통신금융사기 피해금 환급에 관한 특별법(안)」의 조기 통과를 추진하고 있다.

서울지방경찰청 등 8개 지방경찰청 내 「금융범죄수사팀」을 운영한 결과 전화금융사기에 대한 적극적인 인지수사로 소기의 목적한 성과를 달성할 수 있었다. 그래서 행정안전부·기획재정부와 협의하여 「금융범죄수사팀」의 전 지방경찰청 확대설치를 위해 소요정원 95명 확보를 추진하여 전화금융사기 상시단속체제를 구축하여 범죄의지를 완전히 제압할 예정이다. 더불어 단속 효율성을 배가하고, 원천적 피해방지를 위해 유관기관과 협의하여 제도개선 및 홍보활동을 병행하는 등 "할 수 있는 모든 수단을 동원하여, 더 이상 애꿎은 국민들에게 피해가 돌아가는 일이 없도록 최선을 다한다"는 각오로 수사 활동을 전개하고 있다.[96]

3. 국회 등 입법 활동

대부분의 전화금융사기 피해자들이 노인, 주부 등 경제 및 법률지식이 취약한 서민들이 주를 이루는 것으로 판단된다. 따라서 이들의 권익을 적극 보호하고, 현재 지급

94) 2007.05.21, 대만대표부 영사과장 등 초청 수사공조회의 실시, 2007.06.18, 한·대만간 전화금융사기 수사공조회의 개최, 2007.10.22, 한·중 인터폴 실무회의 실시, 2008.06.24부터 같은해 10. 28,까지 전화금융사기 국제공조수사 의뢰(5건에 대하여 중국 내 콜센터 등 정보제공 및 수사촉구로 2건에 33명 검거), 2009.06.25, 전화금융사기 근절을 위한 한·중 인터폴회의 실시, 2009.09.11, 중국 공안부 대표단 방문 전화금융사기 협력방안 논의, 2010.01.26, 한·중 경찰 실무회의 참석(한국), 2010.10.05, 아시아 국제범죄 대책회의(중국), 2010.10.25, 한·일 경찰 협력회의(일본)를 개최하는 등 지속적인 협조체제를 구축하고 있다.

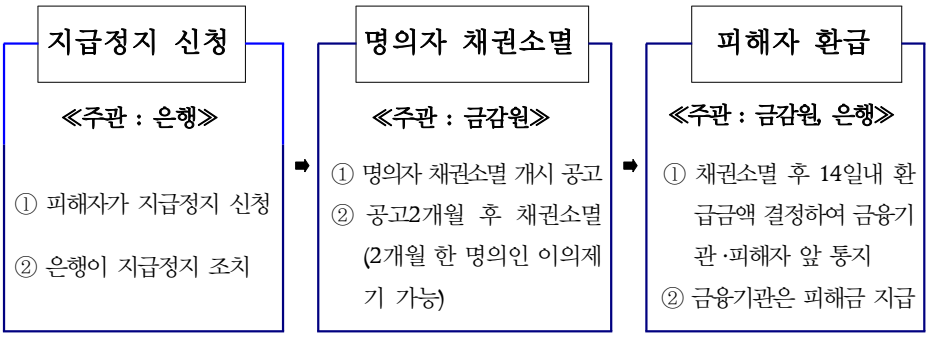
95) 경찰주재관·인터폴 등을 통해 강력한 단속을 요청한 결과 2006년 부터 2010년까지 해외 현지 범죄조직 361명을 검거하였다.

96) 앞의 경찰청 보도자료.

정지된 피해금액이 피해자들에게 하루빨리 환급될 수 있도록 피해회복 간소화를 위한 특별법안이 국회에 제출되었다.[97]

위 법률안은 그 동안 국회 정무위원회 법률안심사소위원회에서 10차례에 걸친 회의 등 15회에 걸쳐 논의가 되었다. 2010년 9월 29일 제294회 국회(정기회) 정무위원회 제5차 전체회의 의결을 거쳐 현재 국회 법제사법위원회에 「전기통신금융사기 피해금 환급에 관한 특별법안」이란 법률명으로 계류 중이다. 이 특별법은 금년 국회회기 중에 통과될 것으로 기대된다. 위 법률안은 18개 조로 구성되어 있다. 허위로 피해구조를 신청하거나, 허위로 지급정지를 요청한자, 허위로 이의제기를 한자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하게 되며,[98] 양벌규정의 적용을 받는다.

<그림 10> 피해금 환급 특별법 진행절차



2009년 4월 1일부터 시행되는 전자금융거래법의 개정으로 전화금융사기에 이용되는 예금계좌 번호 등 접근매체를 양도하거나 양수하는 행위 등에 대한 벌칙을 1년 이하의 징역에서 3년 이하의 징역 또는 2천만원 이하의 벌금에 처하는 것으로 형량을 크게 높였다.[99]

97) 이 법률은 2008년 12월 15일 박선숙의원이 대표 발의한 「보이스피싱 피해보전금 지급에 관한 특별법안」은 283회 국회(정기회) 제5차 정무위원회(2009.07.15)에, 2009년 10월 9일 김용태의원이 대표 발의한 「전화금융사기 등 피해금 환급에 관한 특별법안」은 284회 국회(정기회) 제9차 정무위원회(2009.11.19)에 각각 상정되었다.

98) 위 특별법 제16조(벌칙).

99) 전자금융거래법 제49조제4항.

VI. 결론 - 제도적 대응방안

현대사회는 정보통신사회로 모든 국민이 정보화 환경에서 생활하고 있다. 특히 이동전화 가입자는 2010년 9월 말 현재 5천만 가입자(103.9%)를 넘어선 정보화 선진국이다. 위와 같은 보급률은 그리스(195.0%), 영국(135.3%), 프랑스(107.1%)에 이어 세계 제4위[100]이다.

위와 같은 정보화환경에서 정부를 비롯한 행정기관과 금융권, 언론매체 등 모든 유관기관과 상호 협조하여 전화금융사기 예방을 위한 각종 대책을 시행하였으나 근절되지 않고 있다. 특히 금융권에서는 '단기간 다수계좌 개설목적 확인제도'[101]와 같은 예방대책을 수립 시행하자, 최근에는 대출을 미끼로 한 기존 거래계좌를 이용하는 등 일명 '두더지 효과'가 발생하고 있다. 때문에 은행예금 계좌 등 접근매체를 양도 및 양수하는 행위에 대한 처벌을 강화하고, 금융기관에서는 전화금융사기 미수에 그친 금융계좌 등에 대한 부정계좌 등록을 적극 입력할 필요가 있다. 또한 전화금융사기는 정보통신매체인 전화를 범행수단으로 하고 있어 통신서비스사와 협조하여 국제전화 수신 시 "전화금융사기일 수 있으니, 다시 한 번 확인바랍니다"라는 내용의 경고 메시지를 도입할 필요가 있다.

법적으로 전화금융사기로 인한 피해자 보호를 위한 특별법으로 현재 국회에 계류중인 「전기통신금융사기 피해금 환급에 관한 특별법(안)」이 신속히 통과되어야 한다. 이 법률을 통하여 전화금융사기를 규율하게 되면 구제 절차의 개선뿐만 아니라 법적근거의 강화와 실현 위험의 제거를 동시에 해결할 수 있다. 이와 같은 전화금융사기 관련 특별법의 제정이 가장 시급하고 합리적인 구제방안이라 할 것이다. [102] 아직은 이 법이 시행되지 않고 있으므로 전화금융사기 피해자 One-Stop 구조절차를 적극 홍보할 필요가 있다. 이를 통해 전화금융사기로 인하여 인출되지 않은 피해금을 신속히 회수할 수 있을 것이다.

동창회·종친회·대학교 등을 사칭하는 '의무부과형'이나 '협박형'의 전화금융사기는 범죄조직이 개인정보를 불법으로 수집하여 이를 이용할 경우 더 큰 피해가 발

100) 방송통신위원회 보도자료, 2010.9.15. <http://www.kcc.go.kr>

101) '단기간 다수계좌 개설목적 확인제도'는 전 금융회사가 2010. 3. 29. 기준 최근 1개월간 2개 이상의 예금계좌(보통, 저축예금)를 개설하는 고객에 대해 개설 목적을 확인하고, 그 목적이 불분명한 경우 계좌개설을 거부하는 제도이다.

102) 김수희·한영천, 앞의 논문, 299면.

생할 수 있다. 따라서 온라인상에 본인이 공개하고 있는 개인정보가 전화금융사기 등의 범죄에 악용될 수 있음을 인터넷 이용자들에게 환기시킬 필요가 있다. 우리나라 개인정보보호법제 정비를 통해 개인정보 불법수집 및 유통에 대한규제를 강화하여야 한다.[103] 민간부문의 개인정보보호를 규율하고 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 경우, 규율대상이 온라인상에서 개인정보를 수집·이용하는 사업자 및 호텔·학원 등 특정 오프라인 사업자에 한정되기 때문에 정유사·대형서점 등 일부 민간부분이 규율대상에서 제외되고 있다.[104]

이러한 상황에서 현재 국회에서 심의 중인 정부안과 의원안을 통합한 「개인정보보호법(안)」[105]이 조속히 통과되어야 한다. 그리함으로써 국내 관련산업의 발전을 촉진하고 국제적으로 개인정보보호의 모범이 될 수 있을 것이다.[106] 이 법은 공공부문과 민간부문에 포괄적으로 적용되는 법이므로 시행이 되면 개인정보보호의 사각지대를 해소할 것으로 예상된다.

전화금융사기에 이용되고 있는 국제전화는 대부분 중국, 대만 등 해외에서 우회경로를 이용한 인터넷전화이다. 발신번호 표시가 불분명하거나, 기술적으로 발신번호 조작이 가능할 경우에는 문제해결에 한계가 있다. 세계적으로 최대 규모의 인터넷전화 사업자인 스카이프의 서비스를 이용하여 해외에서 국내에 있는 휴대전화로 전화를 했을 때에는 발신번호 창에 '발신번호 표시금지'로 표시되기 때문에 국제전화 여부를 수신자가 알 수 없다. 또한 검찰 또는 경찰로 위장한 후 발신번호 창에 '발신 02-753-0112 경찰 사이버대응팀'으로 표시되도록 발신번호를 조작하는 사례도 이미 보고된 바 있다.[107] 발신번호 조작의 경우 「전기통신사업법」 제100조 및 제84조제3항[108]에서 금지하고 있으나 해외에 소재한 콜센터를 대상으로 동 법조항

103) 국회입법조사처, 앞의 방안 23면.

104) 이인호, "공공부문 개인정보보호법제에 대한 분석과 비판", 「정보법학」 제6권 제1호, 2002; 김일환, "개인정보보호법제의 체계적 정비방안에 관한 고찰", 「인터넷법률」 통권 제27호, 2005.

105) 이 법은 2010년 9월 29일 국회 행정안전위 법안심사소위를 통과하여 현재 국회 법제사법위원회에 계류중으로 2011년 2월 임시국회에서 논의될 예정이다. 이 법이 금년 2월 국회를 통과하여 공포되면 6개월 간의 준비기간을 거쳐 이르면 금년 8월부터 본격 시행된다.

106) 박훤일. "'개인정보보호법안' 늦춰선 안된다", 디지털타임스. 2010.8.31. <http://www.dt.co.kr/contents.htm?article_no=2010090102012351746002> [2011.1.27. 방문]

107) 홍석근, "'발신번호 위조' 중국 보이스 피싱 조직 적발", YTN, 2009.09.24.

108) 영리를 목적으로 송신인의 전화번호를 변작하거나 거짓으로 표시하는 서비스를 제공한자는 5천만원 이하의 벌금에 처한다. 다만, 공익을 목적으로 하거나 수신인에게 편의를 제공하는 등 정당한 사유가 있는 경우에는 그러하지 아니한다.

을 적용하여 처벌하는 데는 한계가 있다. 때문에 발신번호 조작행위를 제어하기 위한 기술적 대응책을 마련할 필요가 있다.[109]

전화금융사기범죄에 이용된 대포통장을 압수한 이후에 거래내역 등을 파악하기 위해서는 피해금액이 이체된 대포통장 발급은행에 대한 수사가 긴급히 이루어져야 한다. 하지만 「금융실명거래 및 비밀보장에 관한 법률」 제4조제1항제1호에 따르면 금융거래정보는 법원이 발부한 제출명령이나 법관이 발부한 영장에 의해야만 가능하기 때문에 수사에 한계가 있다는 지적이 있다.[110] 이는 전화금융사기의 확산을 방지하고 신속한 대처가 가능해진다는 점에서 긍정적이나, 영장주의의 예외 사안인 만큼 보다 신중하게 접근할 필요가 있다.[111]

금융시스템과 통신시스템의 문제가 복잡하게 얽혀있는 전화금융사기 범죄에 신속히 대응하기 위해서는 경찰과 검찰, 금융감독원, 방송통신심의위원회 등 관련 기관들의 협조가 필수적이다. 또한 원활한 협조를 위하여 대만과 같이 신고를 접수하는 전담신고센터를 설치하고, 접수된 내용에 대하여 즉각적으로 조치를 취할 수 있는 전담부서가 필요하다.

일본은 동경 경시청 내에 100여명 규모의 「전화금융사기 긴급대책본부」를 운영한 결과 2010년 전화금융사기 피해가 2008년에 비해 70%가 감소한 것으로 나타났다. 현재와 같이 경찰에서 전담하고 있는 전화금융사기 수사를 「금융범죄수사팀」에서 확대 운영하기 위해서는 행정안전부와 기획재정부가 경찰력 증원을 적극적으로 고려할 필요가 있다.

전화금융사기는 해외에 근거를 둔 조직의 수사가 어려워 주로 대포통장 검거 위주로 수사가 이루어지고 있으나, 인출조직이나 대포통장 명의자의 처벌만으로는 범죄를 줄이는 데는 한계가 있다. 따라서 국제공조수사를 통하여 검거율을 높일 수 있으나, 국제공조수사가 현실적으로 한계가 있으므로 이에 대한 지속적인 대책 마련이 필요하다고 생각된다.[112] 경찰청은 중국 및 대만 경찰과의 수사공조를 통하여 중국과 대만 당국이 전화금융사기 범죄조직을 검거하도록 촉구하고 있다. 그러나

109) 국회입법조사처, 앞의 방안, 22면.
110) 황정익, "전화금융사기사건에 있어서 명의도용 예금통장에 관한 법적 고찰", 「한국공안행정학회보」, 제17권 제4호 통권 제33호, 한국공안행정학회, 2008, 441~476면. 허성욱·정세종, "국제전화금융사기에 관한 법적 고찰', 「한국경찰연구」 제7권 제2호, 한국경찰연구학회, 121~144면.
111) 국회입법조사처, 앞의 방안, 30면.
112) 김성언·양영진, 앞의 논문, 101~149면.

점조직으로 운영되는 전화금융사기 범죄조직의 특성상 한국에서 검거된 자들이 중국이나 대만 현지의 범죄조직에 대한 정보를 거의 갖고 있지 않아 협조를 구하는데 한계가 있다.[113]

아울러 현재는 전화금융사기 피해 관련 정보를 공유할 수 있는 사이트가 없다. 그러므로 인터넷 사기피해 공유 사이트인 더치트(thecheat.co.kr)와 같이 전화금융사기 정보를 공유할 수 있는 사이트를 개설하여 피해를 예방하는 활동이 요청된다. 무엇보다도 피해 당사자가 현재와 같은 정보화 환경에서 전화 등 정보통신기기를 이용한 금융사기를 당하지 않도록 사기전화 내용에 대한 해당 사실을 확인하는 등 적극적인 대처가 필요하다. 그리고 날로 진화하고 있는 전화금융사기 수법 등에 대한 언론 등의 자발적인 홍보로 예방효과를 극대화하는 노력도 병행되어야 할 것이다.

113) 국회입법조사처, 앞의 방안, 31면.

참고문헌

권성언·양영진, “전화금융사기 범죄의 진화: 보이스피싱(Voice Phising)의 피해구조 분석과 대응”. 한국공안행정학회보 제32호(2008).

권성언, “전화금융사기 범죄의 대한 한국 사회의 대응 : 대만과의 비교 분석”, 형사정책 제22권 제1호(2010. 7).

김수희·한영찬, “전화금융사기(Voice Phishing) 지급인 보호를 위한 금융법적 개선안 검토”, 은행법연구 제3권 2호(2010.11).

김은경·최수형·박정선, “2008년 한국의 범죄피해에 관한 조사연구(Ⅵ)”, 한국형사정책연구원, 2009.

김일환, “개인정보보호법제의 체계적 정비방안에 관한 고찰”, 인터넷법률 통권 제27호, 2005.

양영진, “보이스피싱 범죄의 근절 방안에 관한 연구”, 경남대 석사논문, 2008.

이봉한, “전화금융사기범죄의 유형과 전망”, 수사연구, 2008.08.

_____, “전화금융사기의 유형과 피해자 분석-한국과 일본의 비교”, 한국범죄심리연구 제4권(2008.10.17).

이인호, “공공부문 개인정보보호법제에 대한 분석과 비판”, 정보법학 제6권 제1호(2002).

정 완, 「인터넷법 연구」, 한국형사정책연구원, 2009.

_____, “인터넷사기의 신종유형과 법제도적 방안”, 경희법학 제40권 제1호(2005.06).

_____, “인터넷사기의 최근 동향”, 형사정책연구소식 95호(2006.06).

경찰청·금융감독원, 「주요 불법금융거래 유형 및 해설」, 2009.9.

국회입법조사처, “전화금융사기(보이스피싱) 대응책의 현황 및 개선방안”, 현안보고서 제34호(2009.08.21).

Reppetto, T. A., "Crime prevention and displacement phenomenon," Crime and Delinquency 22, 1976.

경찰청 <http://www.police.go.kr>

금융감독원 <http://www.fss.or.kr>
방송통신위원회 <http://www.kcc.go.kr>
한국인터넷진흥원 <http://www.kisa.or.kr>
경향신문 <http://news.khan.co.kr>, 한국일보 <http://news.hankooki.com>, YTN <http://www.ytn.cokr>, 디지털타임스 <http://www.dt.co.kr>, 네이버 <http://www.naver.com>, 위키피디아 <http://www.wikipedia.org> 등 인터넷자료

Study on the Policy Measures to Prevent Various Types of Phone Phishing

Jeong, Soon-Chae *

Recently an increasing number of the Internet phishing has been reported in Korea. Careless people usually fall victims to such unprecedented communication crimes. The criminals, stationed in foreign countries like China and Taiwan, call any customer at random by disguising themselves as employees of a bank, post office or even prosecutor's office, and demand financial information including bank account numbers or credit card numbers. Some of them urge the victim to remit a certain amount of money to a designated account for the payment of ransom or medical charges of victim's children allegedly in trouble.

It is a kind of international scam activities by using telephones and CD/ATMs. As soon as such voice phishing is recognized, the victim may demand provisional refund only if the cheated money is not withdrawn by the criminals, which requires the confiscation warrant. Otherwise, the victime has to file a suit to claw back the cheated money as unjust enrichment. But such judiciary recovery is hard to get, because complicated proceedings and relatively small amount of money prevent ordinary people from being involved in litigation. With the help from financial institutions and the mass media, the government has staged a combat against telephone financial fraud, but the vice has not been rooted out.

This paper examines various types and techniques of voice phishing, and studies how to prevent such telephone financial fraud with a suggestion of

* Cyber-crime Investigation Team Leader, Seoul Metropolitan Police Agency Dongdaemun Police Station, Graduate student at the Graduate School of International Legal Affairs, Kyung Hee University.

systemic policy measures as follows:

First of all, the government should strengthen punishment against transfer and acquisition of such access media as used for crimes. Also, technical measures are necessary to control manipulation of the transmitting bank account numbers. A warning message upon the receipt of suspicious international call should be applied to mobile phones.

In this regard, the "Special Act for the Refund of Damage from Fraudulent Financial Wire Transactions" and the comprehensive "Data Protection Act", both pending in the National Assembly, should be legislated as soon as possible. Even before the implementation of these laws, the authorities concerned should actively make the "One-Stop Remedy Program" to the victims of telephone financial fraud, by which such victims may recover the cheated money not yet withdrawn by the criminals with the legal assistance from the Korea Legal Aid Corporation.

For the prevention of trust-based crimes via telephone, concerted efforts by such relevant authorities as the police, public prosecutors, the financial regulators are in great need for the time being. In view of the international criminal activities involved in the telephone financial scam, cross-border collaborative investigation should be carried out, but only a few successful results have been reported.

Above all, it is the best policy for everyone to be cautious of the suspicious phone calls which happen to be voice phishing. And it is also advisable for television and newpapers to alert ordinary citizens to such ever-evolutionary phishing skills.

주제어 : 전화금융사기, 피싱, 범죄조직 네트워크, 사기, 범죄의 전이, 개인정보보호, 환급금
voice phishing, phishing, organized crime network, fraud, displacement of crime, data protection, refund