연구총서 23-AB-05

www.kicj.re.kr

보이스피싱 범행단계별 대응방안 연구

A Study on the Response Plan for each Stage of Voice Phishing Crime

윤해성 · 전영실 · 이정민 · 김계환

KICJ 한국형사·법무정책연구원
Korean Institute of Criminology and Justice

보이스피싱 범행단계별 대응방안 연구

연구책임자

윤 해 성 한국형사·법무정책연구원 선임연구위원, 법학박사

공동연구자

전 영 실 한국형사·법무정책연구원 선임연구위원, 사회학박사
이 정 민 단국대학교 교수, 법학박사
김 계 환 법무법인 감우 대표변호사

연 구 지 원

최 혜 선 한국형사·법무정책연구원 조사연구원, 법학박사

발간사

보이스피싱 범죄는 대표적인 서민 경제 침해 범죄로 인식되어져 왔었습니다. 그러나 최근에는 통신과 금융기술의 발달에 힘입어 그 수법이 점점 더 교묘해지고 있는 것을 알 수 있습니다. 2006년 최초 발생한 보이스피싱 범죄는 이제는 전 국민을 대상으로 범죄를 야기하는 것은 물론 피해액도 증가추세에 있습니다. 더구나 신기술과 비대면 인증 서비스로 인하여 보이스피싱 범죄는 더욱더 진화되고 있는 것도 분명합니다. 이에 본 연구에서는 첨단화, 지능화, 고도화에 따른 보이스피싱 범죄의 단계별 보완 대책을 수립하는 것은 물론 예방과 피해구제책도 도모하고자 합니다. 그리고 현재까지 정부에서는 보이스피싱 정부합동 TF를 비롯하여 보이스피싱 관련 대책을 시행하고 있었습니다. 이 가운데 효과적인 대책도 있는 반면 큰 영향력를 발휘하지 못하는 대응책도 있는 것을 알 수 있었습니다. 이에 보이스피싱 관련 정부부처, 금융감독원 및 금융위원회, 경찰청 및 검찰청, 방송통신위원회, 과학기술정보통신부 등 각계의 실무가의 인터뷰를 통해서 현행 보이스피싱 범죄의 문제점을 진단하고 대응방안을 모색해 보았습니다.

특히, 금융감독원과 경찰청의 도움으로 최신 보이스피싱 범죄 관련 통계와 사례 등 자료를 지원받아 실증적 연구를 수행하는데 많은 도움을 주셨습니다. 그 외에도 실무상 보이스피싱 범죄 관련 검사와 변호사의 자문으로 본 연구를 수행하는데 있어 많은 도움을 받았습니다. 이렇듯 많은 전문가와 실무가의 도움 아래 보이스피싱 범죄의 단계별 수법을 가능한 파악하여 범행수법과 피해자 특성 등 범행유형별 수단을 분석하고자 노력하였습니다. 나아가 정부의 대책을 진단하고 피해구제에 대한 시사점을 제시하는데 주력하였습니다. 본 연구의 결과를 토대로 선제적 예방 대책을 수립하고 증거 확보 및 범인 추적의 연구결과에 활용되기를 바라면서 보이스피싱 범죄가 더 이상 뿌리 내리지 않고 국민이 안심하고 이용할 수 있는 4차 산업혁명 기술 발전과 보급에도 이바지하길 기대해 보면서, 내부 공동연구진 전영실 선임 연구위원, 최혜선 조사연구원과 연구를 열심히 도와주다가 유학을 선택한 송승연 조사연구원 그리고

외부 공동연구진 이정민 단국대학교 교수와, 법무법인 감우 김계환 대표 변호사께도 감사의 인사를 전합니다. 아울러 본 연구를 수행하는데 아낌없이 도움을 주신 많은 분들께도 미약하나마 감사의 인사를 전하고자 합니다.

2023년 9월
연구진을 대표하여
선임연구위원 **윤 해 성**

목 차

표 차례

그림 차례

국문요약

보이스피싱 범죄는 2006년 최초 발생하여 서민경제를 침해하는 대표적인 범죄로 인식되고 있다. 보이스피싱 피해액의 경우 국무조정실 자료에 의하면 2017년 2,470억에서 2018년 4,040억, 2019년 6,398억, 2020년 7,000억, 2021년 7,744억으로 점차 늘어나고 있어 상당히 심각한 사회 문제로 대두되고 있다. 초기 서민이나 노인들을 상대로 정부기관을 사칭하였던 서민범죄에서 이제는 대면편취형과 대담한 수법을 사용하여 전 국민을 대상으로 막대한 피해를 입히고 있다. 수법도 나날이 교묘하게 진화하고 있는데, 스미싱, 문자미끼, 전화번호 변조, 악성앱 사용 등 신종수법을 동원하고 있다. 수법도 점점 다양해지고 있다.

그동안 정부는 보이스피싱 범죄 예방 홍보와 법제도 마련 등 각종 예방활동을 벌이고 있었다. 법제도 역시 지연인출제도, 채권소멸절차를 간소화한 피해자 환급 법제, 지급정지 등 많은 법제도와 정책을 시행하여 왔었다. 시행 이후 어느 정도 효과가 있는 듯 하였으나, 다시 원점이거나 보이스피싱 범죄와 피해액은 계속적인 증가추세이다. 게다가 신기술과 비대면 인증 서비스로 인하여 그 허점을 악용한 신종 금융범죄 역시 증가추세에 있다. 대표적으로 문자, 악성앱, 중계기 등 다양한 통신수단을 이용하는 방법이 있다.

이에 정부의 지속적인 단속과 범정부적 TF을 마련하여 시행하고 있음에도 불구하고 보이스피싱 범죄는 좀처럼 줄어들지 않고 있다. 이에 본 연구에서는 제1장 최근 보이스피싱 범죄가 점점 진화하여 새로운 범죄가 등장함에 따라 보이스피싱 범죄의 범행단계별 사례를 바탕으로 이를 소개 및 분석하고 각 부처의 대응과 피해자 구제 방안 등을 시사하면서 이에 대한 연구의 필요성과 목적을 도출하였다. 제2장에서는 보이스피싱 범죄의 동향과 유형을 파악하였다. 이를 위하여 초기의 보이스피싱의 유형과 변화하는 보이스피싱 범죄의 유형을 살피고 피해금 편취방법에 따른 유형과 피해자 기망 수법의 유형을 차근차근 고찰하였다. 곧 이어 보이스피싱 발생추세와 특성을 경찰과 금융감독원에서 제시한 통계를 바탕으로 살펴보았다. 제3장에서는 구

체적 유형별 사례를 분석하고 정부의 정책을 진단하였다. 특히 최근의 보이스피싱 사기범죄의 특성을 유형별로 제시하고 보이스피싱 범죄 수법의 변화를 구체적으로 분석 및 진단하였다. 이를 바탕으로 그동안 정부의 보이스피싱 범죄에 대한 대책을 진단해 보았다. 제4장에서는 보이스피싱 범죄피해자에 대한 피해구제방안을 모색하였다. 민사상 손해배상청구에서 범죄피해자 구조 대상의 확대방안, 피해회복위원회의 설치 방안, 보이스피싱 보험과 기금의 활성화 등 다각적인 방안을 제시하였다. 제5장에서는 앞에서 살펴보고 검토한 내용을 요약 및 정리, 그리고 시사점을 도출하였다.

주요 내용과 시사점을 살펴보면, 보이스피싱 범행준비단계의 경우, 조직 및 물적·인적 구성, 조직원 교육 및 관리 등이 있었고 보이스피싱 총책이 조직을 만들고 사무실 및 집기 등 물적 기반을 마련하게 된다. 물적 기반에는 피해자 개인정보가 담긴 DB, 계좌송금 편취방식의 경우 대포통장 모집, 사례에 따라 변작중계기 등이 포함될 수 있다. 인적 구성을 보면, 총책과 관리자급 조직원, 콜센터상담원(혹은 텔레마케터), 현금인출책(혹은 현금수거책), 환전책 등이 있다. 조직원 가담경로를 보면 텔레마케터와 현금수거책의 경우 주변 사람의 소개도 있지만 다양한 매체의 구인광고를 보고 가담한 경우가 많았다. 조직원에 대한 교육은 구체적인 범행방법이 담긴 매뉴얼을 통하여 이루어지고 있는 것을 확인할 수 있었다.

범행실행단계는 보이스피싱 유형별로 살펴보면, 보이스피싱 유형은 대출사기형과 사칭형(기관사칭형, 가족·지인사칭형)으로 구분하였다. 대출사기형의 범행실행단계는 금융기관 직원을 사칭하여 피해자에게 전화해서 저금리 대출 등을 제안 → 피해자의 개인정보 등을 파악할 수 있는 상담 혹은 휴대전화 앱설치 요구 → 피해자 대출내역 확인 → 피해자가 기존에 대출받은 금융기관 직원 사칭하여 전화해서 계약위반, 법위반 등이라고 하며 기존 대출금 상환요구 → 피해자로부터 피해금 편취(현금수거책이 대면편취 혹은 계좌송금) → 현금수거책(혹은 현금인출책)이 조직원이 지정한 계좌로 송금 등으로 이루어진다. 대출사기형 중 저금리대출을 위한 신용도 향상(고금리 대출기록)을 이유로 대출금을 받게 한 후 편취하는 사례도 있었다.

사칭형 중 기관사칭형의 범행실행단계를 보면 수사기관을 사칭하여 피해자에게 전화해서 피해자 계좌의 범죄이용 등을 말함 → 수사목적의 앱설치 혹은 유선조사 등을 통하여 피해자 개인정보 파악 → 수사(혹은 추가피해방지)를 빙자하여 피해자

계좌에 있는 돈(혹은 신규 대출, 상품권 핀번호 등) 요구 → 피해자 돈 편취(대면편취/계좌송금/물품보관함이용) → 현금수거책(혹은 현금인출책)을 통해 조직원이 지정한 계좌로 송금등으로 이루어진다. 기관사칭형 중 피싱문자(해외 결제 승인문자 등) 발송을 포함한 사례의 경우 피싱문자 발송후 연락온 피해자에게 업체 직원 등을 사칭하여 명의도용(계좌범죄 이용)을 언급하며 수사기관을 연결해 주고, 수사기관을 사칭하여 피해금을 편취하는 방식으로 이루어지고 있었다. 가족·지인사칭형은 인터넷 메신저를 이용하며 요청사항(앱설치 및 계좌번호와 비밀번호요청, 대신 결제 등)을 제시하고 피해자가 이를 이행하면 피해자 정보를 이용하여 피해자 계좌에서 직접 돈을 빼 가거나 피해자가 (대포통장으로) 계좌송금한 것을 편취하는 단계로 이루어지는 것을 확인할 수 있었다.

이상의 범행단계별 특성을 토대로 시사점을 제시해보면, 먼저 범행준비단계와 관련하여 첫째, 개인정보 유출에 대한 엄격한 단속이 필요하다. 둘째, 현금수거책 등 조직원 가담을 막기 위하여 구직사이트 등에 대한 엄격한 관리가 필요하다. 다음으로 범행실행단계와 관련하여 첫째, 예방교육이 중요할 것이다. 둘째, 피싱문자 근절을 위한 대책이 중요할 것이다. 피싱문자 근절을 위하여 금융기관과 공공기관에서 발송한 정상적 문자를 수신자가 확인할 수 있게 하기 위해 안심마크(인증마크+안심문구) 표시 서비스를 시범 도입하였다(2022년 10월). 이러한 안심마크표시 서비스에 대해 일반인이 알 수 있도록 홍보하는 것과 더불어 서비스 도입기관이 확대될 필요가 있다. 셋째, 원격조종 앱 설치를 차단할 수 있도록 하는 노력이 중요할 것이다.

금융감독원 보도자료를 참고하여 시기별로 유행한 보이스피싱 수법을 정리해 보면 보이스피싱 수법이 조금씩 변화한 모습을 확인할 수 있다. 최근의 피해 유형은 개인정보를 탈취하는 수법과 연관되어 있는 것을 알 수 있다. 과거 가족 지인을 사칭하여 메신져 피싱을 통해 개인정보를 탈취한 것에서부터 문자나 카카오톡 등에서 지인으로 사칭하여 개인정보 및 인증정보를 요구하는 수법, 대출문자를 받고 개인정보(신분증, 카드)을 송부하도록 하거나 악성 앱을 설치하도록 하는 수법, 그리고 최근 택배, 정부지원금 등 문자를 받고 출처가 불분명한 URL 클릭하도록 하는 수법, 금융 상품 거래 확인서 피싱과 같이 투자성 금융 상품 거래내역을 가공하거나 거래 관련 고객센터 전화번호로 전화를 유도하는 수법 등 교묘해지고 대담해지는 것을 알 수 있다.

보이스피싱과 관련하여 정부는 새로운 수법이 나타날 때 마다 일선에 빨리 알리고 신속하게 대응할 수 있는 프로세스를 제시하고 있다. 금융감독원 등은 내부적 평가를 통하여 가령 소비자 보호실태 평가 등을 통하여 보이스피싱에 정부의 대책이 어느 정도 효과가 있는지 자체평가를 하지만 그럼에도 불구하고 보이스피싱 범죄는 수법을 바꾸거나 새로운 수법이 나타나면서 금융당국을 당혹하게 만들고 있다. 특히 현재 인터넷이 등장하고 가상자산이 활용되면서 보이스피싱과 같은 범죄는 대응하기 어렵다는 분석도 나오고 있다. 따라서 보이스피싱의 경우 가상자산으로 입금하지 말아야 하는 대대적인 홍보가 필요하며 거래소에서는 자체 지침을 통하여 내부적으로 보이스피싱 범죄 관련 이상징후 포착 등의 교육을 통하여 금융회사처럼 자체적으로 대응할 필요가 있다. 그리고 금융위원회가 가상자산을 담당하고 있으므로 수시로 거래소 점검 및 단속을 통하여 보이스피싱 피해에 만전을 기하여 할 것이다. 은행직원이든 거래소 직원이든 보이스피싱의 예방과 대응과 관련하여 보이스피싱 피해를 방지하거나 범죄자를 검거할 경우 별도의 인센티브나 인사고과에 반영하는 방안도 고려될 수 있다.

한편, 부처간 업무도 상이하고 관할도 다르다. 금융감독원의 경우는 사칭형(메신져, 비메신져)과 대출빙자형을 담당하고 있으며, 전화번호이용중지의 경우는 방송통신위원회가 담당하고 있고 가상자산의 경우는 금융위원회에 담당하고 있다. 또한 전화번호나 변작신고는 인터넷 진흥원(KISA)가 담당하고 있듯이 각 부처의 역할도 서로 다른 것을 확인할 수 있었다. 사실상 현재 상황에서는 신고가 들어와도 부처의 업무가 아닌 이상 다른 곳으로 신고를 해야 한다. 사정이 이렇다 보니 통합신고센터를 만들어서 대응해야 한다는 목소리도 커지고 있는 상황이다. 통합신고센터가 통합신고ㆍ대응센터로 명실상부한 보이스피싱 대응 및 피해구제 기관으로 거듭나려면 상담은 물론 신속한 대응과 피해구제도 함께 가능해야 한다. 보이스피싱 범죄는 하나의 독립된 범죄가 아닌 여러 가지 속성과 특성을 가지고 있기 때문에 각 부처가 별개로 이루어서 대응하기란 사실상 의미가 없을 수도 있기 때문에 함께 하나의 보이스피싱 범죄 대응이라는 목표아래 일사천리로 대응하고 전파하고 예방하는 시스템이 함께 이루어질 필요가 있다.

2023년 7월 초부터는 개인정보가 노출자 시스템을 도입하여 간편송금제도를 보완

및 수정한 일괄지급제도를 시행하고 있다. 정부의 대책대로 지급정지는 보이스피싱을 근절하기 보다는 피해자 구제 차원에서 획기적인 대책으로 평가되고 있었다. 그러나 최근 이러한 전체 지급정지가 오히려 선의의 피해자에게는 피해를 주는 제도가 되고 있는 만큼 정부는 전체지급정지제도에서 부분지급정지제도로 변환하거나 특정은행에 한하여 지급정지를 추진하는 것도 의미가 있다. 아울러 보이스피싱 범행에 가담하지 않게 하기 위해서는 현금수거책이나 그 외 방조범에게도 전반적으로 형량의 구형을 높일 필요가 있으며, 법원은 보이스피싱 방조범에게 범죄단체의 미필적 고의를 확대 해석하여 실형을 선고할 필요가 있다.

한편, 현행 통신사기피해환급법은 금융회사에 대하여 금융거래시 본인확인조치의무와 지급정지의무, 임시조치의무를 부과하고 있고, 이를 이행하지 않을 경우 법원은 손해배상책임을 인정하고 있고, 이는 비대면 전자금융거래 방식의 보이스피싱 피해 예방과 피해구제를 위한 실효적인 제도적 장치가 되고 있다. 피해구제의 측면에서 보완되어야 할 부분을 살펴보면, 본인확인조치 등 피해방지의무를 여신전문금융회사와 대부업체까지 확대할 필요가 있다는 점, 금융회사 등의 피해 방지의무를 좀 더 구체적으로 정하고 이에 대한 손해배상책임을 명문화할 필요가 있다는 점, 대면편취형 보이스피싱의 경우에도 금융회사의 피해방지책임이 인정되는 예시 규정을 둘 필요가 있는지 검토가 필요한 점 등을 들 수 있다.

보이스피싱 피해 구제와 관련해서 보이스피싱 보험의 의무보험화나 금융상품 가입시 금융회사의 설명의무를 도입하는 것도 검토되어야 한다. 그리고 보험가입금액을 1인당 평균적인 피해금액에 비추어 최소한 1,000만 원 이상으로 확대하고, 대면편취형도 보장범위에 포함시켜 피해구제에 빈틈이 생기지 않도록 현실화하여야 한다. 결국, 현행 피해구제 제도의 한계를 고려할 때, 피해구제를 위해 가장 적합한 모델로 고려해 볼 수 있는 것은 자동차손해배상보장법상 의무보험 형태의 책임보험과 연계된 자동차손해배상 보장사업과 약사법상 의약품 부작용 피해구제사업이다. 이러한 모델을 기초로 보이스피싱과 같은 전기통신금융사기 피해자의 피해구제를 위한 피해기금을 마련하여 피해구제를 함으로써, 통신사기피해환급법상 피해환급절차와 금융회사 내지 가해자를 상대로 한 손해배상 청구 등을 통해서도 회복되지 않는 피해자의 손해를 신속하게 보상해주는 제도가 절실히 필요하다.

서 론

윤 해 성

제1장

서 론

제1절 | 연구의 필요성과 목적

보이스피싱 범죄는 2006년 최초 발생하여 서민경제를 침해하는 대표적인 범죄로 인식되고 있다. 보이스피싱 피해액의 경우 국무조정실 자료에 의하면 2017년 2,470억에서 2018년 4,040억, 2019년 6,398억, 2020년 7,000억, 2021년 7,744억으로 점차 늘어나고 있어 상당히 심각한 사회 문제로 대두되고 있다.[1] 초기 서민이나 노인들을 상대로 정부기관을 사칭하였던 서민범죄에서 이제는 대면편취형과 대담한 수법을 사용하여 전 국민을 대상으로 막대한 피해를 입히고 있다. 수법도 나날이 교묘하게 진화하고 있는데, 스미싱, 문자미끼, 전화번호 변조, 악성앱 사용 등 신종수법을 동원하고 있다. 이처럼 보이스피싱 수법은 과거 수법을 반복하기도 하고 새로운 수법을 활용하는 등 피해 수법도 점점 다양해지고 있다.

그동안 정부는 보이스피싱 범죄 예방 홍보와 법제도 마련 등 각종 예방활동을 벌이고 있었다. 예방활동으로는 소비자 경보, 특정 유형 ~~을 주의해 달라 등 문자와 방송, 은행 ATM 기계의 홍보 문구가 대표적이다. 법제도 역시 지연인출제도, 채권소멸절차를 간소화한 피해자 환급 법제, 지급정지 등 많은 법제도와 정책을 시행하여 왔었다. 시행 이후 어느 정도 효과가 있는 듯 하였으나, 다시 원점이거나 보이스피싱 범죄와 피해액은 계속적인 증가추세이다. 게다가 신기술과 비대면 인증 서비스로 인하여 그 허점을 악용한 신종 금융범죄 역시 증가추세에 있다. 대표적으로 문자, 악성앱, 중계기 등 다양한 통신수단을 이용하는 방법이 그것이다. 이에 통신이나 금융

1) 국무조정실, 2022년 9월 29일자 1면 보도자료.

단계에서 사전 차단 및 적발대책이 검토되어야 할 필요가 있다는 주장이 설득력을 얻고 있다. 나아가 보이스피싱 범죄는 독립적인 부처에서만 해결할 상황이 아니라 범정부 내지 관련 부처가 서로 합동하여 대응할 필요가 있다.

보이스피싱 범죄는 계속적으로 지능화, 고도화되어 피해도 증가하고 있다. 이에 정부의 지속적인 단속과 범정부적 TF을 마련하여 시행하고 있음에도 불구하고 보이스피싱 범죄는 좀처럼 줄어들지 않고 있다. 이에 본 연구에서는 보이스피싱 범행단계별 대응방안을 시대별로 진단하고 이에 따른 범행수법이나 피해자 특성 등 범행유형별로 다양한 수단을 분석하고 시사점을 던져주고자 한다. 또한 최근 통신, 금융수단을 이용하고 있는 만큼 이를 사전에 차단하고 범죄피해를 예방할 수 있는 방안도 강구하고자 한다. 아울러 보이스피싱 범죄가 전 국민을 상대로 피해를 주는 범죄인 만큼 피해를 구제할 수 있는 사후방안도 함께 모색하고자 한다.

제2절 | 연구방법과 범위

이 연구의 연구추진방법은 다음과 같다. 보이스피싱 범행단계별 대응방안을 연구하기 위하여 그동안의 선행연구와 사례를 분석하고 관련 법제도를 살펴보는 것은 물론 최근 등장하고 있는 보이스피싱 수법을 소개 및 분석하는데 중점을 두었다. 아울러 그동안의 보이스피싱을 방지하기 위한 유관부처의 정책들을 평가하면서 피해자 구제 방안을 모색하였다. 이처럼 국내외 문헌연구는 물론 수사사례를 조사 분석하여 보이스피싱 범행수법과 단계를 파악하고자 한다. 이를 위해서 경찰청, 금융감독원, 과학기술정통부, 방송통신위원회 등의 실무자 자문회의를 통해 공식통계자료를 정리하고 보이스피싱 추세와 유형에 대한 대응책도 살펴보고자 한다.

본 연구에서는 다음과 같은 구성에 따라 그 범위를 설정하여 고찰하기로 한다. 제1장에서는 최근 보이스피싱 범죄가 점점 진화하여 새로운 범죄가 등장함에 따라 보이스피싱 범죄의 범행단계별 사례를 바탕으로 이를 소개 및 분석하고 각 부처의 대응과 피해자 구제 방안 등을 시사하면서 이에 대한 연구의 필요성과 목적을 도출하

였다.

제2장에서는 보이스피싱 범죄의 동향과 유형을 파악하였다. 이를 위하여 초기의 보이스피싱의 유형과 변화하는 보이스피싱 범죄의 유형을 살피고 피해금 편취방법에 따른 유형과 피해자 기망 수법의 유형을 차근차근 고찰하였다. 곧 이어 보이스피싱 발생추세와 특성을 경찰과 금융감독원에서 제시한 통계를 바탕으로 살펴보았다.

제3장에서는 구체적 유형별 사례를 분석하고 정부의 정책을 진단하였다. 특히 최근의 보이스피싱 사기범죄의 특성을 유형별로 제시하고 보이스피싱 범죄 수법의 변화를 구체적으로 분석 및 진단하였다. 이를 바탕으로 그동안 정부의 보이스피싱 범죄에 대한 대책을 진단해 보았다.

제4장에서는 보이스피싱 범죄피해자에 대한 피해구제방안을 모색하였다. 민사상 손해배상청구에서 범죄피해자 구조 대상의 확대방안, 피해회복위원회의 설치 방안, 보이스피싱 보험과 기금의 활성화 등 다각적인 방안을 제시하였다.

제5장에서는 앞에서 살펴보고 검토한 내용을 요약 및 정리, 그리고 시사점을 도출하면서 결론에 갈음하였다.

보이스피싱 범죄의 동향과 발생추세

전영실 · 이정민

제2장

보이스피싱 범죄의 동향과 발생추세

제1절 | 보이스피싱범죄의 동향과 유형 파악

1. 보이스피싱 범죄의 동향

국내에서는 2006년 최초[2][3]로 발생한 보이스피싱(Voice Phishing)[4][5] 사건을 시작으로, 기술의 발달과 함께 범죄수법은 변화하고 교묘해지면서 지금까지도 많은 피해를 발생시키고 있다. 보이스피싱 범죄는 전기통신과 금융의 발전과 함께 진화하면서 너무나 일상적인 범죄로 자리잡았다. 초기에는 금융지식이 상대적으로 낮은 노년층을

2) 우리나라 최초 보이스피싱 발생은 대부분의 연구자들이 2006년 5월 국세청 세금 환급 사건으로 보고 있다. 서준배, "보이스피싱 현황, 유형, 추이와 대응관련 시사점", 통계청 통계개발원 한국의 사회동향, 2022, 307면 참조; 정정원, "보이스피싱(Voice Phishing)범죄의 형사법적 검토 및 대응방안", 가천법학 통권 15호, 2013, 39면 참조; 이기수, "최근 보이스피싱의 범죄수법 동향과 법적 대응방안", 범죄수사학연구 제4권 제2호, 2018, 3면 참조.

3) 국내에서 최초 발생한 피싱사건의 경우는 2005년 국내 은행 피싱사이트를 제작하여 인터넷 카페에 대출 광고를 게시하고, 이를 보고 연락온 피해자들에게 사이트 접속을 유도하여 피해자들이 입력한 금융정보로 계좌에서 피해금을 인출하는 방법으로 총 12명에게 1억2천만원 상당을 편취한 사건이 있다. 뉴스타운, "무선인터넷 이용 은행 피싱사이트 조직 첫 검거", 2005.11.17. https://www.newstown.co.kr/news/articleView.html?idxno=25093 (최종검색일: 23. 8. 15.) 참조.; 김대근·임석순·강상욱·김기범, "신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구-기술적 수단을 사용한 사이버 금융사기를 중심으로-, 한국형사정책연구원 연구총서 16-CB-03, 2016, 91면 참조.

4) '보이스피싱(Voice Phishing)'이란 음성(Voice)와 개인정보(Private data) 그리고 낚시(Fishing)을 합성한 용어로, '전화를 통해 개인정보를 낚아 올린다.'는 뜻을 가지고 있다. 이유주, "전화금융사기(보이스피싱) 대응책의 현황 및 개선방안", 국회입법조사처 현안보고서 제34호, 2009, 2면 참조.

5) 「전기통신금융사기 피해금 환급에 관한 특별법」 제2조의2에서는 보이스피싱을 '전기통신금융사기'로 규정하며, 전기통신을 이용하여 타인을 기망(欺罔)·공갈(恐喝)함으로써 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하게 하는 행위로 규정하고 있고, 이러한 행위에 자금을 송금·이체하도록 하는 행위와 개인정보를 알아내어 자금을 송금·이체하도록 하는 행위라고 규정하고 있다. 본 연구에서는 일반적으로 통용되고 있는 '보이스피싱'이라는 용어를 사용한다.

대상으로 범죄가 발생하였지만, 어느 순간부터 남녀노소의 구분없이 광범위하게 발생하고 있어 피해범위는 계속해서 확대되고 있다.

또, 보이스피싱은 초기에 연금관리공단 금융기관, 검찰, 경찰, 국세청, 등의 기관사칭형 유형으로 피해자를 현금인출기(ATM)까지 직접 가서 대포통장으로 이체하게하는 수법을 주로 사용했다면, 이러한 사기수법이 많이 알려진 이후에는 경품행사당첨, 대학등록금 환급 등 새로운 시나리오를 사용하는 것에서부터 사전에 입수한 개인정보를 활용해서 대출을 빙자하는 수법, 카드론 대출 등으로 금원을 편취하는 수법을 사용했다.[6)]

최근 정부 보도자료를 살펴보면, 22년 보이스피싱 피해 발생이 16년만에 큰 폭으로 감소 했다는 발표를 하였으나, 기관사칭형과 대출사기형의 경우에 대한 부분인 것으로 확인[7)]되며, SNS와 메신저를 활용한 피싱 범죄의 경우 집계되지 않은 통계자료로 보이스피싱이 줄었다는 '착시현상'에 불과하다는 주장도 있다.[8)]

이처럼 보이스피싱 범죄는 기존 방식에서 머물러 있지 않고, 패턴은 변화하고 있으며, 조직원들은 계속해서 피해자를 기망하고 단순 가담자를 모집하는 시나리오를 연구하여 남녀노소를 불문한 피해자를 양산하고 있다.

2. 보이스피싱 유형 파악

가. 초기의 보이스피싱

보이스피싱 발생 초창기에는 범행수법이 잘 알려지지 않았기 때문에 대부분의 피해자들은 의심없이 돈을 송금했다.

보이스피싱을 '협의'와 '광의'의 구분하는 개념도 있다. 이 분류에서는 "유무선 전

---

6) 윤해성·김유근, "보이스피싱 피해유형별 구체적 예방방안에 관한 연구", 대검찰청 연구용역보고서, 2017, 3면 참조.

7) 국무조정실 국무총리비서실 보도자료, "보이스피싱 대응 범정부 TF 회의, 2023.02.01. https://www.opm.go.kr/opm/news/press-release.do?mode=view&articleNo=152623&srSearchVal=%EB%B3%B4%EC%9D%B4%EC%8A%A4%ED%94%BC%EC%8B%B1&article.offset=0&articleLimit=10 (최종검색일 : 2023. 08. 20.) 참조.

8) 연합뉴스, "[진화하는 보이스피싱] ③ "극단적 선택까지"···갈수록 심해지는 폐해(끝)", 2023.05.27. https://www.yna.co.kr/view/AKR20230526109400061?input=1195m (최종검색일 : 2023. 08. 20.) 참조.

화, 인터넷 전화 등으로 피해자와 직접 대화(voice)를 하고, 기망하여 피해자가 자발적으로 금전을 제공한 경우"를 '협의'의 보이스피싱으로 보고, "피해자에게 금융정보를 편취하여 그 금융정보로 사기범이 금원을 편취하는 경우"는 '광의'의 개념으로 보았다.[9] 보이스피싱의 가장 기본적인 사기과정은 "'사기이용계좌를 확보' → '전화, 문자 메시지 시도' → '피해자 기망 또는 공갈' → '피해자의 계좌이체' → '사기이용계좌에서 금원 인출 또는 송금'"[10]이라고 할 수 있다.

대부분 조직범죄의 형태로 구성되어 있고, 조직 내부에서도 별개의 사업체처럼 경영자가 다른 여러 보이스피싱 조직으로 운영되며, 조직 내부는 유인책(피해자를 속이는 그룹), 모집책(수거책 모집, 피해금원을 입금할 계좌나 통장 모집), 수거책(피해자로부터 현금을 받아서 입금 또는 송금)으로 분류할 수 있다.[11]

[표 2-1] 일반적인 보이스피싱 발생과정

[보이스피싱 과정]
○ 사기이용계좌 확보 : 신용불량자, 노숙자 등을 이용하여 예금통장 매입, 대출 또는 취업을 미끼로 예금통장 편취
○ 콜센터(해외 등)에서 국내로 전화 : 해외에 본부를 둔 조직원이 금융기관 및 검찰, 경찰 등 발신자번호를 조작하여 무작위로 국내에 전화
○ 기망·공갈 : 개인정보 유출, 범죄사건 연루 등의 명목으로 피해자를 기망하여 개인정보와 금융정보를 편취
○ 계좌이체 : 계좌보호조치 또는 범죄혐의 탈피 등의 명분으로 사기계좌로 이체를 유도하거나, 편취한 피해자 개인정보로 공인인증서 재발급받아 사기범이 직접 이체
○ 인출·송금 : 현금인출책이 송금책의 계좌로 입금, 송금책은 환치기 등의 방법으로 조직 본부로 송금

출처: 서울동부지방법원 이은미 변호사, 2023.08.14., 보이스피싱 범죄 유형 관련 인터뷰 참조.

나. 진화하는 보이스피싱

보이스피싱은 최초발생부터 2023년도인 지금까지도 발생하고 있고, 많은 피해를 남기고 있으며 정보통신의 발달과 함께 새로운 기술과 결합하면서 범죄유형이 다양한

9) 김동민, "접근매체를 이용하는 전자금융사기의 범위에 관한 소고", 법학연구 제31권 제2호, 2020, 53-54면 참조.
10) 김민정·김은미, "보이스피싱 피해 경험 및 영향요인 분석", 소비자문제연구 제52권 제1호, 2021, 4면 참조.
11) 서울동부지방법원 이은미 변호사, 2023.08.14., 보이스피싱 범죄 유형 관련 인터뷰 참조.

형태로 진화하고 있다. 뿐만 아니라 피싱범죄에서 피해자를 기망하는 시나리오도 당시 사회상황에 따라 맞추어 변하고 있는 것을 살펴볼 수 있다.

분명 초기에는 외국인 조직원이 한국인을 대상으로 한 피싱범죄로 주로 서울과 경기도를 중심으로 발생하는 것이 일반적이었으나, 이제는 한국인들도 범행에 가담하고, 피해범위는 전국으로 확대되었다.[12][13] 같은 수법을 사용하지 않고, '국내 경제불황, 코로나19' 등 지속적으로 사회상황을 모니터링하고, 그 시기에 맞는 수법을 사용하면서 피해를 꾸준히 확대해나가고 있는 것은 물론, 국가에서 대응을 하기 위해 대응책을 마련하면 또 다른 수법을 사용하며 빠져나간다.[14][15]

우리나라 뿐만 아니라 연변지역 등 에서도 2002년 첫 보이스피싱 시작 당시에는 문자와 전화 등을 이용하였으나, 이후 인터넷, VoIP[16]를 사용하는 등 사기 수단이 빠르게 변화하고 점점 지능형 범죄로 변하면서 초국가적 범죄로 자리 잡았다.[17]

최근 중계기를 단속하면서 발신번호 변작을 차단하였으나, 이제는 전화가 아닌 SNS를 이용하여 메신저 피싱이 활발해지는 등 "특정 수단 또는 도구에 대한 차단은 범죄자들이 새로운 도구를 모색하게 하고 새로운 피싱범죄가 발생"하면서 장기적으로 피싱범죄를 감소시키는 근본적인 대책으로는 부족하다고 평가된다.[18]

---

12) 이기수, "최근 보이스피싱의 범죄수법 동향과 법적 대응방안", 범죄수사학연구 제4권 제2호, 2018, 4면 참조.
13) 김성언·양영진, "전화 금융사기 범죄의 진화", 한국공안행정학회보 제17권 제3호, 2008, 115-116면 참조.
14) 이기수, "최근 보이스피싱의 범죄수법 동향과 법적 대응방안", 범죄수사학연구 제4권 제2호, 2018, 4면 참조.
15) 김성언·양영진, "전화 금융사기 범죄의 진화", 한국공안행정학회보 제17권 제3호, 2008, 115-116면 참조.
16) VoIP(Voice over Internet Protocol)이란, "IP주소를 사용하는 네트워크를 통해 음성을 디지털 패킷(데이터 전송의 최소 단위)으로 변환하고 전송하는 기술"을 의미하고, 간단하게 말하면 '인터넷 전화'를 의미한다. IT dongA, "[IT강의실] 인터넷으로 싸게 전화하자 – VoIP", 2015.10.02. https://it.donga.com/22530/ (최종검색일 : 2023.09.03.) 참조.
17) 김경찬·정군남·김창준·현송학, "중국 동북지역 한국관련 마약범죄와 보이스피싱범죄의 실태 및 대응방안에 관한 연구", 한국형사정책연구원 연구총서 13-AA-13, 2014, 120-122면 참조.
18) 최형욱·이상진, "피싱 범죄의 현황과 대응 방안 모색", 치안정책연구 통권 60호, 2022, 117면 참조.

1) 파밍(Pharming)

2011년도에는 보이스피싱에서 나아가 "공공기관, 금융회사 인터넷 홈페이지를 가장한 피싱사이트를 개설하고, 금융정보를 입력하도록 하는 방법"[19]을 사용했으나, 이후 파밍(Pharming)이 신종범죄로 나타났다. 파밍(Pharming)은 악성코드의 한 종류이며, 사용자의 컴퓨터에 악성코드 감염으로 발생하게 되며[20], 사용자가 평소처럼 진짜 웹페이지에 접속하려고 해도 미리 제작해둔 파밍 사이트로 접속되고, 사용자는 공식 홈페이지로 알고 입력한 금융정보, 탈취한 공인인증서를 활용하여 온라인 뱅킹 서비스를 받아 금전적인 피해를 양산한다.[21]

사기범이 편취한 금융정보를 활용하여 정상적인 경로로 온라인 뱅킹 서비스를 이용하기 때문에 피해자는 본인명의로 대출금이 생겨도 바로 알기가 쉽지 않다는 문제점이 있다.

2) 스미싱(Smishing)

스미싱(Smishing)은 "문자메시지로 은행, 금융기관 등 관련 웹사이트 링크를 발송하여, 휴대폰 사용자가 링크를 클릭하면 악성코드가 설치되고, 설치된 악성코드를 이용하여 휴대폰을 통제하면서 소액결제가 이루어지게 하거나, 금융정보를 탈취하는 수법"이다.[22]

2011년 스미싱 발생 초기에는 금융감독원 명의로 '금융감독원 긴급공지/포털사이트 정보유출로 인한 피해발생 확인 요망(링크)'의 내용의 문자를 발송해 링크로 접속하면 피싱사이트로 유도되고, 공식사이트라고 믿은 피해자가 입력하는 금융정보를 이용하여 피해금을 편취하는 사례가 대부분이었다.[23] 2세대 피싱범죄라고 할 수 있으며,

---

19) 금융감독원 보도자료, "인터넷 피싱사이트를 이용한 신종 전화금융사기 주의!", 2011.01.19. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=8272&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=20 (최종검색일 : 2023.06.27.) 참조.

20) 김기창, "전자금융거래법상 '이용자의 중대한 과실' - 대법원 2013다86489 판결의 문제점-", 정보법학 제18권 제3호, 2014, 196면 참조.

21) 이세빈·이지오·염흥열, "금융정보를 탈취하는 파밍 악성코드 분석 및 대응방안", 정보보호학회지 제27권 제3호, 2017, 48-51면 참조.

22) 김동민, "접근매체를 이용하는 전자금융사기의 범위에 관한 소고", 법학연구 제31권 제2호, 2020, 63-64면 참조.

23) 금융감독원 보도자료, "금융감독원 피싱사이트 유도 문자메시지 주의!", 2012.03.23.

메신저로 연결된 피싱사이트를 통해 “수집한 개인정보(계좌번호, 비밀번호, 금융보안카드번호 등)를 이용하여 예금을 불법으로 인출하는 등의 추가 범행”을 발생시킨다.[24]

금융감독원에서 공개한 스미싱을 통해 피싱사이트로 유도하는 경로는 아래 표와 같다.

[표 2-2] 스미싱을 통해 피싱사이트로 유도하는 경로

① 사기범이 불특정 다수에게 정보유출로 피해발생 여부를 확인하라는 문자메시지를 발송, 금융감독원 피싱사이트로 유도
② 문자메시지 사이트주소 링크로 접속하면 최근 정보유출로 피해가 많이 발생한다는 긴급공지 안내 화면으로 이동
③ 긴급공지 화면에서 확인을 누르면 금융정보 조회하기 화면으로 이동
④ 금융정보 조회하기 화면에서 성명, 주민번호 입력 → ‘조회하기’ 누르면 이용중인 은행 선택화면으로 이동
⑤ 이용중인 은행 선택하고 확인 누르면 ‘대출 사용정보 선택 화면’으로 이동
⑥ 대출사용정보를 선택하고 확인 누르면 대출사용 내역 조회됨 → 대부업체 이용내역 등 전혀 맞지 않는 이용내역이 나타남
⑦ 대출사용정보 조회결과가 틀려서 아니요를 누르면 예금보호등록을 신청하라는 화면으로 이동
⑧ 예금보호등록신청을 누르면 E-금융민원센터 화면으로 이동
⑨ E-금융민원센터에서 동의함을 누르면 계좌정보를 입력하는 화면으로 이동
⑩ 계좌정보를 입력하고 확인 누르면 이용중인 보안정보를 입력하라는 화면으로 이동
⑪ 이용중인 보안정보 선택 화면에서 보안카드를 누르면 보안카드일련번호를 입력하는 화면으로 이동

출처: 금융감독원 보도자료, "금융감독원 피싱사이트 유도 문자메시지 주의!", 2012.03.23. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=9092&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=18 (최종검색일 : 2023. 6. 27.) 참조.

문자메시지보다 ‘SNS’를 더 활발하게 사용하는 현 시대에 맞추어 스미싱에서 카카오톡 또는 인스타그램 DM(Direct Message)를 매개체로 활용하는 메신저피싱으로 범죄수법이 변화한 것을 볼 수 있고, 경품 전달을 빙자한 사이트 접속을 유도하여 개인정보 등을 편취한다.[25]

---

https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=9092&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=18 (최종검색일 : 2023. 6. 27.) 참조.

24) 황석진, "전기통신금융사기 근절을 위한 고찰 -보이스 피싱을 중심으로-", 경찰학연구 제21권 제1호, 2021, 95면 참조.

3) 메신저피싱(Messenger Phishing)[26]

위에서 살펴본 바와 같이, PC보다 스마트폰을 더 이용하고, 메신저를 기본으로 사용하는 사람들이 증가함에 따라 피싱범죄도 함께 문자에서 메신저로 범행환경이 변화하게 되었다. 대부분은 지인과 가족을 사칭하기 때문에 주소록을 해킹하거나 불법적인 거래로 개인정보를 취득하여 메신저로 연락을 주고받을 피해자의 기본적인 정보를 파악하고 있는 경우가 많다.[27] 실제로 일어났던 메신저 피싱 사례를 살펴보면 아래와 같다.

① 계좌이체 요구 : 자녀 또는 지인으로부터 휴대폰 액정이 나가 A/S를 맡겨 통화가 어려운 상태이고, 사정이 있어 친구의 원룸 보증금을 본인이 보관하고 있다가 급히 이체를 해주어야 하는데, 휴대폰 고장으로 은행 인증서 확인이 어려워 그 금액을 대신 송금해달라고 하여 금원을 편취하는 방법이다.[28]

② 문화상품권·기프트카드 PIN번호 전송 요구 : 지인을 사칭하여, 모바일 상품권을 오류가 생겨서 대신 결제해달라거나 문자로 전송되는 PIN번호를 알려달라고 메신저로 요구하는 방법이다.[29]

③ 보이스톡으로 신분 확인 차단 후 요구 : 메신저 피싱 방법이 많이 알려지면서 목소리를 확인하는 경우가 많아지자, 사기범들은 먼저 보이스톡을 시도한 흔적을 남기고 '컴퓨터라 잘 들리지 않는다'라며 추가 신분 확인을 차단하는 방법 등을 사용한다.[30]

---

25) 여혜린, "피싱과 스미싱을 주로 한 사이버 사기의 현황 및 입법 제언", KHU글로벌 기업법무리뷰, 제15권 제1호, 2022, 98면 참조.

26) 메신저 피싱(Messenger phishing)이란, 카카오톡, 네이트온, 페이스북 등 타인의 메신저 아이디를 도용하여 로그인한 뒤, 등록된 지인에게 메시지를 보내 금전을 편취하는 범죄수법이다. 방송통신위원회·금융위원회·경찰청·금융감독원 공동보도자료, "가족, 지인 사칭 「메신저피싱」주의 당부 –이동통신3사 전 가입자 대상 피해예방 문자메시지 발송–", 2022.05.12. (최종검색일 : 2023. 08. 05.) 참조.

27) 정영호·하형준, "메신저피싱 범죄의 실태와 대응방안에 관한 연구", 범죄수사학연구 제8권 제1호, 2022, 33-34면 참조.

28) 카카오, "메신저 피싱, 사기범들은 이렇게 접근합니다(사례를 통해 알아보는 피해 예방 요령), 2019.10.17. https://brunch.co.kr/@andkakao/125 (최종검색일 : 2023. 08. 05.) 참조.

29) 정영호·하형준, "메신저피싱 범죄의 실태와 대응방안에 관한 연구", 범죄수사학연구 제8권 제1호, 2022, 38면 참조.

30) 카카오, "메신저 피싱, 사기범들은 이렇게 접근합니다(사례를 통해 알아보는 피해 예방 요령), 2019.10.17. https://brunch.co.kr/@andkakao/125 (최종검색일 : 2023. 08. 05.) 참조.

④ 신용카드 등 결제정보 요구 : 인터넷 쇼핑 간편 결제 인증이 활성화됨에 따라, 메신저로 자녀 또는 친구를 사칭하며 신분증과 신용카드 사진, 비밀번호를 요구하여 정보를 얻어낸 후, 직접 온라인 문화상품권과 기프트카드 등을 구입하여 현금화하는 방법이다.[31]

⑤ 원격제어 앱 설치 및 조작 : 2020년 하반기부터 나타난 범죄수법이며[32], 정상적인 앱인 것처럼 위장해서 설치하게 하거나, 모르는 사이에 휴대폰에 설치되기도 하며, '악성앱'이 깔린 스마트폰은 피싱 조직원이 중간에 전화를 가로채 피해자가 아무리 경찰, 금융감독원에 전화를 한다고 해도 사기범이 전화를 받을 수 있고, 연락처와 문자 내용을 다 수집하는 방법이다.[33]

딸을 사칭한 사기범은 "액정이 깨져서 수리해야하는데, 계좌 정보가 필요하고, 인증을 위해 보내주는 링크를 눌러서 프로그램을 깔아"라고 요구하며 휴대전화를 먹통으로 만들고 조종했다.[34]

4) 메모리 해킹(Memory Hacking)

"파밍이 변화된 형태의 신종수법으로, 악성코드를 이용해 피해자 금융정보를 편취한다는 점은 파밍과 유사하지만, 메모리해킹은 악성 프로그램을 PC에 설치해서 피해자의 인터넷뱅킹 프로세스에 직접 개입하여 정상적인 거래방법과 동일하게 최소한의 금융정보만 얻는다는 점에서 모든 정보를 요구하는 파밍"과는 다르다.[35] 기존에는 "온라인 게임에서 데이터를 조작하기 위해, 비밀번호를 탈취할 때 주로 사용된 방식이었으나, 신종금융사기에서도 점차 사용이 확대"되었고, 2013년 말까지 피해가 계속되

---

31) 정영호·하형준, "메신저피싱 범죄의 실태와 대응방안에 관한 연구", 범죄수사학연구 제8권 제1호, 2022, 40면 참조.
32) 정영호·하형준, "메신저피싱 범죄의 실태와 대응방안에 관한 연구", 범죄수사학연구 제8권 제1호, 2022, 40면 참조.
33) 카카오뱅크, "내 휴대폰에 숨어 있는 악성앱, 카카오뱅크가 찾아드려요", https://www.kakaobank.com/bank-story/234 (최종검색일 : 2023. 08. 05.) 참조.
34) 연합뉴스, "'앱 하나 깔았다가'···휴대폰 속 모든 정보가 피싱범에게로", 2023.05.25. https://www.yna.co.kr/view/AKR20230525053000061 (최종검색일 : 2023. 08. 05.) 참조.
35) 금융감독원, 「금융사기예방법」, 금융감독원 발간, 2014. 52면을 참조한 김동민, "접근매체를 이용하는 전자금융사기의 범위에 관한 소고", 법학연구 제31권 제2호, 2020, 65면 참조.

었으나, 2014년 이후는 범죄조직 검거 이후 급격하게 발생이 감소했다.[36]

메모리해킹에는 ① 피해자가 인터넷 뱅킹으로 이체하기 위해 금융정보를 입력하면 악성프로그램으로 중간에서 가로채고, 이 정보를 이용하여 피해자 계좌에서 금원을 편취하는 정보유출형 수법이 있고, ② 악성프로그램으로 피해자가 입력한 송금받을 계좌와 금액을 악성프로그램으로 변경하여 금원을 편취하는 정보변조형 수법이 있다.[37]

5) 이메일해킹 무역사기

이메일해킹 무역사기 유형은 주로 국내 무역회사를 대상으로 발생하며, 무역업체의 이메일을 해킹하여 상대 거래처로 위장하고 사기계좌를 통해 무역대금을 송금하도록 유도하는 수법이다.[38]

이메일해킹 무역사기 범죄유형을 살펴보면, ① 판매자 이메일 해킹형 : 판매자의 이메일 계정을 해킹하여 구매자에게 '물품대금 수취계좌'를 변경하는 이메일을 보내어 사기범이 지정한 계좌로 물품 대금을 송금 받는 수법이 있으며, ② 구매자 이메일 해킹형 : 구매자의 이메일을 해킹하여 판매자의 이메일 주소와 유사한 이메일 주소를 생성하고 구매자에게는 물품대금 수취계좌를 변경한다는 이메일을 보내서 사기범이 지정한 계좌로 송금을 유도하여 금원을 편취하는 수법이 있다.[39]

2017년부터 2021년까지 이메일 해킹 무역사기는 꾸준히 피해사례가 발생하였으며, 제3의 국내업체의 거래계좌를 자금 수령 통로로 악용하는 사례까지 발생하면서 자신도 모르는 사이에 제3의 국내업체는 가짜 무역중개상 역할을 수행하며 사기 범죄에 연루되는 경우도 발생했다.[40]

---

36) 김대근·임석순·강상욱·김기범, "신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구", 한국형사정책연구원 연구총서, 2015, 110-112면 참조.
37) 김대근·임석순·강상욱·김기범, "신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구", 한국형사정책연구원 연구총서, 2015, 111면 참조.
38) 금융감독원 보도자료, "외환 무역사기거래에 대한 유의사항 안내", 2021.12.02. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=16658&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EB%AC%B4%EC%97%AD%EC%82%AC%EA%B8%B0&pageIndex=1 (최종검색일 : 2023. 08. 19.) 참조.
39) 김대근·임석순·강상욱·김기범, "신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구", 한국형사정책연구원 연구총서, 2015, 119면 참조.
40) 아시아경제, "금감원 이메일 해킹 '무역사기' 주의보 발령", 2021.12.01. https://view.asiae.co.kr/article/2021120109555910380 (최종검색일 : 2023. 08. 19.) 참조.

6) 몸캠피싱[41]

① 기본적인 수법 : 컴퓨터 또는 스마트폰을 이용하여 음란화상채팅을 유도하고, 해당 영상을 녹화한 후 영상을 유포하겠다고 협박하여 금전을 갈취하는 수법으로, 코로나19로 인하여 비대면으로 관계를 형성하는 경우가 많아지면서 자연스럽게 피해가 급증하게 되었다. 이러한 범죄는 처음에는 200만 원 정도의 금액을 요구하지만 한번 돈을 송금하면 더 큰 금액을 요구하거나, 돈이 없어 보이는 경우 피해자를 협박해서 범행에 끌어들이는 경우도 있다.[42]

② 악성파일 다운 없이 SNS 활용 수법 : SNS를 활발하게 활용하는 청소년과 20대 청년들이 몸캠피싱의 주요 타깃이 되고 있다는 점이 가장 심각한 문제이며, 최근에는 "해킹파일 다운로드를 이용한 기본적인 수법이 대중에게 노출되면서 타인 사진을 도용하여 SNS계정을 생성하고 이를 통해 피해자의 지인 명단을 쉽게 확보하는 방법"을 사용하여 꼭 악성파일을 다운받지 않아도 피해자에게 접근 후 음란행위 영상 또는 사진을 확보한 후, 지인의 SNS계정에 유포한다고 협박하는 수법이 발생하고 있다.[43]

③ 몸캠피싱 상담 및 조언으로 접근하는 수법 : 뿐만 아니라, 몸캠피싱 피해자가 조언이나 상담을 구하기 위해 커뮤니티에 방문하면 '대응법을 알려주겠다.' 또는 '몸캠피싱 대응업체 직원이다." 등으로 본인도 피해자라고 기망하며 접근하여 상담을 핑계로 협박법에게 보낸 영상과 사진을 전달받고, 이를 이용해 협박을 하는 피해자의 간절함을 이용한 수법도 발생하고 있다.[44]

---

41) 몸캠피싱이란, "스카이프 또는 텔레그램 등의 SNS를 통해 음란 화상 채팅을 하자고 접근하여 상대방의 음란 행위를 녹화 및 *apk 파일 설치를 요구하고, 피해자 휴대폰에 악성코드를 심어 피해자 지인의 연락처를 탈취한 다음 해당 영상을 지인들에게 유포한다고 협박하면서 금전을 갈취하는 범죄"이다. 경찰청 사이버안전국 홈페이지, https://www.cyber.go.kr/prevention/prevention10.jsp?mid=020310 (최종검색일 : 2023. 08. 20.) 참조.

42) 정대용, "범죄 스크립트 분석을 활용한 몸캠피싱 범죄수법 분석", 경찰학연구 제21권 제3호, 2021, 20면 참조.

43) 뉴스웍스, "[성년의 날⑭] 피해자 10명 중 4명 '20대'…청년 노리는 '몸캠피싱' 피하려면", 2023. 05.14. https://www.newsworks.co.kr/news/articleView.html?idxno=711610 (최종검색일 : 2023. 08. 20.) 참조.

44) 뉴스웍스, "[성년의 날⑭] 피해자 10명 중 4명 '20대'…청년 노리는 '몸캠피싱' 피하려면", 2023. 05.14. https://www.newsworks.co.kr/news/articleView.html?idxno=711610 (최종검색일 : 2023. 08. 20.) 참조.

7) 딥페이크 피싱

인공지능 AI 기술 개발을 통해 딥페이크와 같은 최신 기술을 활용하는 피싱 범죄도 다수 발생할 수 있을 것이라 예상된다. 아직 국내에서는 딥페이크 피싱이 발생하지는 않았으나, 해외에서는 딥페이크를 활용한 피싱 범죄가 발생한 사례가 보도되고 있다.

이미 2021년 아랍에미리트에서는 은행 임원의 전화를 받고 3500만달러를 송금했으나, 전화 상대방은 은행 임원이 아닌, 딥보이스로 만들어진 목소리였고,[45] 캐나다에서도 손자의 목소리를 복제하여 '교통사고로 유치장에 있고, 보석금이 필요하다'고 기망하여 900만 원을 송금할 뻔한 사건이 발생했다.[46]

8) 로맨스 스캠[47][48]

최근에는 30대 이하 여성을 노리는 로맨스 스캠 수법의 피해가 크게 접수되고 있다. 코로나19로 인하여 전세계적으로 비대면 문화가 보편화되어 사람들에 대한 만남도 대부분 비대면으로 이루어짐을 바탕으로 활발해지기 시작했고, 다른 사람의 사진을 도용해 영국 사업가, 특수 훈련을 받은 비행사, 국제 의료 봉사자 등을 사칭하며 SNS로 외모나 재력 등을 과시하며 여성에게 접근하는 로맨스 스캠 사기단까지 생기기도 했으며, 이후 친분이 쌓이면 통관비, 여권 구입비, 생활비 등을 목적으로 금전을 편취한다.[49]

이 유형은 파병 군인, 재력가 외국인을 사칭해 수수료, 관세, 수술비를 내달라고

---

45) 머니투데이, "[단독] "목소리 소름주의"...400억 가로챈 '딥보이스 범죄' 檢도 나섰다.", 2023. 02. 11. https://news.mt.co.kr/mtview.php?no=2023020913433930492 (최종검색일 : 2023. 08. 20.) 참조.

46) 중앙일보, ""보증금 도와줘"영통까지 한 친구···'딥보이스'피싱에 당했다", 2023.06.18. https://www.joongang.co.kr/article/25170581#home (최종검색일 : 2023. 08. 20.) 참조.

47) 로맨스(romance)와 신용사기를 의미하는 스캠(scam)의 합성어이다. SNS를 통해 접근해서 호감을 표시하고 재력과 외모 등으로 피해자와 신뢰관계를 형성한 뒤, 각종 이유로 금전을 요구하는 수법이다. 김효신·서준배, "로맨스 스캠(Romance Scam) 범죄 현황 및 대응방안에 대한 고찰", 경찰한논총 제14권 제3호, 2019, 120면 참조.

48) 로맨스 스캠의 주요 수법을 살펴보자면, 1) 사회적 신분과 경제력을 과시하면서 급속한 관계로 발전하는 것을 바탕으로 2) 상대방에 대한 과도한 질문공세로 정보를 수집하고 3) 본인의 신분은 비노출하면서 4) 긴급한 상황을 이유로 피해자에게 금전을 요구한다. 정태진, "팬데믹시대 증가하는 로맨스스캠과 몸캠피싱 : 국내외 동향 및 대응방안", 한국경찰연구 제20권 제4호, 2021,317-318면 참조.

49) KBS뉴스, ""넬 사랑해, 병원비 좀"···달콤한 사기 '로맨스 스캠' 기승", 2022.12.18. https://news.kbs.co.kr/news/view.do?ncd=5628560 (최종검색일 : 2023.08.12.) 참조.

요청하는 가장 전형적인 방식인 ① 비용대납형, 해외에 살고 있다고 속이며 현금으로 포인트를 충전한 사이트에서 며칠 내 환전을 하지 않는 경우 모두 소멸하기 때문에 돈을 대신 입금받아 보내달라는 방식인 ② 환전사기, 본인이 가상화폐로 많은 수익을 내고 있으니 같이 투자하자고 유도하는 ③ 코인투자형 유형으로 나누어 볼 수 있다.[50]

SNS를 활발하게 사용하는 젊은 세대의 경우, 대면으로 만나지 않아도 기망당하기 쉽고, 온라인 상에서 대인관계를 형성하는 경우도 많기 때문에 생각보다 분별력이 흐릿해진다. SNS에서 직업 등을 사칭한 남성과 사귀고 있다고 믿고 있는 피해자는 '한국에 들어가서 결혼을 하고 싶은데, 현재 환전 사이트에 돈이 묶여 있다. 여성만 가입이 가능한 환전 사이트인데, 대신 가입해서 약간의 수수료를 내고 묶여 있는 돈을 대신 찾아주라'라는 수상한 말을 믿고 부탁을 들어주는 경우가 발생하는 것이다.[51]

피해자가 SNS로만 대화하는 것에 대해 의심하며 직접 음성통화나 영상통화를 요구하면 핑계를 대거나 거절하면서 피해자가 이상함을 감지하고 신고를 할 수 있었던 초창기와는 다르게, 최근에는 딥페이크 기술과 결합하여 합성된 영상을 편집해서 영상통화를 하는 등으로 진화하여 사기 수법은 더욱 교묘해지고 있다.[52]

3. 피해금 편취 방법의 유형

가. 계좌이체형

1) 계좌이체형 편취 방법

정보기술(IT)이 발달한 한국은 다른 나라들에 비해 첨단 기술을 활용한 피싱범죄에 쉽게 노출되어 있고, 많은 사람들이 편리한 금융기술을 사용하는 만큼 신종 피싱범죄에 노출될 위험도 그만큼 크다고 볼 수 있다.[53]

---

50) 연합뉴스, "'로맨스 스캠' 피해자 70%가 여성···30대 이하가 87%", 2023.05.28. https://www.yna.co.kr/view/AKR20230527033000004 (최종검색일 : 2023. 08 12.) 참조.
51) 서울남부지방법원 주희양 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.
52) KBS뉴스, ""넬 사랑해, 병원비 좀"···달콤한 사기 '로맨스 스캠' 기승", 2022.12.18. https://news.kbs.co.kr/news/view.do?ncd=5628560 (최종검색일 : 2023.08.12.) 참조.
53) 최관·김민지, "한국 보이스피싱 범죄의 진행과정에 관한 연구", 경찰학연구 제15권 제3호, 2015, 234-235면 참조.

가장 일반적으로는 피해자를 기망하여 미리 준비해둔 대포통장으로 금원을 송금 및 이체하도록 하는 수법을 사용하였고, 귀금속 또는 숙박업체 등 물품 판매자의 계좌로 송금하도록 한 뒤, 물품을 받거나 환불조치로 현금화를 하는 등의 수법까지 변화하며 다른 국가보다 3-4년 정도 범죄수법이 진화하는 모습을 보이고 있다.[54]

정상계좌를 이용한 피싱사기의 유형은 다음과 같이 두 개의 유형으로 구분할 수 있다.

① 상품권 판매처 경유 : 사용자 PC를 악성코드로 감염시켜 입력하는 개인금융거래 정보를 편취 → 편취한 개인정보로 E-mail계정 생성 후 상품권 판매처에서 상품권을 구매 → 구매대금은 피해자 금융정보를 이용하여 인터넷뱅킹으로 지급[55]

② 숙박업체 경유 : 인터넷 메신저를 통해 회사 동료를 사칭하여 금전 송금 요청 메시지 발송 → 피해자가 메신저로 보내온 계좌(홍콩 한인민박 계좌)로 금원 송금 → 사기범은 숙박을 취소하고 달러로 반환요청[56]

2) 대포통장 모집 수법 변화

보이스피싱범죄에서 피해금을 편취 후, 범죄수익금으로 보관·이동하는 매체가 되는 대포통장의 역할은 굉장히 크다. 이에 대포통장을 근절하기 위해 "전자식카드 등 접근매체를 양도, 양수, 부정 대여 또는 질권 설정행위를 하거나 이런 행위들을 알선하는 행위를 금지하고, 이를 위반한 경우 처벌"[57]하기 위해 2008년 12월 31일 전자금융거래법이 일부개정되었다. 그 결과 대포통장을 모집하기 어려워지면서 조직원들은 대포통장 모집에 있어서도 새로운 수법을 활용하기 시작했다.

대포통장을 모집하는 모집책이 따로 있을 정도로 대포통장은 보이스피싱 완성의

---

54) 최관·김민지, "한국 보이스피싱 범죄의 진행과정에 관한 연구", 경찰학연구 제15권 제3호, 2015, 235면 참조.

55) 금융감독원 보도자료, "대포통장이 아닌 정상계좌를 이용한 피싱사기 주의", 2013.07.16. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=10155&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=17 (최종검색일: 2023. 6. 27.) 참조.

56) 금융감독원 보도자료, "대포통장이 아닌 정상계좌를 이용한 피싱사기 주의", 2013.07.16. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=10155&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=17 (최종검색일: 2023. 6. 27.) 참조.

57) 국가법령정보센터, 전자금융거래법 전체 제정·개정이유, https://www.law.go.kr/LSW/lsRvsRsnListP.do?lsId=010199&chrClsCd=010202&lsRvsGubun=all (최종검색일 : 2023. 8. 16.) 참조.

핵심이라고 할 수 있다. 가장 일반적으로는 노숙자 명의로 대포통장을 개설하거나, 급전이 필요한 사람에게 대출업체 직원을 사칭하여 거래실적을 만들기 위해 체크카드 또는 통장을 보내줄 것을 요구하는 등의 방법으로 기망하여 체크카드와 비밀번호를 확보 후 해당 계좌로 보이스피싱 피해금을 이체 받는다.[58]

대출피싱문자를 무작위로 발송하여 대출을 받고자 연락하는 사람들을 대상으로 '대출을 해주기 위해서는 원금회수용 통장과 카드가 필요하다.' 또는 '고금리 대출이기 때문에 불법대출이라고 신고할 우려가 있어 담보용으로 통장을 받는 것이다.'라는 핑계로 계좌를 확보한다.[59] 또는 유령회사를 만들어서 법인 명의로 수 개의 통장을 확보하기도 한다.[60]

이미 금융정보를 다 파악하고 있는 조직원이 피해자에게 전화를 걸어 피해자의 실제 금융거래내역 등을 안내하면서 "지점 실적을 채우기 위해 체크카드를 주면 통장 거래실적을 만들어줄 수 있고, 그러면 3천만 원 정도 대출이 가능하다"라는 제안을 하며, 피해자도 금융정보를 다 알고 있는 조직원이 진짜 은행직원이라고 믿고 체크카드를 넘기게 되는 것이다.[61]

나. 대면편취형

1) 대면편취형 유형의 등장

주요 계좌이체 유형으로 이루어졌던 피싱 범죄에 대한 대응책으로 '지연인출제도'[62]와 '계좌 인출한도 축소'[63], '신규계좌 개설 절차 강화' 등을 시행했고, 그 결과

---

58) 하담미, "전자금융거래법상 접근매체 대여에 있어 '대가'의 의미 고찰 - 최근 판례들을 중심으로 -", 일감법학 제46권, 2020, 106면 참조.
59) 서울동부지방법원 이은미 변호사, 2023.08.14., 보이스피싱 범죄 유형 관련 인터뷰 참조.
60) 인천지방법원 김도윤 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.
61) 서울남부지방법원 주희양 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.
62) 금융감독원 보도자료, ''12.6.26일(화)부터 「지연인출제도」 시행", 2012.06.11. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=9245&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EC%A7%80%EC%97%B0%EC%9D%B8%EC%B6%9C%EC%A0%9C%EB%8F%84&pageIndex=1 (최종검색일 : 2023. 08. 05.) 참조.
63) 금융감독원 보도자료, "해외 주요국의 금융사기 피해실태-대응조치 및 시사점", 2015.06.11. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=11681&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%95%B4%EC%99%B8+%EC%A3%BC%EC%9A%94%EA%B5%AD%EC%9D%98+%EA%B8%88%EC%9C%B5%EC%82%AC%EA%B8%B0&pageIndex=1 (최종검색일 : 2023. 05. 05.) 참조.

계좌송금 대신 직접 피싱자금을 인출 및 수거하는 '대면편취형' 유형이 다수 발생하게 되었다.

대면편취형으로 피해금을 편취할 경우, 피해자가 직접 본인의 돈을 인출하여 이체를 하기 때문에 금융 정책적 수단을 적용하기가 어렵고, 인출 한도 제한이 있어도 본인이 직접 한도를 조정할 수 있기 때문에 실효성이 약하다고 할 수 있어 대면편취형 수법은 많이 사용되었다.[64]

2) 대면편취형 수법

① 정치자금 운반 : 60대 이상의 노인을 대상으로 한 범죄수법으로 정치자금 또는 정부의 지하자금을 옮기는 일이고, 지하 경제를 양지화시키기 위해서는 필요한 업무라고 기망하며, 정치협회 또는 대한민국 정부 마크가 박힌 명함이나 상장 등을 보여주며 믿을 수 밖에 없게 만드는 수법이다.[65]

② 정부기관 및 금융회사 사칭 : 검찰, 경찰 금감원 등의 정부기관을 사칭하여 "범죄에 연루되었으며, 본인 계좌에 남아있는 잔액을 안전하게 보관하는게 필요하다."고 기망하여 현금으로 전달하도록 유도하는 방법과 금융회사를 사칭하여 "저금리 대환대출을 해줄테니 기존 대출금은 우리가 보내는 금융회사 직원에게 직접 현금으로 상환하라"고 기망하여 수거책을 보내 현금을 대면편취하는 방법이다.[66]

③ 물품보관함 이용 : 보이스피싱으로 피해자를 기망하여 지하철 등에 있는 물품보관함에 금전을 넣어두도록 유도하고, 이후 수거책을 시켜 금전을 회수하도록 지시하는 방법이다. 물품보관함의 경우 "무인으로 이용할 수 있으며, 보관할 때 설정한 비밀번호를 누르기만 하면 보관해 둔 물품을 바로 수령"할 수 있기 때문에 이러한 특성을 이용하여 꾸준히 이용되고 있다.[67]

---

64) 최형욱·이상진, "피싱 범죄의 현황과 대응 방안 모색", 치안정책연구 통권 60호, 2022, 114-115면 참조.

65) 서울남부지방법원 주희양 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.

66) 금융감독원 보도자료, "9.1.[목]부터 대면편취형 보이스피싱 피해예방 활동이 강화됩니다.", 2022. 08.25. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=56670&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=2 (최종검색일 : 2023. 07. 08.) 참조.

4. 피해자 기망 수법의 유형

가. 대출빙자형(대출사기형)

2017년도부터 2018년도에는 대출금리 인상으로 경제상황이 악화 되면서, 이를 악용한 조직원들은 대출이 필요한 사람들에게 대환대출을 미끼로 하는 대출빙자형 사기 수법을 특히 교묘하게 사용했으며, 대부분 은행, 캐피탈 등 금융기관을 사칭해 “고금리대출을 받으면 저금리대출로 바꿔주겠다.”라는 명목으로 대출금을 편취하는 신종 수법을 사용하였고, 대출빙자형 형태는 경제활동이 활발한 40·50대 남성 피해자가 가장 많이 발생한 것으로 확인했다.[68][69] 금감원에서 참고자료로 공개한 대출빙자형 보이스피싱 사례를 살펴보면 아래와 같다.

① 정부지원 서민대출[70] : 햇살론 등 정부지원 서민대출 상품을 알선으로 기망하고, 신용보증서 발급을 위한 발급비용 등의 명목으로 돈을 편취하거나, “서민지원대출을 받기 위해서는 이미 사용하고 있는 고금리 대출을 상환해야 한다.”라고 속여 상환자금을 편취하는 수법

② 고금리대출을 저금리대출로 대환대출[71] : 금융기관을 사칭하여 피해자가 이용하는 제2금융권, 대부업체 등의 고금리대출을 저금리대출로 대환해 준다고 기망하여 고금리대출 상환을 명목으로 금원을 편취하는 수법

③ 신용등급 상향조정비, 대출작업비[72] : 대출을 받기 위해서는 신용등급 상향이

---

67) 아주경제, “지하철 물품보관함, 보이스 피싱 장소로 전락?...교통공사 주의 당부”, 2022.02.15. https://www.ajunews.com/view/20220215164829682 (최종검색일 : 2023.08.30.) 참조.

68) 이기수, “최근 보이스피싱의 범죄수법 동향과 법적 대응방안”, 범죄수사학연구 제4권 제2호, 2018, 7-9면 참조.

69) 금융감독원 보도자료, "대출빙자형 보이스피싱에 주의하세요, 2016.08.31. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=12745&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=14 (최종검색일 : 2023. 07. 01.) 참조.

70) 금융감독원 보도자료, "대출빙자형 보이스피싱 사기범 목소리 최신사례 공개", 2016.09.12. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=12775&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=13 (최종검색일 : 2023. 07. 01.) 참조.

71) 위의 금융감독원 보도자료 참조.

72) 위의 금융감독원 보도자료 참조.

필요하고 이를 위한 작업 등이 필요하다고 기망하는 수법으로 초기에는 작업비용으로 소액을 송금받았으나 이후 “실제로 고금리대출을 받게하고, 신용등급 상향조정 특별상환 등을 이유로 대출금을 모두 대포통장으로 송금”받는 수법으로 변화

④ ARS를 이용하여 무작위로 피해자 물색 : ARS로 불특정 다수에게 연락 후 정부지원대출을 중개하고, 안내를 신청하면 조직원이 연락하여 ‘보증서 발급비용, 대환대출자금’ 등을 편취하는 수법

정부기관 사칭 보이스피싱에 대한 홍보와 예방대책 등이 시행되면서 관련 범죄에 대한 국민들의 대처능력이 높아졌으며, 결과적으로 피싱조직은 정부기관 사칭수법 대신 급전이 필요한 서민들을 공략하여 대출빙자형 수법을 더 많이 활용하게 되었다.[73]

나. 기관사칭형

1) 보상제공형(이익제공빙자형)

주로 국민건강보험공단, 의료보험관리공단, 국세청 등을 사칭해 초과납부한 세금 또는 연금, 보험금 등을 환급해준다거나 경품 당첨 등[74]을 미끼로 사람들의 심리를 교묘하게 이용하고, 피해자가 “ATM기에 카드를 넣고 불러주는 코드를 입력하여 범행계좌로 이체하도록 하며, 피해자는 환급을 받는다고 생각하고 의심없이 지시에 따르게 되는 수법”이다.[75]

초기에는 주로 노년층을 중심으로 피해가 발생했으나, 점점 연령대와 무관하게 발생하는 추세이며, 특정 기관을 사칭하는 수법이 많이 알려지면 또 다른 기관을 사칭하는 방법으로 변화하고 있다.[76]

---

73) 금융감독원 보도자료, "대출빙자형 보이스피싱에 주의하세요, 2016.08.31. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=12745&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=14 (최종검색일 : 2023. 07. 01.) 참조.

74) 김성언·양영진, "전화 금융사기 범죄의 진화", 한국공안행정학회보 제17권 제3호, 2008, 121면 참조.

75) 최관·김민지, "한국 보이스피싱 범죄의 진행과정에 관한 연구", 경찰학연구 제15권 제3호, 2015, 248면 참조.

코로나19 이후에는 정부에서 다양한 지원 정책을 실시하는 것을 이용한 피싱 범죄도 발생했다. 조직원은 '정부긴급재난 지원 대출 안내'를 빙자하여 문자를 보내고, '선착순 지급', '한도 소진 임박' 등의 표현으로 "긴급한 자금이 필요한 소상공인과 영세사업자의 불안한 심리를 악용하는 경우"도 다수 발생했다.[77]

2) 보호형(피해방지빙자형)

보이스피싱 범죄에서 일반적으로 사용되는 수법으로 금융기관, 검찰을 중심으로 경찰, 국세청, 법원 등을 사칭[78]하며, 공공기관 또는 수사기관을 접한 경험이 별로 없는 젊은 여성들과 속기 쉬운 노년층이 범행 대상으로 노출될 위험이 많다.[79] 대체로 '범죄에 연루된 피해자를 보호' 또는 금융정보가 유출되어 '카드대금 연체 등 손해를 막고 금융정보 보안 강화를 위함'이라고 기망하며 개인정보 또는 금전이체를 요구하는 수법이 주로 사용된다.[80]

보호형의 경우, 피해자가 자신이 돈을 보낸다는 사실에 대해 인식하지 못하는 경우(처분행위의 결과를 인식하지 못함)에 해당하여 사기죄로 처벌하기 어려웠으나, "피기망자가 자신의 작위 또는 부작위에 따른 결과까지 인식하여야 처분의사를 인정할 수 있는 것은 아니다."[81]라고 판시한 2017년 대법원 전원합의체 판결에 따라 "착오라는 하자 있는 의사 상태에서 처분결과까지 인식하지 않더라도 처분의사를 인정하여 사기죄로 처벌이 가능"[82]하게 되었다.[83]

---

76) 곽대경, "보이스피싱의 실태와 대책에 관한 연구", 형사사법연구 제1권 제1호, 2011, 45면 참조.
77) 금융감독원 보도자료, "코로나19 정부지원대출 빙자 보이스피싱, 스미싱 주의", 2020.04.29. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=15709&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=5 (최종검색일 : 2023. 07. 08.) 참조.
78) 윤해성·곽대경, "보이스피싱의 예방과 대책마련을 위한 연구", 한국형사정책연구원, 2009, 21-22면 참조.
79) 이기수, "최근 보이스피싱의 범죄수법 동향과 법적 대응방안", 범죄수사학연구 제4권 제2호, 2018, 11면 참조.
80) 윤해성·곽대경, "보이스피싱의 예방과 대책마련을 위한 연구", 한국형사정책연구원, 2009, 22-27면 참조.
81) 대법원 2017. 2. 16. 선고. 2016도13362 전원합의체 판결 참조.
82) 대법원 2017. 2. 16. 선고. 2016도13362 전원합의체 판결 참조.
83) 윤해성·김유근, "보이스피싱 피해유형별 구체적 예방방안에 관한 연구", 대검찰청 연구용역보고서, 2017, 22-29면 참조.

3) 신용카드 연체 명의도용 빙자형

신용카드사 직원을 사칭하여 ① 소지하고 있는 은행카드로 소비한 비용이 연체되었다는 안내와 상담을 유도, ② 상담자가 연체 금액을 입금하라고 안내, ③ 해당 카드를 사용한 사실이 없다라고 대답하면, 카드가 도용당한 것 같아 경찰에 신고해 준다고 하며 통화를 종료, ④ 이후 경찰 수사관을 사칭한 다른 사기범이 전화하여, 신분확인 목적으로 이름, 주민번호, 휴대폰번호 확인 및 금감원 전화가 올 것이라고 안내, ⑤ 금감원 직원 사칭한 사기범이 "카드사에서 다른 계좌의 예금을 인출할 수 있어 '보안코드'를 설정해야한다고 현금지급기 조작 유인 및 예금을 이체 받아 편취하는 절차로 범행이 진행된다.[84][85]

다. 지인사칭형

가족 또는 지인을 사칭해 피해자에게 접근한 후 금전을 편취하는 수법으로 그 중에서도 자녀를 사칭하는 경우가 많고, 보이스피싱 뿐만 아니라 메신저피싱에서도 많이 발생한다. 초창기에는 "카카오톡으로 지인의 이름과 SNS프로필 사진을 도용하여 휴대폰 고장 등을 이유로 수리 비용을 요구하거나, 통화를 회피하며 긴급한 사유로 계좌송금을 요청"하는 방법이 주로 사용된 수법이었다.[86]

지인사칭형 메신저 피싱은 코로나19이후 비대면 문화를 이용해 더 활발하게 발생했다. "액정파손 등으로 휴대전화 사용이 어려워 PC로 카카오톡을 보낸다고 하면서 접근하여, '선배에게 빌린 돈을 상환해야 한다.', '대출금을 상환해야 한다.', '친구 사정으로 대신 입금해줘야 한다.' 등의 긴급한 상황을 연출" 하는 기본적인 수법 뿐만 아니라, "문화상품권 구매 후에 핀번호를 전송해달라고 하거나, 스마트폰에 원격제어 어플을 설치하도록 유도하여 개인정보 탈취 및 온라인 결제로 금전을 편취하거나, 신용카드 사진과 비밀번호 전송을 요구"하는 등의 수법이 새롭게 발생했다.[87]

---

84) 윤해성·곽대경, "보이스피싱의 예방과 대책마련을 위한 연구", 한국형사정책연구원, 2009, 23-24면 참조.
85) 강구민·윤해성, "보이스피싱 범죄에 대한 쟁점과 대책", 성신법학 제9호, 2010, 10면 참조.
86) 금융감독원 보도자료, "지인을 사칭한 메신저피싱 주의 당부", 2018.12.18. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=14721&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=7 (최종검색일 : 2023. 07. 06.) 참조.

라. 의무부과형

단순히 기관을 사칭하거나 지인을 사칭하는 유형에서 그치지 않고, 해당 수법이 홍보로 많이 알려진 이후에는 새로운 수법으로 의무부과형 수법이 등장하게 되었다. 동창회 또는 종친회의 명부를 입수하여 회비송금을 요구하는 경우 지인사칭형이면서 의무부과형 유형이 될 수 있으며, 택배회사나 우체국을 사칭하며 '우편물이 계속 반송되어 개인정보가 필요하다'라고 기망하며 개인정보를 요구하는 경우는 기관사칭형이면서 의무부과형 유형이 될 수 있다.[88]

이외에도 '대학교 추가합격 등록금 납부' 등으로 피해자를 기망하고, 직접 돈을 이체하도록 유도하는 수법도 종종 발생했다.[89]

마. 공갈·협박형

가장 많이 발생하는 공갈·협박형 수법에는 '자녀를 납치하여 데리고 있으니 돈을 송금하라' 또는 '아들이 도박 빚으로 납치됐으니 돈을 송금하라'[90]고 요구하는 방법을 가장 많이 사용하며, 피해자에게 자녀가 있는지에 대한 부분 등의 구체적인 개인정보를 사전에 입수하여 특정 피해자에게 연락해서 금원을 편취하는 수법이다.[91]

'가족에게 채무가 있어 강제집행을 하겠다.'라는 협박을 하는 등을 피해자의 심리적 두려움을 이용한 방법으로 악질적인 범죄이다.[92] 또한, 피해자에게 절박한 상황을 연출하며 판단력을 흐리게 하고, 심리적으로 압박을 가해 성공률이 높을 수 밖에 없다.[93] 이외에도 가족이나 먼 친척을 위장하여 급전이 필요하다는 부탁으로 송금을

---

87) 금융감독원 보도자료, "가족 또는 지인 사칭해 개인정보와 돈을 요구하는 메신저 피싱 근절 위해 관계기관 힘 모아", 2020.06.24. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=15800&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=5 (최종검색일 : 2023. 07. 08.) 참조.

88) 윤해성·김유근, "보이스피싱 피해유형별 구체적 예방방안에 관한 연구", 대검찰청 연구용역보고서, 2017, 16-21면 참조.

89) 윤해성·김유근, "보이스피싱 피해유형별 구체적 예방방안에 관한 연구", 대검찰청 연구용역보고서, 2017, 25면 참조.

90) 곽대경, "보이스피싱의 실태와 대책에 관한 연구", 형사사법연구 제1권 제1호, 2011, 14면 참조.

91) 김성언·양영진, "전화 금융사기 범죄의 진화", 한국공안행정학회보 제17권 제3호, 2008, 121-122면 참조.

92) 강구민·윤해성, "보이스피싱 범죄에 대한 쟁점과 대책", 성신법학 제9호, 2010, 10면 참조.

93) 장주성, "금융소비자 보호를 위한 보이스피싱 대응방안 연구", 금융감독연구 제9권 제1호, 202

유도하는 방법을 사용하기도 한다.[94]

[표 2-3] 보이스피싱 범죄 유형

구분		사칭기관	수법
불특정다수대상	보호형	경찰, 검찰, 법원	범죄 사건 연루조사, 개인정보 유출 등
		은행, 카드사, 금융감독원	-카드대금, 금융거래정보 유출
		우체국	우편물, 택배, 카드반송 등
	보상제공형	건강보험공단, 연금공단, 국세청	연금, 보험료, 세금환급 등
		통신회사	전화요금 환급 등
	피싱사이트형	공공기관, 은행 등	-정보유출 등
특정인대상	협박형	폭력조직	자녀납치, 가족상해 협박 등
	지인사칭형	가족, 친구, 직장동료 등	급전요구, 합의금 등
	의무부과형	동창회, 대학교 등	-회비요구, 대학추가합격 등록금 납부 등

출처: 최관·김민지, "한국 보이스피싱 범죄의 진행과정에 관한 연구", 경찰학연구 제15권 제3호, 2015 참조.

제2절 | 보이스피싱 발생추세 및 특성

보이스피싱 발생추세는 경찰의 통계자료를 중심으로 살펴볼 수 있다. 경찰 통계자료를 통해서 보이스피싱 발생추세 및 편취수법, 피해금액과 더불어 피의자·피해자 특성 등에 대해 파악해볼 수 있다. 한편 금융감독원에서는 「전기통신금융사기피해방지 및 피해금환급에 관한 특별법」에 따라 피해구제신청접수(1차 계좌)된 것을 기준으로 보이스피싱 통계자료를 발표하고 있다. 금융감독원의 통계에서는 동법의 적용을 받지 않는 사례가 제외되지만, 은행권역별 피해금액 등 경찰통계에서 파악할 수 없는 내용이 포함되어 있다. 따라서 여기서는 경찰과 금융감독원의 통계자료를 중심으로 보이스피싱 발생추세 및 특성에 대해 파악해보고자 한다.

2, 129면 참조.

94) 한국인터넷 진흥원 보도자료(2007.8)을 인용한 곽대경, "보이스피싱의 실태와 대책에 관한 연구", 형사사법연구 제1권 제1호, 2011, 15면 참조.

1. 경찰통계

가. 유형별 발생현황

보이스피싱범죄의 발생현황은 경찰통계자료를 통하여 파악해 볼 수 있다. 보이스피싱 발생건수는 2018년 34,132건에서 2019년에 3천 건 이상 증가하였으나 이후 감소하는 경향을 보여서 2022년에는 21,832건에 이르고 있다.[95] 보이스피싱 검거건수 및 검거인원 역시 발생건수와 유사한 경향을 보여서 2018년에서 2019년 증가하였으나 이후 감소하는 것으로 나타났다. 보이스피싱 피해액을 보면, 2018년 4,041억원에서 2021년까지 지속적으로 증가하여 7,744억원까지 증가하였다. 이후 2022년에는 큰 폭으로 감소하여서 5,438억원이었다. 다만 2022년도의 피해액은 2018년에 비해서 많다는 것을 알 수 있다.

경찰에서는 보이스피싱 유형을 크게 기관사칭형과 대출사기형으로 구분하여 통계를 내고 있다. 보이스피싱 유형별 발생현황을 보면, 기관사칭형의 경우 2018년 6,221건에서 대체로 증가하는 경향을 보여서(2021년 제외) 2022년에는 8,930건까지 증가하였다. 2023년 4월까지의 발생건수도 3,553건으로 나타나서 발생건수 증가현상이 이어질 가능성이 있다. 기관사칭형 피액액을 보면, 2018년 1,430억원에서 2019년 2,506억원으로 증가하였으며 이후 감소추세를 보여 2021년에 1,741억원으로 낮아졌으나 2022년에는 다시 증가하여 2,077억원에 이르고 있다. 기관사칭형 검거건수와 검거인원은 2018년 각각 4,673건, 5,491명에서 2019년에 증가하였으나 이후 2021년까지는 감소하는 경향을 보였으며 2022년에는 다시 증가하여 각각 4,103건, 4,500명이었다. 대출사기형의 발생건수를 보면, 2018년 27,911건에서 2019년 30,448건으로 증가하였으나 2020년 이후 대체로 감소하는 경향을 보여서 2022년에는 12,902건에 이르고 있다. 검거건수와 검거인원 역시 발생건수와 유사하게 2018년에서 2019년에 증가하였으나 이후 감소하는 경향을 보이고 있다. 피해액을 보면, 2018년 2,610억원에서 2021년에는 6,003억원으로 증가하였으며, 2022년에는 3,361억원으로 감소하였다.

---

95) 경찰청 실무자와의 자문에 의하면, 보이스피싱 발생건수는 피해자의 신고접수를 기준으로 하고 있다. 다만 신고접수후 수사과정에서 다른 피해가 있을 수 있다고 한다. 따라서 발생건수가 피해자수와 일치하지는 않는다고 한다.

경찰통계자료를 통하여 보이스피싱 발생건수를 보면, 전체적으로 최근에 감소하는 경향을 보이고 있음을 알 수 있다. 다만 피해액의 경우 2021년까지 꾸준히 증가하였으며 2022년에 감소한 것을 보여준다. 또한 유형별로 보면, 2018년의 경우 대출사기형이 81.8%, 기관사칭형이 18.2%였으나 2022년의 경우 대출사기형과 기관사칭형이 각각 59.1%, 40.9%이었다. 즉, 보이스피싱 범죄에서 대출사기형이 여전이 많은 비율을 차지하고 있지만 그 비율은 이전에 비해 낮아진 것을 알 수 있다. 반면 기관사칭형의 경우 2018년 18.2%에서 2022년 40.9%로 두 배 이상 증가한 것을 알 수 있다. 즉 최근에 기관사칭형 보이스피싱의 비율이 증가하고 있는 것에 대해 주목할 필요가 있다.

[표 2-4] 전화금융사기 유형별 현황

구분	합 계				기관사칭형				대출사기형			
	발생 건수	피해 (억원)	검거 건수	검거 인원	발생 건수	피해 (억원)	검거 건수	검거 인원	발생 건수	피해 (억원)	검거 건수	검거 인원
2018	34,132	4,040	29,952	37,624	6,221	1,430	4,673	5,491	27,911	2,610	25,279	32,133
2019	37,667	6,398	39,278	48,713	7,219	2,506	5,487	6,045	30,448	3,892	33,791	42,668
2020	31,681	7,000	34,051	39,324	7,844	2,144	4,297	4,797	23,837	4,856	29,754	34,527
2021	30,982	7,744	27,647	26,397	7,017	1,741	1,954	1,895	23,965	6,003	25,693	24,502
2022	21,832	5,438	24,522	25,030	8,930	2,077	4,103	4,500	12,902	3,361	20,419	20,530
2023 (~4월)	5,747	1,291	5,206	5,375	3,553	682	1,588	1,688	2,194	609	3,618	3,687

출처: 경찰청 내부자료

나. 편취수법별 현황

보이스피싱의 편취수법별 현황을 살펴보면 아래의 표와 같다. 편취수법 중 계좌이체의 비율은 2018년 89.7%에서 2019년 81.0%로 낮아졌으며, 그 이후 큰 폭으로 감소하여서 2022년에는 9.9%까지 낮아졌다. 2023년 4월까지의 자료를 보면, 2023년에는 다시 증가하여서 17.5%에 이르고 있다. 대면편취의 비율은 2018년 7.5%에서 2021년에는 73.4%까지 증가하였으며 2022년에는 조금 감소한 64.4%를 차지하고 있다. 한편 상품권 등 요구의 비율은 2018년에는 0.3%에 불과했으나 점차 증가하여서 2022년과

2023년(~4월)의 경우 각각 21.3%, 35.0%였다.

보이스피싱 편취수법별 현황을 보면, 2018년, 2019년에는 계좌이체의 비율이 80% 대로 높은 편이었으나 2020년 이후로는 대면편취가 가장 높은 비율을 차지하고 있음을 알 수 있다. 또한 상품권 등 요구의 비율이 최근에 증가하여서 2021년 이후로는 대면편취에 이어 두 번째로 높은 비율을 차지하고 있다. 참고로 절도의 경우는 피해자가 인출한 현금을 물품보관함에 두게 하고 가져가는 경우, 피해자로 하여금 현금을 문고리 등에 걸어두게 하고 가져가는 경우 등이 해당될 수 있다.[96]

[표 2-5] 전화금융사기 편취수법별 현황

구분	합계	계좌이체	가상계좌	대면편취	특정장소 지정	절도	상품권 등 요구	배송형	피싱 혼합형
2018	34,132 (100.0)	30,611 (89.7)	362 (1.1)	2,547 (7.5)	274 (0.8)	123 (0.4)	115 (0.3)	51 (0.1)	49 (0.1)
2019	37,667 (100.0)	30,517 (81.0)	244 (0.6)	3,244 (8.6)	338 (0.9)	142 (0.4)	727 (1.9)	149 (0.4)	2,306 (6.1)
2020	31,681 (100.0)	10,596 (33.4)	226 (0.7)	15,111 (47.7)	139 (0.4)	160 (0.5)	3,582 (11.3)	276 (0.9)	1,591 (5.0)
2021	30,982 (100.0)	3,362 (10.9)	121 (0.4)	22,752 (73.4)	166 (0.5)	89 (0.3)	3,900 (12.6)	418 (1.3)	174 (0.6)
2022	21,832 (100.0)	2,161 (9.9)	170 (0.8)	14,053 (64.4)	98 (0.4)	20 (0.1)	4,641 (21.3)	431 (2.0)	258 (1.2)
2023 (~4월)	5,747 (100.0)	1,004 (17.5)	42 (0.7)	2,432 (42.3)	51 (0.9)	2 (0.0)	2,012 (35.0)	119 (2.1)	85 (1.5)

출처: 경찰청 내부자료

다. 피해금액

보이스피싱 피해금액별 현황을 보면, 2020년(2-12월)의 경우 피해금액이 1,000-2,000만원인 비율이 27.4%로 가장 높았으며, 다음은 2,000-5,000만원의 비율이 26.1%였다. 2021년 이후로는 피해금액 2,000-5,000만원이 가장 높은 비율을 차지하고 있다. 또한 피해금액대별로 각각 10-20%대 비율이 많은 것으로 나타나서 피해금액대가 다양하다는 것을 알 수 있다. 한편 피해금액이 1억원 이상인 비율도 연도에

96) 뒤의 사례에서도 피해자로 하여금 현금을 물품보관함에 두게 한 후 가져간 현금인출책이 절도로 처벌받은 사례가 제시되어 있음.

관계없이 2%대를 차지하고 있으며, 최근에 대체로 비율이 증가하는 것으로 나타났다.

[표 2-6] 전화금융사기 피해금액별 현황

구분	합계	100만원 미만	100만원~500만원	500만원~1,000만원	1,000만원~2,000만원	2,000만원~5,000만원	5,000만원~1억원	1억원 이상
2020 (2~12월)	28,884 (100.0)	2,058 (7.1)	3,034 (10.5)	5,844 (20.2)	7,916 (27.4)	7,546 (26.1)	1,837 (6.4)	649 (2.2)
2021	30,982 (100.0)	2,351 (7.6)	2,399 (7.7)	4,404 (14.2)	8,907 (28.7)	9,776 (31.6)	2,364 (7.6)	781 (2.5)
2022	21,832 (100.0)	2,567 (11.8)	2,542 (11.6)	2,705 (12.4)	5,479 (25.1)	6,146 (28.2)	1,760 (8.1)	633 (2.9)
2023 (~4월)	5,747 (100.0)	1,130 (19.7)	1,056 (18.4)	603 (10.5)	1,114 (19.4)	1,248 (21.7)	441 (7.7)	155 (2.7)

※ 경찰에서 피해금액별 현황은 '20. 2월부터 관리 중임.
출처: 경찰청 내부자료

라. 피해자 특성

보이스피싱 피해자의 특성은 피해자 성별 연령별 현황을 통해 살펴보았다. 먼저 남성의 연령별 분포를 보면 2018년의 경우 50대가 31.4%로 가장 높았으며, 다음은 40대가 29.9%, 30대가 17.5%, 60대가 12.1%, 20대 이하가 7.0% 등의 순이었다. 남성의 경우 2021년까지는 50대의 비율이 가장 높은 것으로 나타났으며, 2022년 이후로는 20대의 비율이 가장 높은 것으로 나타났다. 여성의 경우를 보면, 2018년에는 40대의 비율이 27.7%로 가장 높았으며, 다음은 50대가 22.8%, 30대가 20.6%, 20대 이하가 19.7% 등의 순이었다. 2019년 이후로는 대체로 50대가 가장 높은 비율을 차지하는 것으로 나타났다(2020년의 경우는 20대 비율이 26.2%로 가장 높음). 20대 이하의 비율은 2020년 가장 높은 것으로 나타난 것과 더불어 이후로도 50대에 이어 두 번째로 높은 비율을 차지하고 있다.

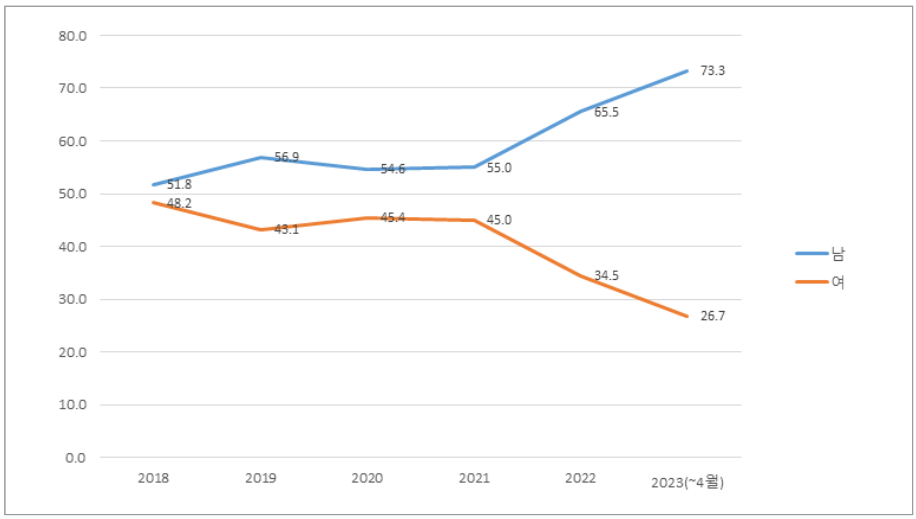
[표 2-7] 전화금융사기 피해자 성별 · 연령별 현황

구분	합계	성별	소계	20대 이하	30대	40대	50대	60대	70대 이상
2018	34,132	남성	17,673 (100.0)	1,231 (7.0)	3,094 (17.5)	5,287 (29.9)	5,557 (31.4)	2,133 (12.1)	371 (2.1)
		여성	16,459 (100.0)	3,249 (19.7)	3,389 (20.6)	4,555 (27.7)	3,756 (22.8)	1,256 (7.6)	254 (1.5)
2019	37,667	남성	21,424 (100.0)	2,040 (9.5)	3,583 (16.7)	5,576 (26.0)	6,808 (31.8)	2,816 (13.1)	601 (2.8)
		여성	16,243 (100.0)	1,815 (11.2)	2,458 (15.1)	4,688 (28.9)	5,017 (30.9)	1,801 (11.1)	464 (2.9)
2020	31,681	남성	17,293 (100.0)	1,553 (9.0)	2,800 (16.2)	4,296 (24.8)	5,541 (32.0)	2,615 (15.1)	488 (2.8)
		여성	14,388 (100.0)	3,770 (26.2)	1,606 (11.2)	3,408 (23.7)	3,676 (25.5)	1,573 (10.9)	355 (2.5)
2021	30,982	남성	17,027 (100.0)	2,083 (12.2)	2,053 (12.1)	3,605 (21.2)	5,611 (33.0)	2,976 (17.5)	699 (4.1)
		여성	13,955 (100.0)	3,376 (24.2)	1,246 (8.9)	3,150 (22.6)	3,953 (28.3)	1,802 (12.9)	428 (3.1)
2022	21,832	남성	14,308 (100.0)	5,218 (36.5)	1,197 (8.4)	1,892 (13.2)	3,229 (22.6)	2,253 (15.7)	516 (3.6)
		여성	7,524 (100.0)	1,587 (21.1)	624 (8.3)	1,521 (20.2)	2,149 (28.6)	1,209 (16.1)	437 (5.8)
2023 (~4월)	5,747	남성	4,211 (100.0)	2,344 (55.7)	356 (8.5)	347 (8.2)	575 (13.7)	449 (10.7)	140 (3.3)
		여성	1,536 (100.0)	388 (25.3)	133 (8.7)	271 (17.6)	392 (25.5)	258 (16.8)	94 (6.1)

출처: 경찰청 내부자료

보이스피싱 피해자 성별 분포를 보면, 다음의 그림과 같다(〈표 2-7〉 참조). 남성의 비율은 2018년 51.8%에서 증감을 반복하면서 2021년까지 50%대를 차지하였으며, 이후 2022년에는 65.5%, 2023년에는 73.3%로 증가하였다. 여성의 비율을 보면, 2018년 48.2%에서 증감을 반복하면서 2021년까지 40%대를 보였으며, 이후 2022년에는 34.5%, 2023년에는 26.7%로 낮아졌다. 보이스피싱 범죄 피해자 성별 분포를 보면, 2018-2021년까지는 남성과 여성이 각각 50%대, 40%대로 남성이 조금 높은 비율을 보였으나 최근에 남성의 비율이 증가하고 여성의 비율이 감소하는 경향을 보이고 있다.

[그림 2-1] 전화금융사기 피해자 성별 현황(비율)



마. 피의자 특성

보이스피싱 피의자 특성은 역할 및 연령별 분포를 통해 살펴보았다. 먼저 보이스피싱 피의자의 역할별 검거인원을 보면, 계좌명의인의 비율은 2018년에 76.9%에서 2022년까지 계속 감소하여서 2022년에는 19.4%로 낮아졌다. 이후 2023년(-4월)에는 25.2%를 차지하고 있다. 하부 조직원(대면편취책·인출책·절취책 등)의 비율은 2018년 18.9%에서 2021년까지 계속 증가하여서 2021년에는 59.8%였으며, 2022년에도 전년도와 비슷한 58.0%를 차지하였다(2023년(-4월)의 경우 52.0%). 기타(통신업자·환전책 등)의 비율은 2018년 2.7%였으나 계속 증가하여서 2022년에는 20.0%로 나타났다(2023년(-4월)의 경우 19.6%). 한편 조직 상선의 비율은 대체로 1-2%대를 보이고 있다(2023년(-4월)의 경우 3.2%).

피의자 역할별 검거인원 비율을 보면, 2018년-2020년까지는 계좌명의인의 비율이 가장 높았지만, 이후로는 하부 조직원의 비율이 가장 높은 것을 알 수 있다. 이는 앞에서 본 바와 같이 최근에 대면편취 수법이 많아지면서 현금수거책 등이 검거되는 경우가 많아졌기 때문일 것이다. 기타(통신업자 등)의 비율도 최근에 증가하고 있으며, 조직 상선의 비율은 연도에 관계없이 매우 낮았다.

[표 2-8] 전화금융사기 피의자 유형별 검거인원

구분	총 검거인원	역할별 검거 인원			
		조직 상선	하부 조직원	기타(통신업자 등)	계좌명의인
2018	37,624 (100.0)	528 (1.4)	7,128 (18.9)	1,028 (2.7)	28,940 (76.9)
2019	48,713 (100.0)	1,152 (2.4)	10,748 (22.1)	2,329 (4.8)	34,484 (70.8)
2020	39,324 (100.0)	845 (2.1)	13,813 (35.1)	3,224 (8.2)	21,442 (54.5)
2021	26,397 (100.0)	527 (2.0)	15,785 (59.8)	3,902 (14.8)	6,183 (23.4)
2022	25,030 (100.0)	657 (2.6)	14,511 (58.0)	5,016 (20.0)	4,846 (19.4)
2023(~4월)	5,375 (100.0)	171 (3.2)	2,796 (52.0)	1,054 (19.6)	1,354 (25.2)

※ 하부조직원은 대면편취책·인출책·절취책 등, 기타는 통신업자·환전책 등
출처: 경찰청 내부자료

보이스피싱 피의자 특성으로 연령별 검거인원을 살펴보았다. 경찰청 관계자에 의하면, 보이스피싱 피의자 연령별 현황은 2021년 4월부터 관리 중이다. 여기서는 가용한 자료를 중심으로 피의자 연령별 분포를 파악해보았다. 2021년(4-12월), 2022년, 2023년(-4월) 모두 20대 이하의 비율이 40%대로 가장 높은 것으로 나타났다. 다음은 30대가 연도에 관계없이 20%대를 차지하였다. 20대, 30대의 비율이 높은 것은 하부조직원이 검거되는 경우가 많은 것과 관련될 수 있을 것이다. 보이스피싱 피의자의 연령별 분포를 보면 젊은 층의 비율이 높으며, 연령이 많을수록 비율이 낮아지는 것을 알 수 있다.

[표 2-9] 연령별 전화금융사기 피의자 검거인원

구분	합계	20대 이하	30대	40대	50대	60대	70대 이상
2021 (4~12월)	22,045 (100.0)	9,149 (41.5)	4,711 (21.4)	3,777 (17.1)	3,152 (14.3)	1,133 (5.1)	123 (0.6)
2022	25,030 (100.0)	11,342 (45.3)	5,555 (22.2)	3,799 (15.2)	2,792 (11.2)	1,319 (5.3)	223 (0.9)
2023 (~4월)	5,375 (100.0)	2,473 (46)	1,276 (23.7)	815 (15.2)	502 (9.3)	255 (4.7)	54 (1.0)

※ 경찰에서 피의자 연령별 현황은 '21. 4월부터 관리 중임.
출처: 경찰청 내부자료

2. 금융감독원 통계

가. 피해현황 개관

보이스피싱 발생현황은 경찰통계를 중심으로 살펴보았다. 금융감독원의 경우 보이스피싱 통계는 사기에 의한 자금의 송금·이체인 경우에 한정하고 있다. 「전기통신금융사기피해방지 및 피해금환급에 관한 특별법」의 적용범위가 아닌 대면편취형 및 재화·용역을 가장한 사기는 포함하지 않고 있다.[97] 따라서 전체적인 보이스피싱 범죄 피해현황을 파악하기에는 한계가 있는 자료이지만 금융감독원 통계에 한정하여 대략적인 추세를 파악해 보고자 한다.

금융감독원의 경우 「전기통신금융사기피해방지 및 피해금환급에 관한 특별법」의 대상이 되는 보이스피싱 범죄피해에 대해서 피해구제신청접수(1차 계좌)를 기준으로 통계자료를 생산하고 있다. 먼저 보이스피싱 피해 현황에 대해 살펴보면 다음의 표와 같다. 피해금액을 보면 2018년의 경우 4,440억원에서 2019년 6,720억원으로 증가하였으나 2020년에는 2,353억원으로 큰 폭으로 감소하였다. 이후에도 감소추세를 보여 2022년에는 1,451억원이었다. 환급액을 보면, 2018년 1,011억원에서 2019년 1,915억원으로 증가하였으나 이후 감소추세를 보여 2022년에는 379억원이었다. 환급률의 경우 2018년 22.8%에서 2020년 48.5%까지 증가하였으나 이후 감소추세를 보여 2022년에는 26.1%였다.

금융감독원에서 집계한 보이스피싱 피해자수를 보면, 2018년 48,765명에서 2019년 50,372명으로 감소하였으며, 이후에도 꾸준히 감소추세를 보여 2022년에는 12,816명으로 낮아졌다.

앞서 살펴본 경찰통계에서 보이스피싱 발생건수 및 피해자수가 2018년에서 2019년에 증가한 이후 감소하는 경향을 보였다. 금융감독원의 자료에서도 피해자수의 경우 유사한 경향을 보이고 있다. 다만 경찰의 경우 신고된 사건 중심인 반면, 금융감독원의 경우 피해구제신청접수(1차 계좌) 기준으로 하고 있다는 점에서 통계자료를 직접적으로 비교하기는 어렵다.

---

97) 금융감독원 2023년 4월 21일 보도자료, "2022년 보이스피싱 피해현황 및 주요 특징 (https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=127319&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=&pageIndex=14, 검색일: 2023년 6월 10일).

[표 2-10] 보이스피싱 피해현황

(단위 : 억원, 명, %, %p)

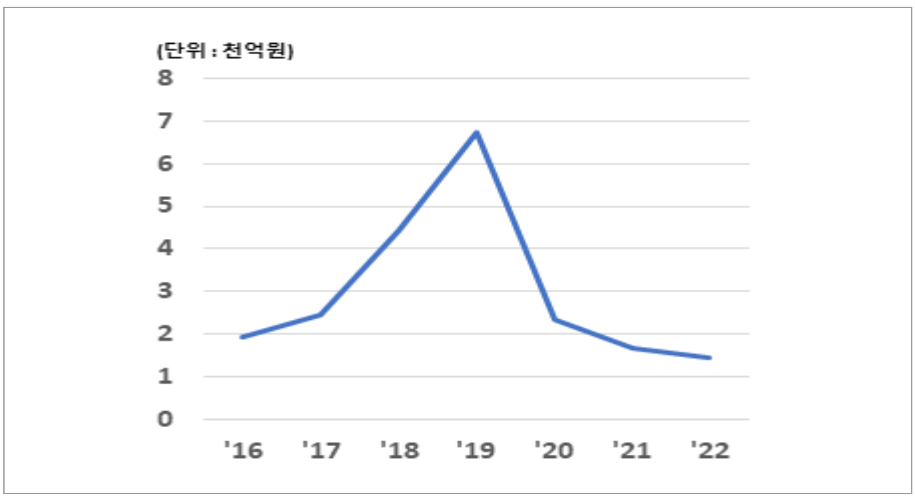
구 분	피해금액*	환급		피해자수
		환급액	환급률	
'18년	4,440	1,011	22.8	48,765
'19년	6,720	1,915	28.5	50,372
'20년	2,353	1,141	48.5	18,265
'21년	1,682	603	35.9	13,213
'22년	1,451	379	26.1	12,816
전년대비 증감(률)	(△13.7)	(△37.1)	(△9.8)	(△3.0)

* 피해구제신청접수(1차 계좌) 기준 (이하 동일)

출처: 금융감독원 2023년 4월 21일 보도자료, "2022년 보이스피싱 피해현황 및 주요 특징 (https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=127319&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=&pageIndex=14, 검색일: 2023년 6월 10일).

금융감독원 자료를 통하여 보이스피싱 전체 피해금액 추이를 보면 〈그림 2-2〉와 같다. 보이스피싱 전체 피해금액은 2016년부터 2019년까지 증가하다가 이후로는 감소하는 것으로 나타났다. 다만 이는 보이스피싱 유형 중 현금 대면편취 등이 포함되지 않았다는 한계가 있다.

[그림 2-2] 보이스피싱 전체 피해금액 추세(금융감독원 통계)

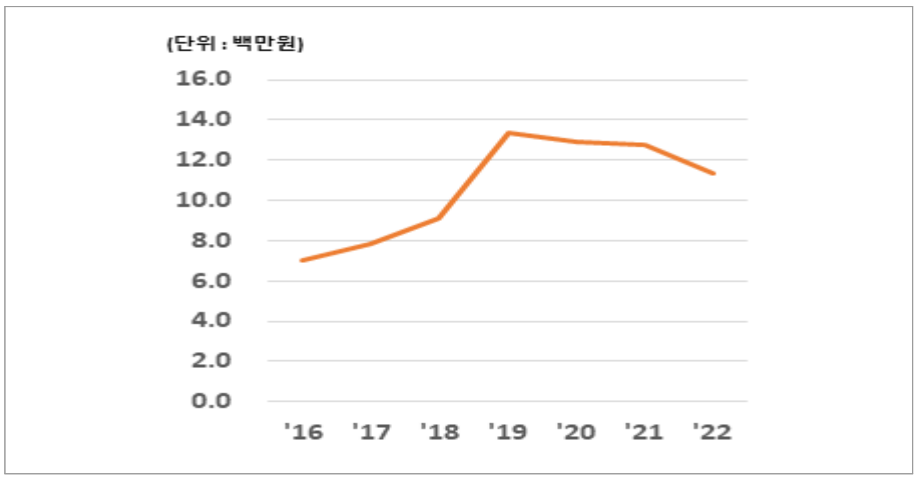


출처: 금융감독원 2023년 4월 21일 보도자료, "2022년 보이스피싱 피해현황 및 주요 특징" (https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=127319&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=&pageIndex=14, 검색일: 2023년 6월 10일).

나. 1인당 피해금액

금융감독원 통계를 통하여 1인당 피해금액을 보면, 2016년부터 2019년까지 증가하였으며, 2020년, 2021년에도 높게 유지되었고 2022년에는 조금 감소하였다. 같은 금융감독원 통계에서 보이스피싱 전체 피해금액은 2019년 이후로 크게 감소한 반면, 1인당 피해금액은 2019년 이후로도 높은 편임을 알 수 있다. 다만 앞에서도 언급했듯이 금융감독원 통계가 제한적이라는 점을 고려할 필요가 있다.

[그림 2-3] 보이스피싱 1인당 피해금액(금융감독원 통계)



출처: 금융감독원 2023년 4월 21일 보도자료, "2022년 보이스피싱 피해현황 및 주요 특징" (https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=127319&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=&pageIndex=14, 검색일: 2023년 6월 10일).

다. 보이스피싱 유형별 피해금액

보이스피싱 유형별 피해금액은 아래의 표와 같다. 금융감독원의 경우 보이스피싱 유형을 크게 대출빙자형과 사칭형으로 구분하고 있으며, 사칭형은 다시 메신저피싱과 기관사칭형으로 구분하고 있다. 2018년부터 2020년까지는 대출빙자형이 60%대, 사칭형이 30%대로 나타났다. 그러나 2021년에는 사칭형이 69.0%, 2022년에는 78.6%로 상당히 높은 것으로 나타난 반면, 대출빙자형의 경우 2021년과 2022년에 각각 31.0%, 21.4%로 낮아졌다. 사칭형을 메신저피싱과 기관사칭으로 구분해서 보면 2018년부터

2020년까지는 기관사칭형의 비율이 더 높았으나 2021년 이후로는 메신저피싱의 비율이 빠르게 증가하여 사칭형 중 상당 비율은 메신저피싱에 해당하는 것을 보여준다. 메신저, SNS 등 비대면채널 이용이 증가하면서 피해금액 중 가족이나 지인을 사칭하는 메신저피싱 비중이 증가하였다고 볼 수 있다.[98]

[표 2-11] 유형별 보이스피싱 피해금액 현황

(단위 : 억원, %, %p)

구 분	대출빙자형	사칭형*	사칭형		합 계
			메신저피싱	기관사칭	
'18년	3,093 (69.7)	1,346 (30.3)	216 (4.9)	1130 (25.5)	4,439 (100.0)
'19년	4,506 (67.1)	2,214 (32.9)	342 (5.1)	1,872 (27.9)	6,720 (100.0)
'20년	1,566 (66.6)	787 (33.4)	373 (15.9)	414 (17.6)	2,353 (100.0)
'21년(A)	521 (31.0)	1,161 (69.0)	991 (58.9)	170 (10.1)	1,682 (100.0)
'22년(B)	311 (21.4)	1,140 (78.6)	927 (63.9)	213 (14.7)	1,451 (100.0)
증감(B-A)	△210 (△9.6)	△21 (9.6)	△64 (5.0)	43 (4.6)	△231 (-)

출처: 금융감독원 2021년 4월 16일 보도자료, "'20년 중 보이스피싱 현황 분석"
(https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=16265&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EB%B3%B4%EC%9D%B4%EC%8A%A4%ED%94%BC%EC%8B%B1&pageIndex=3, 검색일: 2023년 6월 10일).
금융감독원 2021년 9월 6일 보도자료, "'21년 상반기 보이스피싱 피해 현황"
(https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=16510&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EB%B3%B4%EC%9D%B4%EC%8A%A4%ED%94%BC%EC%8B%B1+%ED%94%BC%ED%95%B4+%ED%98%84%ED%99%A9&pageIndex=1, 검색일: 2023년 6월 10일).
금융감독원 2023년 4월 21일 보도자료, "2022년 보이스피싱 피해현황 및 주요 특징"
(https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=127319&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=&pageIndex=14, 검색일: 2023년 6월 10일).

98) 금융감독원 2023년 4월 21일 보도자료.

라. 금융권역별 피해금액

금융권역별 보이스피싱 피해금액을 보면, 은행(인터넷전문은행 포함)의 비율은 2020년 74.2%에서 2021년 64.2%로 낮아졌으나 2022년에는 다시 증가하여 76.6%에 이르고 있다([표 2-12]). 비은행의 비율은 2020년 25.8%에서 2021년에 35.8%로 증가하였으나 이후 2022년에는 23.4%로 낮아졌다. 금융권역별 피해금액 현황을 보면, 은행권의 비율이 높으며, 특히 최근에 증가한 것을 보여준다. 특히 인터넷전문은행 피해금액의 비율이 2020년 2.1%에서 2021년에는 7.7%, 2022년에는 20.9%로 증가하여서 인터넷전문은행 계좌가 보이스피싱 범죄에 이용되는 것을 막기 위한 노력이 중요함을 보여준다. 비은행의 피해금액을 보면, 비증권사의 피해금액이 증권사에 비해 큰 것을 알 수 있다.

[표 2-12] 금융권역별 보이스피싱 피해금액 현황

(단위 : 억원, %, %p)

구 분	'20년	'21년(A)	'22년(B)	증감(B-A)
	금액(%)	금액(%)	금액(%)	금액(%)
은행	1,745(74.2)	1,080(64.2)	1,111(76.6)	31(12.4)
인터넷전문은행	49(2.1)	129(7.7)	304(20.9)	175(13.2)
비은행	608(25.8)	602(35.8)	340(23.4)	△262(△12.4)
증권사	90(3.8)	220(13.1)	34(2.3)	△186(△10.8)
非증권사	518(22.0)	382(22.7)	306(21.1)	△76(△1.6)
합 계	2,353(100.0)	1,682(100.0)	1,451(100.0)	△231

출처: 금융감독원 2023년 4월 21일 보도자료, "2022년 보이스피싱 피해현황 및 주요 특징" (https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=127319&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=&pageIndex=14, 검색일: 2023년 6월 10일).

마. 연령별 피해금액

금융감독원 통계자료 중 연령별 보이스피싱 피해금액 현황은 [표 2-13]과 같다. 2020년, 2021년의 경우 50대의 피해금액 비율이 각각 36.3%, 39.3%로 가장 높았으나 2022년의 경우에는 60대 이상의 비율이 46.7%로 가장 높은 것으로 나타났다. 또한 50대 이상이 차지하는 피해금액 비율은 2020년 65.7%에서 2021년, 2022년에는 각각

76.3%, 79.8%로 증가하였다. 즉 금융감독원에 피해구제신청접수가 된 피해자의 연령대별 피해금액을 보면, 50대 이상의 피해금액이 다른 연령층에 비해 크다는 것을 알 수 있다. 특히 가장 최근 통계에서는 60대 이상의 피해금액이 가장 큰 것으로 나타나서 연령층이 높은 사람들의 보이스피싱 피해 예방을 위한 노력이 중요함을 시사해준다.

[표 2-13] 연령별 보이스피싱 피해금액 현황*

(단위 : 억원, %, %p)

구 분	20대 이하	30대	40대	50대	60대 이상	합계
'20년	66 (2.8)	243 (10.5)	485 (20.9)	843 (36.3)	683 (29.4)	2,320 (100.0)
'21년(A)	52 (3.1)	121 (7.3)	219 (13.2)	650 (39.3)	612 (37.0)	1,654 (100.0)
'22년(B)	92 (6.4)	53 (3.7)	145 (10.1)	477 (33.1)	673 (46.7)	1,440 (100.0)
증감(B-A)	40 (3.3)	△68 (△3.6)	△74 (△3.1)	△173 (△6.2)	61 (9.7)	△214 (-)

* 피해구제신청접수(1차 계좌) 기준(법인 피해자 제외)

출처: 금융감독원 2023년 4월 21일 보도자료, "2022년 보이스피싱 피해현황 및 주요 특징" (https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=127319&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=&pageIndex=14, 검색일: 2023년 6월 10일).

보이스피싱 구체적 유형별 사례분석 및 진단

윤해성 · 전영실 · 이정민

제3장

보이스피싱 구체적 유형별 사례분석 및 진단

제1절 | 보이스피싱 유형별 범행단계 분석

1. 자료수집

보이스피싱 범행단계를 파악하기 위하여 2023년 6월 30일을 기준으로 법원행정처 홈페이지에 게시된 전국 법원 주요판결 중 보이스피싱 키워드를 통해 검색된 판결문을 분석대상으로 하였다. 보이스피싱의 경우 수법이 계속적으로 변화되기 때문에 비교적 최근 사례들을 살펴볼 필요가 있다. 이러한 맥락에서 본 연구에서는 2018년 이후 판결된 사례들을 분석대상으로 하였다. 여기에 해당하는 사례는 총 34건이었으며, 유사한 사례들의 경우 대표적인 하나의 사례만 제시하였다. 이와 더불어 보이스피싱은 수법이 계속 다양화되고 있다는 점을 고려하여 최근 언론보도나 관련부처 보도자료 등을 통해 나타난 새로운 사례들도 살펴보았다. 다만 언론보도나 부처 보도자료 등의 경우 판결문에 비해 범행단계 파악이 제한적일 수 있다.

보이스피싱 범행단계는 보이스피싱 유형별로 파악해 보았다. 여기서 보이스피싱 유형 구분은 경찰청과 금융감독원에서의 유형 구분을 토대로 하였다. 앞에서 살펴본 경찰통계의 경우 보이스피싱의 유형을 크게 대출사기형과 기관사칭형으로 구분하며, 금융감독원 통계의 경우 대출빙자형과 사칭형(메신저피싱+기관사칭형)으로 구분하고 있다. 참고로 금융감독원 실무자와의 자문에 의하면 메신저피싱의 경우 주로 가족이나 지인을 사칭한 경우들이라고 볼 수 있다. 이 연구에서는 보이스피싱 유형을 크게 대출사기형과 사칭형으로 구분하고, 사칭형의 경우 기관사칭형과 가족·지인사칭형으

로 구분하여 살펴보고자 한다. 금융감독원 통계에서의 유형구분과 같이 '메신저 피싱'이라고 할 경우 가족·지인사칭형과 더불어 피싱문자 등을 포함한 수사기관 사칭 사례들도 포함될 수 있기 때문이다.

이러한 유형구분에 따라 각 유형별 사례를 제시하고 범행단계를 정리해 보았다. 이 연구에서 살펴본 보이스피싱 판결문의 경우 대면편취책·현금인출책이나 콜센터 상담원 판결문이 주를 이루고 있는데, 이는 앞의 경찰통계에서 보았듯이 보이스피싱 검거인원 중 하부 조직원이 상당 부분을 차지하고 있기 때문이다. 판결문을 통해서 보이스피싱 범행단계-계획수립 및 구체적인 범행단계-를 살펴보고자 한다. 이와 더불어 대면편취책(현금수거책)의 가담경로가 제시된 경우 이에 대한 내용도 제시하였다. 이는 국내 현금수거책 가담을 예방하기 위한 대책마련에 기초자료가 될 수 있다는 점을 고려해서이다.

2. 보이스피싱 유형별 범행단계

가. 대출사기형

1) 저금리 대출유도 후 기존 대출받은 기관 사칭하여 대출금 편취

이 유형의 범행단계를 보면 먼저, 보이스피싱 조직원이 금융기관 직원을 사칭하여 피해자에게 전화하여 저금리대출을 제안하고 피해자의 대출신청을 유도한다. 이후 피해자가 기존 대출받은 금융기관 직원을 사칭하여 다시 전화해서 기존 대출금 상환을 요구, 피해자로부터 현금 혹은 계좌송금을 통하여 돈을 교부받는 단계로 이루어진다.

구체적인 사례를 통해서 범행단계를 살펴보면 아래의 〈사례1〉의 경우 ① 은행(혹은 다른 금융기관) 직원 사칭하여 저금리대출제안(전화) → ② 피해자대출신청 → ③ 기존 대출받은 기관사칭하여 계약위반이라고 하며 대출금 상환 요구 → ④ 현금수거책이 피해자로부터 현금 교부받음(위조된 대출상환증명서 사용) → ⑤ 조직책에게 계좌송금 등이다. 여기서 사례로 제시하지는 않았지만 계약위반이라고 하면서 금융감독원 신고 및 위약금 납부를 해야 한다고 겁을 주고, 현금을 편취하면서 위조된 채무완납증명서를 사용하는 경우(서울 중앙지방법원 2020고단 1662), 금융감독원에 통보되어 신용불량자가 되고 기존 통장 거래가 정지된다고 겁을 주는 방법을 사용하는 경우(대

구지방법원 2021고단2439) 등이 있다.

〈사례1〉

2021.12.8경 성명불상의 보이스피싱 조직원은 불상의 장소에서 ○○은행 직원 사칭하여 피해자에게 전화(4천만원까지 저금리대출 가능하다고 거짓말)→피해자 대출신청→12.10.경 다른 조직원이 △△저축은행 직원 사칭하여 피해자에게 전화(피해자가 받은 대출은 대환대출이 불가능한데 신규대출을 신청한 것은 계약위반이라고 함. 직원보낼테니 즉시 대출금 상환하라고 요구)→현금 대면편취(12.10.경 현금수거책이 △△저축은행 직원 사칭하여 □□아파트 지하주차장에서 피해자로부터 현금 19,648,000원을 교부받음)→계좌송금(현금수거책이 조직원이 지정하는 계좌로 송금)

※ 현금수거책 가담경로 및 역할
데이트어플을 통해 F를 알게 되고 F를 통해 E팀장 소개받음(대면한 적은 없음)→E팀장으로부터 텔레그램 메시지 등을 통해 지시받고 택시이용하여 피해자 만남(금감원, 은행, 저축은행 직원 등 사칭)→피해자로부터 현금받고 E팀장이 지정하는 계좌로 수차례에 걸쳐 송금.
출처: 울산지방법원 2021고단4620

위의 〈사례1〉 판결문에는 제시되지 않았지만 피해자의 기존 대출내역을 확인하는 방법은 크게 두 가지로 구분될 수 있는데 하나는 피해자의 앱 설치 및 대출신청서 작성을 통한 것이며, 다른 하나는 전화를 통한 대출상담 형식을 통하여 피해자의 개인정보 및 대출내역을 알아내는 것이다.

첫째, 앱 설치 및 대출신청서 작성 등을 이용하는 보이스피싱의 경우 주로 전화로 은행직원을 사칭하여 접근하고 있다. 구체적인 범행단계를 보면, ① 은행직원 사칭하여 저금리대출제안(전화) → ② 대출신청위한 앱 설치 요청(카톡) → ③ 앱 설치(피해자) → ④ 피해자의 기존 대출내역 확인 → ⑤ 기존 대출받은 기관사칭하여 피해자에게 전화해서 계약위반이라고 하며 기존 대출금 상환 요구(협박 등 포함) → ⑥ 피해자 현금인출 → ⑦ 현금수거책이 금융기관 직원사칭하여 피해자 만나서 현금 교부받음→ ⑧ 현금수거책이 보이스피싱 조직책의 지시대로 (100만원 단위로) 계좌송금 등이다. 다음에서는 이에 해당하는 사례들을 제시하였다.

〈사례2〉

2020.11.19.경 성명불상 보이스피싱 조직원은 불상의 장소에서 C캐피탈 직원사칭하여 피해자에게 전화(저금리 정부지원 자금 대출이 가능)→휴대전화에 카카오톡으로 보내 주는 어플 설치후 대출신청하라고 함)→피해자가 휴대전화에 어플설치→피해자의 기존대출내역을 확인→다른 성명불상자가 피해자가 기존에 대출받았던 D저축은행 직원 서민정을 사칭하여 전화(대출을 받은 때로부터 3개월 이내에 다른 기관(C캐피탈)에 대출 신청을 했기 때문에 금융거래법위반. 당일 원금을 상환하지 않으면 신용불량자로 등록되고 직장에 압류까지 들어간다고 함)→현금 대면편취(2020.11.20. 현금수거책이 성명불상자 지시에 따라 F농협 남부지점 앞에서 피해자에게 D저축은행 직원 사칭하여 서민정과장이 보내서 왔다고 하면서 피해자로부터 현금 7천만원 교부받음)→현금수거책이 보이스피싱 조직책이 지시하는 계좌로 100만원 단위로 무통장 송금
출처: 울산지방법원 2020고단5419, 2021고단612(병합)

〈사례3〉

2021.9.7.경 성명불상 보이스피싱 조직원은 불상의 장소에서 ○○캐피탈 직원을 사칭하여 피해자에게 전화(저금리 대출제안하며 어플리케이션 설치 후 개인정보 입력 요구)→피해자가 어플리케이션 설치 및 개인정보 입력→피해자가 기존에 대출받았던 △△△저축은행 직원 사칭하여 피해자에게 전화(기존 △△△저축은행 대출금 상환하지 않고 ○○캐피탈 대출을 받으면 위법임. 직원을 보낼테니 기존 대출금 상환하라고 요구)→현금 대면편취(2021.9.8. 18:27경 ○○앞길에서 현금수거책이 △△△저축은행 직원을 사칭하여 피해자로부터 현금 1천 50만원을 교부받음)→은행 ATM 기기에서 성명불상자(일명 '박 대리')가 알려준 계좌들로 100만원씩 분산 송금.

※ 현금수거책 가담경로
대부업체에서 알바를 구한다는 구인광고 문자를 받고 연락→ 2020. 8. 25.경 성명불상자(보이스피싱 조직원으로 일명 '박 대리')로부터 '고객의 돈을 받아 지정하는 계좌로 입금해주면 일일 최소 200,000원 이상 지급해 주겠다. 일이 없는 경우 대기해도 100,000원을 지급해주겠다'는 취지의 제안을 받고 성명불상자(일명 '박 대리')의 지시(텔레그램 이용)에 따라 피해자로부터 현금 수거, 이를 성명불상자(일명 '박 대리')가 알려준 계좌로 무통장 송금해주는 '수거책' 활동
출처: 춘천지방법원 2021고단51,2021고단 471(병합), 2021초기43, 2021초기316

〈사례4〉

2021.9.8.경 성명불상의 보이스피싱 조직원은 ○○은행 대출담당자를 사칭하여 피해자에게 전화(연 3.2%의 금리로 3,400만 원까지 대출이 가능하다고 함)→어플설치 요청(카카오톡으로 보내주는 어플을 설치하고 대출 신청을 하라고 함)→피해자가 어플설치 및 대출신청→다른 조직원이 피해자가 기존에 대출받았던 금융기관 직원 사칭하여 피해자에게 전화(△△ 직원인데 기존에 대출받은 금액 중 미변제 잔액 806만 원을 상환해야 ○○은행에서 대출이 가능하다고 함. 직원을 보낼테니 기존 대출금 전액을 현금으로 전달하라고 함)→현금 대면편취(2021.9.9. 11:40경 □□병원 주차장에서 현금수거책이 금융기관 직원을 사칭하여 피해자로부터 대출상환금 명목으로 806만 원을 교부받음)→보이스피싱조직책이 텔레그램을 통해 현금수거책에게 입금자 명단 및 송금할 계좌번호 전달→현금수거책은 806만 원 중 본인 수당 17만원을 제외한 789만원을 한 명당 100만원씩(한 명은 89만원) 무통장송금

※ 현금수거책 가담경로
구직광고보고 연락→ 투자증권 팀장이라는 사람으로부터 비대면 계좌개설 예약 고객이나 권한 대행

을 요청한 고객내방하여 확인서명받는 것이 주요 업무라고 설명들음→현금수거책 역할(통상적 채용 절차 거치지 않음)
출처: 대구지방법원 2022노3874

〈사례5〉

2020.9.23.경 성명불상 보이스피싱 조직원은 불상의 장소에서 ○○은행 직원 사칭하여 피해자에게 전화(저금리 대환대출 가능. 온라인신청서 작성요구)→피해자가 온라인신청서 작성→피해자의 기존 대출내역 확인→2020.9.24. 피해자가 기존에 대출받았던 △△△저축은행 직원 사칭하여 피해자에게 전화(△△△에서 대출받은 상품은 대환대출 신청 불가능함. 대출을 받으려면 기존 대출금 현금으로 변제요구)→2020.9.25. □□매장 인근에서 현금수거책이 △△△저축은행 직원을 사칭하여 피해자를 만나(보이스피싱 조직원이 앞서 알려준 직책과 가명(허위) 등을 미리 생각함) 피해자로부터 현금 1,990만원 교부받음→조직책이 알려준 계좌로 100만원 단위로 나누어 무통장 입금(입금자를 피해자 이름이 아닌 상선이 알려준 인적 사항 이용. 가상의 휴대전화번호를 기재하기도 함)

※ 현금수거책 가담경로
아르바이트 소개 사이트에 이력서를 올림→형식적인 신분확인만 한 뒤 곧바로 채용됨. 상선이 차는 피해자와의 약속장소에서 좀 떨어진 곳에 주차하고 피해자가 있는 장소에는 택시 혹은 도보로 이동해서 동선 노출을 방지하고자 함. 지정한 곳으로 차량을 타고 이동하여 무통장 입금.
출처: 광주지방법원 2021고합36,49(병합)

앞의 사례들에서 보았듯이 앱 설치 및 대출신청서 작성은 보이스피싱 조직원이 피해자에게 전화하여 대출신청을 제안하면서 이루어지는 것이다.

이 외에 ① 유튜브 배너광고를 통해 저금리 대출광고 → ② 피해자가 대출신청서 작성(연락처 등 기재) → ③ 은행 직원 사칭하여 피해자에게 전화(앱 설치후 대출신청서 작성 요구) → ④ 앱설치 및 대출신청서 작성(피해자) → ⑤ 피해자의 기존 대출내역 확인 → ⑥ 피해자가 기존 대출받은 대부업체 직원 사칭하여 피해자에게 전화해서 금융법위반, 고발고지하겠다고 하며 기존 대출금 상환 요구 → ⑦ 피해자 현금마련 → ⑧ 현금수거책이 대부업체 직원사칭하여 피해자 만나서 현금 교부받음 등의 단계로 이루어진 사례도 있다(대구지방법원 2021노3922).

둘째, 전화를 통한 대출상담을 통하여 피해자의 개인정보 및 대출내역을 알아내는 방법이 있다.

〈사례6〉의 경우 구체적 범행단계를 보면, ① 1차 상담원이 금융기관 직원 사칭하여 전화로 대출상담 → ② 전화를 통해 대출상담 명목으로 개인정보 및 기존 대출내역 확인(속칭 '원장' 생성) → ③ 2차 상담원 전화(기존 대출금 일부 상환 필요. 계좌송금

요구) → ④ 피해자가 대포통장으로 송금(※ 조직에서 보관하고 있던 DB에 있는 사람들에게 전화하여 신용등급 향상 등 명목으로 대포계좌(체크카드) 받음) → ⑤ 대포통장 소유자가 현금인출 → ⑥ 현금인출책이 보이스피싱 총책에게 전달(혹은 현금인출책이 체크카드로 현금인출하여 전달) 등이다.

〈사례6〉

Ⅰ. 범행준비단계
2015.1.경 보이스피싱 총책 D는 중국 ○○○시에 사무실 마련(전화기, 컴퓨터, 인터넷 설비 등 물적 시설 갖춤). 이후 다른 장소로 옮김→조직원 모집(관리자급 조직원, 피해자와 전화통화하는 콜센터 상담원 업무 조직원, 국내 대포통장에 입금된 피해금을 현금인출하는 조직원, 범행에 사용하는 사무실 전화번호 및 전화기 수급담당 조직원 등) 및 관리(관리자급 조직원들은 신규조직원에게 범행방법교육. 여권보관하여 임의귀국 막고, 탈퇴의사 밝힐 경우 폭행, 국내 수사기관에 제보하겠다고 협박하는 등 탈퇴방지)→조직원 통솔체계수립 및 업무지시(관리자급 조직원, 팀원 등으로 구분. 조직원 근무시간은 국내 금융기관 근무시간에 맞추어 오전 9시-18시로 함. 업무시간 이후에는 숙소생활. 외출, 외박, 개인적 모임 등은 제한적으로 허락)→총책이 피해자들 개인정보가 담긴 DB구해서 관리자급 조직원을 통해 상담원 역할 하위조직원에게 배포(하위조직원들은 범행가담기간 및 숙련도에 따라 각각 1차, 2차 상담원 역할)

Ⅱ. 범행실행
1. 일반적 보이스피싱 단계
1차 상담원 역할 조직원이 금융기관 직원 사칭하여 피해자에게 전화(대출상담을 해주는 것처럼 거짓말하는 방법으로 성명, 주민등록번호, 거주지, 기존 대출내역 등 정보 수집(속칭 '원장 생성)→2차 상담원 역할조직원이 피해자에게 전화(신용도를 높여 대출해주겠다는 등 거짓말을 하여 피해자로 하여금 국내 G가 보관 중인 대포통장으로 돈을 송금하도록 유인)→ G는 입금된 피해금을 인출한 후 총책에게 전달
2. 구체적 범행내용
2015.7.8. 피고인1(관리자급 조직원. 하위조직원 관리 및 피해자에게 전화)은 중국 칭다오시 청양구에 있는 보이스피싱 콜센터 사무실에서 금융기관 직원을 사칭하여 피해자에게 전화(기존 대출금 일부를 상환하면 저금리 대환대출 가능하다고 거짓말)→2015.7.9. 피해자로부터 대포통장으로 천만원 송금받음. 피고인2,3(각각 1차 상담원 역할)도 비슷한 수법으로 송금받음.
출처: 부산지방법원 2022고단3390

2) 저금리대출 등에 필요한 신용도 향상 혹은 고금리 대출기록 등을 이유로 대출금 편취

〈사례7〉의 경우 코로나19관련 대환대출 등을 제안하면서 고금리 대출을 유도한 것으로 구체적인 범행단계를 보면, ① 보이스피싱 조직원이 금융기관 직원 사칭하여 피해자에게 전화(코로나19관련 대환대출 제안) → ② 고금리 대출기록이 필요하니 카드론으로 대출받아 카드사에 변제할 것을 요구 → ③ 직원에게 현금으로 전해달라고

요구 → ④ 대출금완납증명서 위조 및 출력 → ⑤ 현금수거책이 금융기관 직원사칭하여 피해자만나서 현금 교부받음 → ⑥ 현금수거책이 조직책이 지정하는 계좌에 송금 등이다.

〈사례7〉

2020.9.24.경 성명불상자는 불상의 장소에서 금융기관 직원 사칭하여 피해자2에게 전화(정부에서 지원하는 코로나19관련 대환대출 가능)→대출받기 위해서는 고금리로 대출을 받은 기록 필요→카드론으로 대출받아 그 돈을 카드사에 변제하면 됨→직원을 보낼 테니 현금을 전달하라고 함→대출금완납증명서 위조(9.25. 11:00경 성명불상자가 현금수거책에게 대출금완납증명서 보냄)→현금수거책이 텔레그램을 통해 위조증명서받아서 출력. 해당카드사 대표 및 직원이 날인되어 있음)→2020. 9. 25. 11:30경 현금수거책은 금융기관 직원사칭하여 ○○○ 앞에서 피해자로부터 현금 2,500만원 교부받고 대출금완납증명서 교부)→현금수거책이 성명불상자가 지정하는 계좌에 송금.

※ 현금수거책 가담경로
2020.9경 성명불상자로부터 알려주는 곳으로 가서 사람을 만나서 돈을 받은 다음 알려준 계좌로 무통장 송금 시 해당금액의 2%를 수당으로 주겠다는 제안받음.
출처: 대구지방법원 2020고단5249,2020고단5588(병합)

〈사례8〉의 경우 저금리 마이너스통장사용을 위한 명목으로 고금리 대출을 유도하여 현금을 편취한 사례로 구체적인 범행단계를 보면, ① 보이스피싱 조직원이 금융기관 직원 사칭하여 피해자에게 전화 → ② 대출가능여부 확인 등을 이유로 개인정보 파악 → ③ 카드론 대출받아 즉시 완납할 경우 신용도 향상되어 저금리 마이너스통장 사용가능하다고 거짓말 → ④ 피해자가 카드론 대출받아 계좌송금 → ⑤ 보이스피싱 조직책이 현금인출책에 입금정보 전달 → ⑥ 현금인출책이 현금인출 → ⑨ 현금수거책이 조직책에 전달 등이다.[99]

99) 이외에도 금융기관 직원을 사칭하여 근로복지공단 생계지원비를 받을 수 있다고 전화한 후 이를 위해서는 제2금융권에서 대출을 받아 상환하는 방식으로 신용등급을 향상시켜야 한다고 속여 피해자로 하여금 대출받게 한 다음 대출금을 현금으로 대면편취한 사례도 있다(대전지방법원 2022노3417).

〈사례8〉

Ⅰ. 범행준비단계
2014. 10경 피고인A는 국내와 말레이시아에 사무실과 숙소공간 임차 및 조직원 모집→역할분담(피고인A는 전화금융사기 위한 대포통장, DB, 통신장비, 사무실 물품 등 마련, B는 전화금융사기 초기 자금 5,000만원 투자 뒤 범죄 수익금 관리·배분 담당, C는 콜센터 상담원 모집·교육 및 관리 업무, D 등 콜센터 상담원들은 은행대출담당 직원 사칭하여 저금리 대출을 위한 계좌이체 유도, 국내 인출책 E 등은 피해금 인출 후 수수료(3~10%)를 제외한 범죄 수익금을 B에게 전달하여 조직원들에게 분배하는 방식으로 계획)→조직원 통솔체계 및 업무배분(총책 3명은 사장 또는 실장 등으로 호칭하고, 상담원들은 서로 가명을 부르거나 대리로 호칭. 근무시간은 월-금요일 09:00-17:00경. 피고인A 등 총책 3명이 범죄 수익금의 1/3씩 갖고, 상담원은 숙식제공과 더불어 보이스피싱 성공 시 피해자가 입금한 돈의 약 30%를 수당으로 받음)

Ⅱ. 범행실행
콜센터 상담원들은 피고인 A로부터 받은 데이터베이스에 있는 피해자들에게 금융기관 사칭하여 전화(대출이 가능한 지 확인하는데 필요하다고 거짓말해서 기본 정도- 사업자 여부 등-를 제공받음)→다시 전화(카드론 대출을 받아서 기존 대출금 즉시 상환 시 신용평점이 올라 마이너스 통장(2,500만원) 저금리 사용이 가능하다고 하며, 카드론 대출을 받아 송금하라고 요구)→피해자가 카드론 대출받아 계좌송금→현금 인출팀에 입금정보 전달(피고인A와 B,C 등이 참여한 위챗 및 텔레그램 단체 대화방 등을 통해 입금 정보를 국내 현금 인출팀에게 전달)→현금인출팀이 현금인출(미리 받은 피해금 입금 계좌와 연결된 체크카드 이용)→보이스피싱 총책에게 전달
출처: 광주지방법원 2021고단1647

나. 사칭형

1) 기관사칭형

기관사칭형의 경우 경찰, 검사, 수사관 등을 사칭하여 피해자의 돈을 편취하는 사례들이 해당된다. 이 유형의 경우 범행단계에서 가짜 경찰청 앱이나 검찰청 사이트 접속 유도 등을 사용한다. 이 외에도 카카오톡 등을 통한 검사 재직증명서와 불기소 이유서 등 전달[100], (가짜) 수사기관 실무자 전화 연결, 수사를 이유로 한 협박(구속될 수 있다는 등), 사건번호 제시 및 구체적인 피해액수 언급[101], 위조문서[102] 등을 이용

100) 서울북부지방법원 2019고단4983 2019고단5645(병합), 2020고단1617(병합).
101) 검찰수사관을 사칭하여 피해자에게 전화한 후 피해자 명의의 통장·카드 등이 사용된 사건번호, 피의자 성명, 구체적인 피해금액 등을 제시한 사례도 있다(울산지방법원 2019고단4647).
102) 여기에 해당하는 사례로는 '검찰이 금융감독원에 제기한 민원에 대한 답변'이라는 제목하에 '금융범죄 금융계좌추적 민원'이라는 문서를 피해자에게 제공하고 금융감독원 직원을 사칭하여 현금을 대면편취한 사례가 있다(서울북부지방법원 2019고단4983). 또 다른 사례로 위조된 금융감독원 명의의 '검수확인서'를 사용한 사례가 있는데, 내용을 보면 '신청인에 피해자이름, 문서중간 부분에 '검수신청 금액은 익일 2시간, 6시간 □□은행 ****-****계좌로 반환됩니다. 말미에 금융감독원'이라고 기재하였다(춘천지방법원 2021노680). 이러한 위조문서는 내용이 구체적이고 금융감독원 등에 의해 작성된 문서라고 되어 있어서 피해자 입장에서 위조라고

하고 있다. 이러한 방법들을 이용하여 피해자의 돈을 편취하는 것이다.[103]

다음에서는 기관사칭형 유형별로 범행단계를 정리하였다.

가) 수사기관 사칭하여 전화한 후 수사목적(혹은 피해방지) 등을 빙자하여 피해금 편취

〈사례9〉의 경우 수사목적의 대출을 요구하여 현금을 편취한 사례이다. 구체적으로 범행단계를 보면, ① 보이스피싱조직 콜센터상담원이 검사와 수사관 사칭하여 피해자에게 전화(계좌가 범죄이용되어 수사필요) → ② 가짜 검찰청 사이트 접속 및 개인정보 입력 유도 → ③ 수사목적의 대출요구 → ④ 피해자가 대출받음 → ⑤ 검수확인을 명목으로 금융감독원 직원에게 전달하라고 요구[104] → ⑥ 현금수거책이 피해자 만나 현금 교부받음 등으로 이루어졌다.

〈사례9〉

Ⅰ. 범행준비단계
중국에 근거지 둔 조직결성(수시로 근거지를 옮기며 아파트나 오피스텔 임차(콜센터와 조직원 숙소로 사용))→검찰청 사칭수법이 전화대출사기수법보다 한 번 범행으로 더 많은 돈을 벌고 대면편취할 수 있다고 판단(대포통장 구입비용-1계좌당 100만원 이상에 거래- 줄임)→관리자급 조직원이 피해자들의 개인정보 데이터베이스를 수사관 역할 조직원에게 나누어 줌.

Ⅱ. 범행실행
2017.9.29.경 콜센터에서 서울중앙지방검찰청 검사와 수사관 사칭하여 피해자에게 전화(계좌가 범죄에 이용되어 피해자인지 피의자인지 확인필요하다고 함)→가짜 검찰청 사이트 접속유도(서울중앙지방검찰청 홈페이지와 유사한 가짜검찰청 사이트 인터넷 도메인 주소를 불러주어 가짜 검찰청 사이트 접속을 유도함. 피해자가 개인정보를 입력하여 사건조회를 할 경우 피해자관련 사건이 실제 접수되어 수사가 진행 중인 것처럼 화면 표시되게 함).→수사위한 대출 요구("신용등급을 일시적으로 10등급

생각하지 못할 수 있을 것이다.

103) 여기서 사례로 제시하지는 않았지만, 금융감독원 보도자료에 의하면 검찰 수사관을 사칭한 사기범이 '국제마약사건에 연루되었으니 검찰로 출두하라'는 요구에 피해자가 의심하자 (가짜)대검찰청 홈페이지 사이트주소를 불러준 후 이름과 주민등록번호를 입력하도록 하여 (가짜)영장을 보여줌으로써 피해자에게 진짜라는 확신을 주어 사기범이 요구한 대로 계좌이체를 한 사건이 있었다(금융감독원 2022년 4월 20일 보도자료, '21년 보이스피싱 피해현황 분석(https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=55444&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EB%B3%B4%EC%9D%B4%EC%8A%A4%ED%94%BC%EC%8B%B1&pageIndex=2, 검색일: 2023년 7월 17일).

104) 여기서 사례로 제시하지는 않았지만 검찰수사관 및 검사를 사칭한 보이스피싱 사례 중에는 피해자에게 피해자 입증에 필요하다며 현금을 인출하여 (가짜) 수사관에게 전달하라고 요구한 사례(울산지방법원 2019고단2615), 보호조치를 위해 통장잔액을 금융감독원 계좌로 입금하라고 요구한 사례(울산지방법원 2019고단4647)도 있다..

으로 낮출 테니까 대출을 시도해 봐라, 신용등급이 10등급으로 내려가면 대출 승인이 안 되어야 하는데 만약 대출이 되면 신용정보가 조작되어 범죄에 이용되고 있다는 증거이니, 일단 대출을 해 봐라."라고 거짓말)→피해자가 대출받음(2,000만원을 대출받게 한 후 "대출승인 금액을 보니 당신의 개인정보가 심각하게 유출된 것 같다. 검수를 해봐야 하니 대출받은 돈을 현금으로 인출해서 우리가 보내는 금융감독원 직원에게 건네라"고 함)→현금 대면편취(9.29. 15:30경 금융감독원 직원 사칭한 현금수거책이 ○○아파트 부근에서 피해자로부터 현금 2,000만원을 교부받음).
출처: 부산지방법원 2022고단4244

〈사례10〉과 〈사례11〉의 경우 피해자에게 추가피해를 막기 위한 것이라고 속여 현금을 편취한 유형이다. 〈사례10〉의 범행단계를 보면 ① 보이스피싱조직 콜센터상담원이 검사와 수사관 사칭하여 피해자에게 전화(계좌가 범죄이용되어 수사필요)→② 일차적으로 유선조사할 것이며, 혐의점 발견되면 소환조사나 영장발부될 수 있다고 겁을 줌 → ③ (가짜) 유선조사 진행(개인정보, 계좌개설 내역 및 예치금액 등 파악) → ④ 추가피해 막기 위해 피해자 명의계좌의 모든 돈을 현금으로 인출하여 지정한 장소에 보관하도록 요구 → ⑤ 피해자가 현금인출하여 물품보관함에 둠 → ⑥ 현금수거책이 보관함에서 현금을 가져감 등으로 이루어졌다.

〈사례10 〉

Ⅰ. 범행준비단계
물적 시설 마련(2016.2. 초순경 중국 칭다오시에 사무실을 두고 수시로 사무실 이전. 피해자들의 인적 사항, 연락처 등이 담긴 DB 등을 불상의 방법으로 취득후 조직원에게 배포하여 피해자 물색하는 방법으로 콜센터 운영)→조직원 역할분담('N'은 보이스피싱 조직의 총책. 사무실과 숙소 임차, 집기설치, 조직원들을 총괄 관리·운영, 범행 지시 및 조직원들에 대한 숙식 제공, 범행 성공수당을 지급·관리하는 역할, 'Q'는 콜센터와 연계해서 '장집' 운영, 대포통장, DB 마련해서 콜센터 조직에 공급, 'R'은 신규 조직원을 모집하고, 대포전화 세팅, DB관리(피해자 개인정보), 가짜 검찰 홈페이지 사이트 개설 및 관리, 'S'는 중국 공안에게 뇌물 상납 등으로 단속을 대비하는 역할, 'T'는 콜센터 조직원에게 범행 지시, DB 제공, 조직원 실적 관리 등 콜센터 총괄 및 신규 조직원 모집, 피고인 A(가명 'U'), 피고인 B 등 콜센터 상담원. 이 중 일부는 콜센터상담원 활동과 동시에 대포통장 모집하는 전화상담원 역할도 담당, 국내에서 현금수거하여 송금하는 '세탁집'조직원 등)→신규 조직원 교육('T'와 'Q' 등은 신규 조직원을 대상으로 범행 시 피해자와 대화할 멘트가 기재된 매뉴얼 제공. 검사와 수사관을 사칭하며 법률용어를 말하는 요령과 노하우를 알려주는 등 교육실시, 조직원들이 범행수법을 습득하게 되면 범행에 투입시키며 관리)→조직원 관리(조직원들간 가명 사용 및 위챗, 큐큐 등 메신저 사용(대한민국 수사기관 추적 어렵도록 하기 위해), 개인 휴대전화에도 중국 유심칩 사용, 월-금요일 오전 8시 출근)→수익배분(수사관 역할을 하는 조직원은 최초로 전화해서 유인한 피해자로부터 받은 돈의 10%, 검사 역할의 조직원들은 피해금원의 15%, 관리자급 이상 조직원들은 사무실 운영비와 위 조직원들에게 분배한 금원을 공제한 나머지 금원을 각 직급에 따라 일정한 비율로 받음).

Ⅱ. 범행실행
2019.10.18. 09:45분경 중국 콜센터 사무실에서 서울중앙지방검찰청 검사, 수사관을 사칭하여 피

해자에게 전화(금융사기 사건에 피해자 명의 통장이 발견되어서 사건 연루여부에 대한 조사 필요. 피해자 개인정보가 유출된 것인지, 사기사건에 가담한 것인지에 대한 검찰조사 받아야 함. 본인 명의 통장을 판매했거나 대여한 것이면 처벌을 하기 위한 조사를 해야 하고, 개인정보가 유출된 피해자라면 실시간 보호조치 진행. 이를 알아보기 위해 일차적으로 유선 조사를 하며, 혐의점이 발견되면 유선조사 중단, 소환조사를 받게 되거나 영장발부가 될 수 있다고 말함. 계속하여 피해자에게 이름, 생년월일, 실제 거주지, 직업, 신분증의 분실이나 대여 여부, 본인 명의의 계좌개설 관련 정보, 해당 계좌에 있는 금원 등을 질문함→추가 피해를 막기 위해 피해자 명의 계좌에 있는 돈을 모두 현금으로 인출하여 지정한 장소에 보관하라고 함→현금을 보관함에 두게 함(10.18. 18:45 경 ○○구 주민센터 무인택배함에 현금 1천 2백만원을 보관하게 함)→현금수거책이 가져감.
출처: 부산지방법원 2021고단1438

〈사례11〉의 범행단계를 보면 ① 성명불상 조직원이 사이버수사대 경찰을 사칭하여 피해자에게 전화(계좌가 범죄이용되어 수사필요) → ② (가짜) 경찰청 앱 설치 요구[105] → ③ 담당검사로부터 연락올 것이라고 함 → ④ 대검찰청 검사 사칭하여 피해자에게 전화(추가피해 막기 위해 대출받아 금융감독위원회 계좌로 송금하도록 요구. 마무리되면 반환해 준다고 함) → ⑤ 피해자가 계좌송금 → ⑥ 계좌명의자가 현금인출하여 계좌모집책에 전달 → ⑦ 계좌모집책은 받은 돈을 전달책에 전달 → ⑧ 전달책이 환전소를 통해 조직원에게 송금 등으로 이루어졌다.

〈사례11〉

2020. 4.13.경 성명불상 조직원은 불상의 장소에서 사이버 수사대 정현우 경사를 사칭하여 피해자에게 전화(사건번호 2020형제7849호 사건 관련 피해자 명의 통장이 범행에 이용되는 중이니 알려주는 앱(경찰청 폴 안티스파이 3.0 Team Viewer)을 다운받도록 함. 담당검사로부터 연락이 올 것이라고 함)→같은 날 대검찰청 최재현 검사를 사칭하여 피해자에게 전화(피해자 명의 대포통장으로 인해 다른 재산상 피해가 발생할 수 있으니 추가 피해를 막기 위해 대출을 받아 금융감독위원회 명의의 금융계좌로 송금하라고 함. 사건이 마무리되면 반환해주겠다고 함)→피해자가 계좌송금(2020.4.14.11:39경 조직원이 알려준 2개의 계좌(H명의, K명의)로 2차례에 걸쳐 각각 2,600만원, 2,500만원 송금)→현금인출 및 조직원에게 송금(H는 4.14.피해자가 입금한 2,600만원을 인출하여 수고비 500만원을 제외한 2,100만원을 E에게 건네줌. E는 같은 날 사무실에서 2,100만원을 F에게 건네주고, F는 같은 날 R환전소를 통해 불상의 보이스피싱 조직원에게 송금)
출처: 울산지방법원 2020고단5201

〈사례12〉는 수사기관을 사칭하여 피해자의 개인정보를 알아낸 후 피해자 명의로

105) 이와 유사하게 수사기관 등을 사칭하여 전화·비대면조사를 위해 '진술서'를 작성해야 한다는 명목으로 휴대전화에 악성 앱을 설치하도록 하는 사례도 있다(국무조정실 2022년 9월 29일 보도자료, "보이스피싱 범죄근절을 위한 통신·금융분야 대책 발표"((https://www.fsc.go.kr/no010101/78643, 검색일: 2023년 6월 10일).

대출받아 편취한 유형이다. 구체적인 범행단계를 보면, ① 보이스피싱 조직원이 경찰·검사를 사칭하여 피해자에게 전화(금융범죄연루로 계좌추적 필요) → ② 앱 설치 및 공인 인증서 발급 후 비밀번호 알려달라고 함 → ③ 대출에 필요한 정보 파악 → ④ 피해자 명의로 대출받음 → ⑤ 피해자에게 다시 전화(금융감독원에서 해외로 세탁하려는 돈을 찾아서 피해자 명의 계좌로 입금했다고 하고 찾아서 수사관에게 달라고 함)→ ⑥ 피해자 현금인출 → ⑦ 현금수거책이 피해자로부터 현금받음(위조된 금융범죄 금융계좌추적 서류 교부) → ⑧ 현금수거책이 보이스피싱 총책이 지정한 계좌로 송금으로 이루어졌다.

〈사례12〉

2019. 10. 30.경 성명불상의 보이스피싱 조직원은 경찰관과 검사 사칭하여 피해자에게 전화(개인정보가 유출되었고, 금융범죄에 연류되어 계좌추적 필요) → 앱 설치 및 공인인증서 발급 받고 비밀번호를 알려 달라고 함→피해자로부터 대출을 위해 필요한 정보를 알아낸 후 피해자 모르게 피해자 명의로 ○○생명에서 대출받음(2,700만원)→피해자에게 다시 전화(금융감독원에서 범죄자들이 해외로 세탁하려는 돈을 찾아서 피해자의 ○○은행 계좌로 2,700만 원을 입금했으니 돈을 인출하여 수사관에게 전달하라고 함)→피해자는 2,700만원 중 1,500만원 인출 → 현금 대면편취(같은 날 20:20경 □□시 택시승강장 앞길에서 현금수거책이 피해자에게 '금융범죄 금융계좌추적 민원' 서류 1장을 건네주고 1500만원을 받음→현금수거책이 보이스피싱 총책이 지정한 계좌로 송금(현금수거책 수당 30만원 제외한 1,470만원 송금)

※현금수거책 가담경로
페이스북 구인광고를 보고 김실장(보이스피싱 총책)과 연락 → 피해자들을 직접 만나 금융감독원 직원사칭하여 현금받은 후 송금(또는 전달)하는 역할하기로 함.
출처: 서울북부지방법원 2019고단4983 2019고단5645(병합), 2020고단1617(병합)

다음의 〈사례13〉은 수사기관을 사칭하여 상품권 결제를 하도록 유도한 후 핀번호를 알아내어 편취한 유형이다. 구체적 범행단계를 보면, ① 성명불상자가 검사를 사칭하여 피해자에게 전화(중고거래 사기에 계좌가 사용되었다고 함) → ② 피해자에게 수사협조의뢰서 보냄 → ③ 상품권 결제 지시(피해수법 재연에 필요하다고 함) → ④ 피해자가 소셜커머스에서 상품권 결제 → ⑤ 피해자에게 상품권 식별번호(핀번호) 알려달라고 함 → ⑥ 식별번호로 상품권 사용 등으로 이어지는 것이다.

〈사례13〉

2023년 3월 성명불상자는 서울중앙지검 검사를 사칭하여 피해자(23세)에게 전화(계좌가 중고거래 사기에 사용되었다고 하며 수사협조의뢰서 보냄)→상품권 결제 지시(피해수법 재연에 필요하다고 함)→피해자는 소셜커머스에서 8차례에 걸쳐 상품권 570만원 결제후 온라인에서 상품권쓸 때 사용되는 식별번호(핀번호)를 성명불상자에게 알려줌.

출처: 조선일보 2023년 5월 8일자, 직접 결제해 상품권 번호까지 넘겼다…진화한 상품권 피싱에 눈물 흘리는 청년들(https://www.chosun.com/national/national_general/2023/05/08/3GM6DRTQFRHL3IPEQRL4YTQTBY/?utm_source=naver&utm_medium=referral&utm_campaign=naver-news, 검색일: 2023년 5월 10일).

나) 피싱문자 발송후 연락온 피해자에게 수사기관 사칭하여 피해금 편취

여기에 속하는 유형 중 〈사례14-1〉과 〈사례14-2〉의 범행단계를 보면, ① 피해자에게 물품구입 문자발송 → ② 피해자가 구입사실 없다고 전화 → ③ 피해자명의 계좌의 대포통장 사용 등 피해가능성 언급하며 수사실무자 연결 → ④ 수사실무자 사칭하여 통화(추가 피해막기 위해 현금인출하여 금융감독원 직원 등에게 전달하라고 요구)→ ⑤ 피해자 현금인출 → ⑥ 현금수거책이 금융감독원 직원 등을 사칭하여 피해자로부터 현금 교부받음 등으로 이루어진다.

〈사례14〉

Ⅰ. 범행준비단계

조직구성 및 역할(① 'TM(텔레마케터)'(KG모빌리언스를 사칭해서 불특정 다수에게 문자메시지를 보낸 후 이를 받은 사람들 중 전화를 한 사람들에게 서울지방경찰청 사이버수사대 형사와 검찰청 검사 등을 사칭해서 계좌가 범죄에 사용되었으니 지정한 계좌에 돈을 이체하라며 피해자들을 속여 피해자가 돈을 이체하거나 교부하도록 하는 역할), ② '환전책'(피해자들이 이체한 금원을 전달받아 자금을 세탁한 후 총책에게 전달), ③ '팀장'(TM이 KG모빌리언스를 사칭해서 피해자를 속힌 다음 전화를 넘겨주면 서울지방경찰청 사이버수사대 형사, 검찰청 검사를 사칭해서 범행을 지휘, TM의 출퇴근 등 관리), ④ '실장'(컴퓨터로 모든 데이터 관리, 피해자 휴대폰에 설치된 '팀뷰어 퀵서포트' 앱을 조작해서 TM에게 피해자의 개인정보 자료를 주고 개별 범행 지시), ⑤ 'TM 모집책'(한국에서 보이스피싱 TM으로 일할 사람을 중국 보이스피싱 사무실로 보냄), ⑥ 총책(조직전반 관리)

Ⅱ. 범행실행

〈사례14-1〉

2019.9.6.경 보이스피싱 텔레마케터는 중국 청도의 보이스피싱 콜센터에서 피해자에게 피싱문자 발송(KG모빌리언스를 사칭해서 문자 메시지 보냄(청소기가 정상적으로 구입되었다는 내용)→피해자는 문자 메시지 받은 후 청소기 구입사실이 없다며 전화→피해자에게 대포 통장이 사용된 것 같으니 서울영등포경찰서 수사과장을 연결해준다고 함→다른 조직원이 서울영등포경찰서 수사과장과 서울지방경찰청 수사과장을 사칭하여 통화(개인정보 유출로 은행에 보관된 돈을 그대로 두면 위험, 현재 범인을

검거하고자 하는 상황이니 검거될 때까지 돈을 보관해주겠다고 함)→피해자가 현금인출→현금 대면 편취(9.9. 15:00경 현금수거책이 △△초등학교 앞에서 피해자로부터 3,720만 원을 교부받고, 동일한 장소에서 9.10. 17:00경 3,000만원을, 9.11. 16:00경 1,857만원을 교부받는 등 총 8,577만원을 교부받아 편취.

〈사례14-2〉

2019.10.8. 10:00경 보이스피싱 텔레마케터는 중국 청도 보이스피싱 콜센터에서 피싱문자 발송(KG모빌리언스를 사칭해서 맥북 노트북 구매로 499,000원 결제하겠다는)→피해자가 문자 메시지를 받고 노트북 구입사실이 없다며 전화→수사기관에 대신 신고해 준다고 함→다른 조직원이 서울지방경찰청, 금융감독원, 검찰청을 사칭하여 전화하여 계좌가 대포 통장으로 이용되었으니 어플을 원격으로 설치하라고 함→대포 통장으로 사용된 계좌의 현금을 인출하여 금융감독원 직원에게 보여주면 일련번호 확인후 다시 입금해주겠다고 함→10.8. 17:00-18:00경 현금수거책이 □□빌라앞 골목길에서 금융감독원 직원을 사칭하여 피해자로부터 현금 5,000만원을 교부받음.

※ 보이스피싱 TM가담경로

-2019.6. 초순경 ○○공터에서 친구로부터 '중국 보이스피싱 조직에서 일하도록 소개해 줄 수 있으며, 월 천만원-이천만원 벌 수 있다는 말을 듣고 같은 해 8.23. 중국 청도 콜센터에서 일함.

출처 : 춘천지방법원 2020고단1396

〈사례15-1〉도 〈사례14-1〉, 〈사례14-2〉와 유사한 범행단계로 이루어짐을 알 수 있다. 〈사례15-1〉의 경우 범행단계 중 하나로 수사기관을 사칭하여 퀵서포트라는 앱을 설치하도록 하는 단계가 있다. 참고로 '팀뷰어 퀵서포트'(TeamViewer QuickSuppor) 앱을 설치할 경우 휴대전화의 아이디가 부여되며 이를 보이스피싱 범죄자에게 알려주면, 범죄자는 이 아이디를 이용해서 피해자 휴대전화를 원격으로 모니터링하고 임의로 파일 전송받는 것 등이 가능하게 된다.[106]

〈사례15-2〉의 범행단계를 보면, ① 피해자에게 해외결제 승인문자 발송→② 피해자가 문자보고 전화→③ 경찰 사칭하여 휴대전화에 퀵서포트 설치요구→④ 금융감독원 직원 사칭하여 전화(많은 사람이 피해자를 고소했고 피해자 명의 통장으로 현금세탁 정황있음. 신용한도만큼 대출받아서 보관필요하다고 함) → ⑤ 피해자 대출받음 → ⑥ 현금수거책이 피해자로부터 현금 교부받음(위조된 금융위원회 명의 금융계좌추적 민원서류 1장 교부) → ⑦ 현금수거책이 성명불상자가 지정하는 사람에게 현금전달 등으로 이루어졌다.

106) 김경진·서준배, 보이스피싱 현황과 정책제언, 시큐리티연구 제66호, 2021, 123면.

〈사례15〉

〈사례15-1〉
2021.6.2.경 성명불상의 보이스피싱 조직원들은 불상의 장소에서 피해자에게 해외결제 승인문자 발송→문자보고 연락한 피해자에게 아마존닷컴 직원 사칭(스미싱피해를 당한 것 같다고 함)→인천서부경찰서 이상화경위 사칭하여 휴대폰에 어플리케이션 설치요구(수사위해 피해접수 필요. 퀵서포트라는 어플리케이션 설치요구)→금융감독원 불법금융조사1국 안혁준과장 사칭((피해자 명의가 도용되어 중고사이트 등에서 피해자 계좌를 이용하여 피해자 발생(70여명). 이들이 당신을 고소한 상태라고 함. 수사기관이 비밀리 조사 진행 중이라고 하며 담당 검사와 통화 해보라고 함)→ 김현우 검사사칭(금융감독원 과장의 부탁으로 약식 기소로 진행할테니 비밀리에 조사 협조요청. 계좌 돈을 그대로 두면 범죄에 계속 이용될 수 있으니 모든 계좌 돈을 법원보관금으로 보관할 필요가 있다고 함. 이후 피해자로 입증될 경우 돌려준다고 함)→6.11. 16:22경 G아파트 지하주차장에서 피해자로부터 현금 9,300만 원을 교부받음→9,250만 원을 성명불상자가 지정하는 사람에게 전달.

〈사례15-2〉
2021.6.11.경 성명불상의 보이스피싱 조직원들은 불상의 장소에서 피해자에게 해외결제 승인문자 발송→문자보고 연락한 피해자에게 인천서부경찰서 직원 사칭(휴대전화에 퀵서포트 설치요구)→금융감독원 직원사칭(많은 사람이 당신을 고소했고, 피해자 명의 대포통장으로 현금세탁 정황있다고 함. 국세청에 신용한도만큼 대출받아서 보관해야 한다고 거짓말)→6.14. 16:16경 H초등학교 정문 앞길에서 위조한 금융범죄 금융계좌추적 민원서류1장(현금수거책이 이메일을 통해 전달받음. 금융위원회 명의의 서류로 "서울중앙지방검찰청 담당 검사 및 수사관에게 피해자의 금융계좌 추적을 실시할 수 있도록 지도하였고, 계좌 추적 후 불법계좌 및 불법자금이 확인될 경우 동결처리 및 국고 환수조치가 될 것이다. 피해자에게 국가안전보안 계좌코드를 발급할 것이며 금융자산 추적 및 감독 이후 안전하게 원상복구할 것이다"는 내용)을 피해자에게 교부하고, 피해자로부터 현금 4,000만원 교부받음. 6.17. 15:29경 H초등학교 정문 앞길에서 2,400만원 교부받음→성명불상자가 지정하는 사람에게 각 3,980만원, 2,380만원 전달

※현금수거책 가담경로
'한유정'이라는 사람(성명불상자)이 일일알바 채용관련 문자메시지 발송→연락하여 '온누리 대행업체'에서 대출금 상환관련 업무 제의받음→인터넷으로 회사검색해서 그런 명칭의 회사가 있다는 것만 확인→'한유정'으로부터 카카오톡으로 매번 현금교부받는 장소와 시간, 현금교부받을 사람의 정보(성별과 인상착의 등)를 전달받음→'한유정'이 카카오톡으로 알려주는 성명불상자들에게 현금을 그대로 전달.
출처: 대구지방법원 2022고합200, 2022초기10150, 10151

다) 우체국직원 사칭하여 전화하여 해외 카드사용 알린 후 수사시관 사칭하여 피해금 편취

〈사례16〉은 보이스피싱 조직원이 피해자에게 우체국 직원을 사칭하여 해외에서 카드사용이 되었다고 거짓말한 후 수사기관을 사칭하여 다시 전화하여 추가피해를 막기 위해 현금을 물품보관함에 보관하도록 한 후 편취한 유형이다. 구체적인 범행단계를 보면, ① 보이스피싱 조직원이 우체국 직원사칭하여 피해자에게 전화(해외에서 카드사용되었다고 거짓말) → ② 경찰에서 연락올 것이라고 함 → ③ 경찰사칭하여 피

해자에게 전화(추가피해 막기 위해 현금을 물품보관함에 보관하라고 함)→④ 피해자 현금인출 → ⑤ 물품보관함 2곳에 현금보관(열쇠잠그지 않음) → ⑥ 조직원이 상황을 현금수거책에게 전달 → ⑦ 현금수거책이 물품보관함에서 현금을 꺼내어 감 등이다.

〈사례16〉

> 2019.9.18. 09:50경 성명불상 보이스피싱조직원은 불상의 장소에서 우체국 직원 사칭하여 피해자(74세)에게 전화(피해자 명의 카드가 발행되어 일본에서 280만원이 사용됨. 경찰서에서 연락을 줄 것이라고 함)→피해자에게 다시 전화(□□은행에 돈이 있으면 다 빠져나가니 돈을 찾아 ○○지하철역 물품보관함에 보관후 새 주민등록증을 신청하고 □□은행 통장 재발급하라고 함)→같은 날 피해자가 □□은행에서 2회에 걸쳐 현금인출→같은 날 지하철역 물품보관함 2곳에 열쇠를 잠그지 않은 상태로 각각 현금 500만원, 380만원 넣어 둠→성명불상 조직원은 현금수거책에게 이 사실을 전달→같은 날 현금수거책은 물품보관함에서 현금을 꺼내어 감.
> 출처: 부산지방법원 2019고단4533

2) 가족·지인사칭형

가족이나 지인을 사칭하는 보이스피싱은 메신저를 이용하는 경우들이 많다. 참고로 앞에서 살펴본 금융감독원 통계에 의하면, 최근 가족·지인사칭 메신저피싱 비중이 크게 증가한 것으로 나타나고 있다. 가족이나 지인을 사칭하는 보이스피싱의 경우 메신저를 통하여 급하게 돈이 필요한 상황을 설명한 후 계좌송금을 유도하거나 휴대폰 원격제어 프로그램 앱설치를 유도한 후 피해자 은행계좌에 접속하여 직접 계좌이체를 하기도 한다. 아래의 〈사례17〉과 〈사례18〉은 자녀·지인사칭형 보이스피싱 사례이며, 구체적인 범행단계는 다음과 같다. 〈사례17〉의 경우 ① 보이스피싱 조직원이 인터넷 메신저를 통해 자녀를 사칭하여 피해자에게 연락(휴대전화 단말기파손으로 보험금 청구에 필요하니 피해자 은행 계좌번호와 비밀번호 알려달라함) → ② 피해자에게 휴대폰 원격제어 프로그램 앱설치 요청 → ③ 피해자가 앱설치하고 계좌번호 및 비밀번호 알려줌 → ④ 보이스피싱 조직원이 피해자 정보 이용하여 피해자 은행계좌 접속후 타 계좌(대포통장)로 송금 → ⑤ 보이스피싱 조직원이 현금수거책에게 현금인출 지시 → ⑥ 현금수거책이 현금 인출(대포통장 소유자 명의 체크카드와 비밀번호 이용) → ⑦ 현금수거책이 보이스피싱 조직책에게 계좌송금 등이다.

〈사례17〉

2021.12.9. 17:00경 성명불상자는 불상의 장소에서 피해자에게 아들인 것처럼 가장하여 카카오톡 메시지 보냄(휴대전화 단말기 파손되어 보험금 청구에 필요하니 피해자 ○○은행 계좌번호와 비밀번호를 알려달라고 하면서 피해자로 하여금 휴대폰 원격제어 프로그램 앱을 설치하게 함)→피해자가 앱 설치하고 은행 계좌번호와 비밀번호 알려줌→성명불상자는 같은 날 이 정보를 이용하여 피해자 은행 계좌에 접속하여 990,000원을 B명의의 계좌로 송금하는 등 6회에 걸쳐 5,790,000원 송금함→성명불상자가 현금수거책에게 현금인출 지시(위챗으로 B의 은행계좌 비밀번호를 알려주면서 6백만원을 현금인출하라고 지시)→현금수거책이 현금인출(미리 소지한 B명의 체크카드와 비밀번호를 이용하여 6회에 걸쳐 6백만원 현금인출)→현금수거책이 보이스피싱 조직책에 계좌송금(환전소에서 6백만원을 중국 은행계좌로 송금).

※ 현금수거책 가담경로
21.12경 텔레그램에서 성명불상자가 올린 아르바이트광고를 보고 알게 됨→ 제안을 받고(일당 20만원) 성명불상자가 택배를 통해 보낸 B명의의 기업은행 체크카드 수령.
출처: 대구지방법원 2022구단10929

〈사례18〉의 경우 지인사칭 유형으로 범행단계를 보면, ① 보이스피싱 조직원이 인터넷 메신저를 통해 지인을 사칭하여 피해자에게 연락(급히 결제필요하나 오류로 이체가 되지 않으니 대신 결제 요청)→② 피해자가 (대포통장 명의자 통장으로) 계좌송금→③ 현금인출책이 현금인출(대포통장 명의자 체크카드 이용)→④ 현금인출책이 보이스피싱 조직원이 지시하는 계좌로 무통장 송금 등이다.

〈사례18〉

2018.6.14. 10:52경 성명불상의 보이스피싱 조직원은 인터넷 C메신저를 통해 피해자 지인사칭(피해자 거래업체인 노인복지관 영양사 사칭)하여 연락(급하게 결제해야 하는데 오류로 인해 이체가 안되니 결제를 대신해 달라고 부탁. 17:00 이전에 변제하겠다고 함)→피해자가 계좌송금(같은 날 11:14경 피해자가 H명의 ○○은행계좌로 5백9십6만원, 13:35경 다른 사람 명의 △△은행 계좌로 6백3만원 등 2회에 거쳐 1,199만원 송금)→현금인출책이 체크카드로 현금인출(현금인출책은 보이스피싱 조직원인 성명불상자의 지시에 따라 6.14 11:47부터 11:53까지 택배로 배송받아 보관하고 있던 H명의 체크카드로 6회에 걸쳐 596만원 인출)→무통장 송금(현금인출책이 성명불상자가 지시하는 계좌로 무통장 송금).
출처: 창원지방법원 2019고단1055

다. 기타 유형

여기서는 최근에 나타난 새로운 유형들을 제시하고 범행단계를 살펴보았다.

1) 링크 포함된 문자발송 후 악성앱 설치를 통한 편취

〈사례19〉의 경우 ① 피해자 휴대전화로 결혼식 초대장 링크 포함된 문자발송→② 피해자가 초대장 링크 클릭→③ 피해자 휴대전화에 악성앱 설치됨→④ 피해자 휴대전화에 보관하고 있던 개인정보, 금융정보 등이 사기범에게 전송됨→⑤ 사기범은 피해자 명의 은행 앱에 접속하여 신규 비대면 대출받음→⑥ 사기범이 대출받은 자금을 다른 계좌로 이체 등의 단계로 이루어졌다.

〈사례19〉

A씨는 휴대전화로 결혼식 초대장 링크가 있는 문자를 받았음. 이에 별다른 의심을 하지 않고 초대장 링크를 클릭했는데 악성 앱(모바일초대장.apk)이 설치되어 휴대전화에 있던 개인정보와 금융정보 등이 사기범에게 전송되었음. 사기범은 이러한 정보를 이용해서 A씨 명의 ○○은행 앱에 접속하여 신규 비대면 대출을 받아 자금을 이체
출처: 경찰청 내부자료

2) 주식거래 손해보상 회사 직원을 사칭하여 개인정보 알아낸 뒤 피해자 명의로 대출받아 편취

〈사례20〉의 경우 ① 주식거래 손해를 보상해 주는 회사를 사칭하여 피해자에게 전화(손실금 1억원 송금하겠다고 함)→② (피해자 개인정보 알아낸 후) 피해자 명의로 대출받음→③ 피해자 계좌로 1억원 입금(피해자 명의로 대출받은 돈)→④ 피해자에게 다시 전화(수익률 좋은 코인에 투자해 주겠다고 함)→⑤ 피해자가 계좌송금 등으로 이루어졌다.

〈사례20〉

경찰청 국가수사본부에 따르면 최근 주식거래로 입은 손해보상을 해주겠다고 속여 접근하는 보이스피싱 유형이 많이 발생하고 있다고 함. 010으로 시작하는 번호로 피해자에게 전화(주식거래 손해를 보상해주는 회사인데 손실금 1억원을 송금하겠다고 함)→피해자명의로 대출받음→다음 날 피해자 계좌로 1억원 입금(피해자 명의로 대출받은 돈)→피해자에게 다시 전화(수익률 좋은 코인에 투자해주겠다고 하며 계좌송금유인)→피해자가 계좌송금
출처: 연합뉴스 2023년 5월 9일자, '주식손해보상' 미끼로 접근…신종 보이스피싱 주의보 (https://www.yna.co.kr/view/AKR20230509081400004?input=1195z, 검색일: 2023년 7월20일).

3) 통신회사 직원 사칭하여 조합사무실 전화번호 착신유도 후 조합원 분담금 등 편취

〈사례21〉의 경우 핵심 개인정보를 입수한 후 이를 이용한 일회성·맞춤형 보이스피싱에 해당한다. 언론 보도자료이기 때문에 내용 파악에는 한계가 있지만, 범행단계를 보면 다음과 같다. ① 조합원 관련 사전 정보 파악(조합사무실 전화번호, 조합원 대상 비용청구 등) → ② 통신회사 직원 사칭하여 조합사무실에 전화(통신장애를 이유로 다른 전화번호 착신유도) → ③ 조합원이 사무실에 건 전화가 용의자에게 연결됨 → ④ 조합원에게 분담금과 옵션비 명목으로 송금 요구 → ⑤ 피해자가 계좌송금 등으로 이루어졌다.

〈사례21〉

> 용의자는 통신회사 직원 사칭해 ○○아파트 조합사무실에 전화(통신장애가 발생했다며 다른 전화번호 착신유도)→조합원들이 조합사무실에 전화하면 용의자에게 연결됨→분담금과 옵션비 명목으로 송금요구→피해자가 1,500만원 송금
> 출처: 서울경제 2023년 5월 3일자, '해외직구 결제 639,000원'…보이스피싱 그놈 미끼였다 (https://www.sedaily.com/NewsView/29PFOGNET4, 검색일: 2023년 5월 10일).

제2절 | 보이스피싱 범행단계별 특성 정리

앞에서 판결문과 언론보도자료 등을 통하여 보이스피싱 유형별 사례를 제시하고, 각 사례별 범행단계를 정리해 보았다. 여기서는 이 연구의 분석대상이 된 자료들을 토대로 보이스피싱 범행준비단계와 실행단계로 구분하여 각 단계별 특성을 정리하였다.

1. 범행준비단계

가. 조직구성 및 물적 구성

판결문을 통해서 보이스피싱 범행준비단계를 보면, 먼저, 조직구성 및 물적 자원을 확보하는 단계가 있다. 보이스피싱 조직의 총책이 주로 외국에 근거지를 두고 사무실, 전화기, 컴퓨터, 인터넷 설비 등 물적 기반을 마련하고 있다(〈사례6〉, 〈사례8〉, 〈사례

9〉, 〈사례10〉). 근거지는 중국(사례6〉 〈사례9〉, 〈사례10〉), 말레이시아(〈사례8〉) 등이며, 조직의 사무실은 적발을 피하기 위해 수시로 옮기고 있었다(〈사례6〉, 〈사례9〉, 〈사례10〉).

다음으로 보이스피싱 범행을 위한 대포통장, 피해자의 개인정보가 담긴 DB 등을 확보하였다((사례8〉). 대포통장의 경우 통장명의자가 보이스피싱 범행에 이용되는 것을 인지하였음에도 불구하고 통장을 빌려주는 사례가 있다. 그러나 본인도 모르는 사이에 대포통장으로 이용될 수도 있다. 참고로 중고거래 앱에서 중고물품 판매글을 올리고 직거래로 구매자에게 물품을 전달하고 본인 계좌로 돈이 입금되어 정상적인 거래라고 생각했지만, 전기통신금융사기 이용계좌로 신고되어 지급정지된 사례도 있었다(경찰청 내부자료). 이 연구에서 살펴본 판결문들에는 피해자의 개인정보가 담긴 DB를 불상의 방법으로 취득하였다고만 되어 있다(〈사례6〉 〈사례9〉, 〈사례10〉. 이는 하부 조직원 판결문이 대부분이기 때문이다.

마지막으로 변작중계기를 활용하는 경우도 있다. 보이스피싱 조직은 발신번호가 국제전화, 인터넷 전화 등으로 표시될 경우 보이스피싱 범행으로 의심하는 경우가 많아짐에 따라 우리나라에 발신번호 변작중계기를 설치, 이동통신사에 가입된 스마트폰의 전화·문자메시지 연동 기능 등을 이용하기도 한다. 이를 통해 외국에서 전화나 문자메시지를 발송하였음에도 국내 이동통신을 이용한 것처럼 가장될 수 있는 것이다(부산지방법원 2022고단4239).

나. 인적 구성

1) 조직원 구성 및 역할

보이스피싱 조직의 구성은 개별 조직에 따라 다를 수 있지만, 총책, 관리자급 조직원, 피해자에게 직접 전화하는 콜센터 상담원 업무를 담당하는 조직원, 현금 인출책이나 현금수거책 등으로 구분된다(〈사례6〉).

총책의 경우 조직을 구성, 대포통장을 사용할 경우 통장모집, 기관사칭하는 경우 가짜 홈페이지 사이트 개설·관리하는 역할 등을 담당하였다(사례10〉. 관리자급 조직원의 경우 신규 조직원 교육 및 관리 등을 담당한다(〈사례6〉, 〈사례8〉). 텔레마케터

(TM)의 경우 불특정 다수에게 문자메시지 발송 후 전화를 걸어온 사람들 상대로 수사기관 사칭하여 계좌가 범죄에 이용되었으니 지정 계좌에 자금 이체하라로 하는 등의 역할(〈사례14〉), 콜센터 상담원은 금융기관 등을 사칭하여 피해자에게 전화하는 역할(〈사례6〉,〈사례8〉), 현금 인출책은 국내 대포통장에 입금된 피해금을 (체크카드 등을 이용하여) 현금 인출하는 역할, 현금수거책은 피해자를 직접 만나 피해금을 수거하는 역할을 담당한다. 이 외에 피해자들이 이체한 금원을 전달받아 자금세탁 후 총책에게 전달하는 환전책(〈사례14〉) 등이 있다.

2) 조직원 가담경로

이 연구에서 살펴본 판결문을 통하여 TM(텔레마케티)과 현금수거책의 가담경로를 살펴보았다. 먼저 TM 가담경로를 보면 친구가 중국 보이스피싱 조직에서 일할 수 있도록 소개하고, 월 1-2천만원 벌 수 있다고 해서 중국 보이스피싱 콜센터 조직에서 일한 사례가 있었다(〈사례14〉).

현금수거책의 가담경로를 보면, 직접 사람으로부터 소개받은 경우(〈사례1〉, 〈사례7〉), 구인광고를 통한 가담 사례가 있다(〈사례3〉, 〈사례4〉, 〈사례12〉, 〈사례15〉). 구인광고는 문자메시지, 페이스북, 텔레그램, 인터넷 구직사이트, 생활정보지, 교차로 등 다양하였다. 이렇듯 다양한 구인광고를 통하여 보이스피싱 조직이 현금수거 등을 담당할 조직원을 찾는 것이다. 이와 관련하여 경찰청에서는 가짜 구인광고 게시자를 검거하기도 하였는데, 이 사례의 경우 전화금융사기 조직으로부터 구직사이트 기업회원 계정을 받아 고수익 아르바이트, 당일 지급 등을 빙자해 현금수거책 모집광고를 한 것이다.[107]

보이스피싱 조직이 현금수거책에게 제안한 내용을 보면, 부동산 최저 가격 조사업무(춘천지방법원 2021노680), 알려주는 장소로 가서 사람을 만나서 돈을 받아 알려주는 계좌로 입금(〈사례3〉, 〈사례7〉), 대출금 상환업무(〈사례15〉), 비대면 계좌개설 예약고객이나 권행대행 요청한 고객 만나서 확인 서명받는 것(〈사례4〉) 등이었다.

현금수거책에 대해서 통상적 채용절차는 거치지 않았다. 형식적인 신분확인만 하고

107) 경찰청 2022년 7월 17일 보도자료, "2022년 상반기 전화금융사기 발생·검거 현황 분석" (https://police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20220718094502653, 검색일: 2023년 6월 10일).

채용하였으며(〈사례5〉), 운전면허증, 주민등록번호 등을 모바일 앱을 이용해 성명불상자에게 송신하기만 하고, 면접이나 대면절차, 4대보험이나 근로계약서 작성 등은 없었다(춘천지방법원 2021노680). 다른 사례에서도 현금수거책이 채용과정에서 회사를 방문하거나 면접을 하지는 않았다(창원지방법원 2021노250).

3) 조직원 관리 및 교육

관리자급 조직원은 조직원의 여권을 보관하여 임의귀국을 막고, 협박 등을 통해 탈퇴를 방지한다(울산지방법원 2021고단4682). 또한 조직원 상호간에 가명을 사용하였다(〈사례8〉, 〈사례10〉, 울산지방법원 2021고단4682).

근무시간은 국내 금융기관 근무시간에 맞게 월-금요일 09:00-18:00로 한 경우(〈사례6〉), 09:00-17:00(〈사례8〉) 중국 현지시각 08:00-14:00(울산지방법원 2021고단4682) 등이 있었다. 업무시간 이후 숙소생활, 외출이나 외박 등은 제한적으로 허락되고 있었다(〈사례6〉).

조직원에 대한 교육을 보면, 범행시 피해자와 대화할 멘트가 기재된 매뉴얼 제공, 검사와 수사관 사칭 시 법률용어를 말하는 요령과 방법을 교육한 사례(〈사례10〉), 피해자로 하여금 파밍사이트에 접속하도록 유도하는 대화내용 등이 기재된 매뉴얼을 제공하고 교육하며, 업무 매뉴얼에 따라 약 2주간 교육받은 후 범죄에 투입한 사례가 있었다(부산지방법원 2022고단2648,3369,4459).

2. 범행실행단계

범행실행단계는 보이스피싱 유형별로 살펴보았다.

가. 대출사기형

1) 저금리 대출유도 후 기존 대출받은 기관 사칭하여 대출금 편취

① 금융기관 직원 사칭하여 전화(저금리 대출 등 제안)

이 유형의 범행단계를 보면 첫째, 금융기관 직원을 사칭하여 피해자에게 전화를 한다. 판결문 자료를 보면 금융기관은 은행 직원(〈사례1〉,〈사례4〉), 캐피탈 직원(〈사례

2〉,〈사례3〉) 등 구체적으로 표현된 경우도 있고, 금융기관 직원(〈사례6〉)이라는 표현으로 되어 있는 경우도 있다.

보이스피싱 조직원이 피해자에게 전화를 한 경우 저금리 대출(〈사례1〉,〈사례3〉,〈사례4〉), 저금리 정부지원자금 대출(〈사례2〉), 저금리 대환대출(〈사례5〉), 기존 대출금 일부 상환시 저금리 대환대출(〈사례6〉) 등을 제안하였다. 즉 대출사기형의 경우 피해자에게 저금리 대출을 제안하며 접근하는 것이다.

② 피해자 개인정보 파악을 위한 대출빙자 상담 혹은 휴대전화에 앱설치 등 요구

보이스피싱 조직원은 피해자에게 대출제안을 하면서 휴대전화에 앱 설치(〈사례2〉,〈사례3〉,〈사례4〉), 온라인 신청서 작성(사례5) 등을 요구한다. 이러한 요구에 피해자가 응할 경우 피해자의 기존 대출내역을 확인할 수 있게 된다(〈사례2〉,〈사례3〉,〈사례4〉,〈사례5〉).

③ 피해자 기존 대출내역 확인 후 기존 대출받은 기관 사칭하여 전화

피해자의 기존 대출내역을 확인한 경우 기존 대출받은 기관 직원을 사칭하여 피해자에게 전화한다(〈사례1〉,〈사례2〉,〈사례3〉,〈사례4〉,〈사례5〉). 이 연락을 통해 피해자가 새로 대출받는 것에 대해 계약 위반(〈사례1〉), 법 위반(〈사례2〉,〈사례3〉), 신용불량자로 등록되고 직장에 압류가 들어간다(〈사례2〉)고 하거나 기존 대출금 중 미면제 잔액을 상환해야 대출이 가능하다고 하면서(〈사례4〉,〈사례5〉) 기존 대출금의 상환을 요구한다. 대출금 상환방법으로는 주로 현금을 직접 받는 방법을 제안하며, 계좌송금을 요구하기도 한다.

④ 피해자가 기존 대출금 상환할 돈 마련

위의 내용을 들은 피해자는 급박한 상황으로 인식하고 기존 대출금을 상환할 돈을 마련한다.

⑤ 피해자로부터 피해금 편취(현금 대면편취 혹은 계좌송금)

보이스피싱범이 피해자로부터 피해금을 편취한다. 피해금 편취방법으로 우선 현금 대면편취가 있다. 이는 현금수거책이 금융기관 직원을 사칭하여 피해자를 직접 만나 피해금을 수거하는 것이다(〈사례1〉,〈사례2〉,〈사례3〉,〈사례4〉,〈사례5〉). 현금수거책은 조직원이 알려준 허위의 직책과 가명을 포함한 멘트를 생각하고 피해자를 만나며(〈사례5〉), 위조된 대출상환증명서를 교부하기도 한다(〈사례1〉). 여기서 살펴본 판결문을

보면 피해자에게 최초 전화후 현금을 수거한 날은 1일 뒤(〈사례2〉,〈사례3〉,〈사례4〉), 2일 뒤(〈사례1〉,〈사례5〉) 등이며, 피해자를 만나는 장소는 아파트 지하주차장(〈사례1〉), 병원주차장(〈사례4〉), 노상(〈사례2〉),〈사례3〉,〈사례5〉) 등이다. 즉 현금수거장소를 보면 사람들 눈에 띄지 않는 주차장이나 길거리 등이 주를 이루고 있다. 피해금 편취방법으로 또다른 방법은 피해자로부터 계좌송금(대포통장 명의자 계좌)을 받는 것이다. 여기에 해당하는 사례의 경우 최초 전화후 1일 뒤 송금을 받았다(〈사례6〉).

⑥ 현금수거책이 조직원이 지정한 계좌로 송금

현금 대면편취의 경우 현금수거책이 조직원이 지정한 계좌로 송금한다(〈사례1〉,〈사례2〉,〈사례3〉,〈사례4〉,〈사례5〉).

2) 저금리대출 등에 필요한 신용도 향상 혹은 고금리 대출기록 등을 이유로 대출금 편취

여기에 속하는 유형의 범행단계를 보면 다음과 같다.

① 금융기관 직원 사칭하여 전화(저금리 대출 등 제안)

앞의 유형과 마찬가지로 보이스피싱 조직원이 금융기관 직원을 사칭하여 피해자에게 전화한다. 이 때 코로나19관련 대환대출(〈사례7〉), 저금리로 마이너스통장 이용(〈사례8〉) 등을 제안한다.

② 대출상담 빙자하여 피해자의 개인정보 파악

대출가능 여부 등을 확인하기 위한 이유로 피해자의 개인정보를 파악한다.

③ 신용도 향상 혹은 고금리 대출기록이 필요하다며 카드론 대출받아 변제하라고 요구

보이스피싱 조직원은 피해자에게 저금리 대출 등을 위해서는 신용도 향상 혹은 고금리 대출기록이 필요하다고 하며, 카드론 대출을 받아 카드사에 변제할 것을 요구한다(〈사례7〉,〈사례8〉).

④ 피해자 카드론 대출받음

⑤ 피해자 대출금 편취

앞의 유형과 마찬가지로 피해금을 편취하는 방법으로는 현금 대면편취와 계좌송금이 사용된다. 전자의 경우 카드사 직원을 사칭하여 피해금을 편취(위조된 대출금완납

증명서 사용)하였으며, 최초 전화후 1일뒤 노상에서 피해자를 접촉하였다(〈사례7〉). 후자의 경우 피해자가 조직원이 지정한 계좌(대포통장)로 송금하였다(〈사례8〉).

⑥ 현금수거책(혹은 현금인출팀)이 보이스피싱 조직에 피해금 전달

현금수거책의 경우 조직원이 지정하는 계좌에 송금(〈사례7〉)하거나 현금인출팀이 대포통장과 연결된 체크카드를 이용하여 현금인출 후 보이스피싱 총책에게 전달하게 된다(〈사례8〉).

나. 사칭형

1) 기관사칭형

가) 수사기관 사칭하여 전화한 후 수사목적(혹은 피해방지)을 빙자하여 피해금 편취

① 수사기관 사칭하여 전화(피해자 계좌의 범죄 이용 등 언급)

먼저 보이스피싱조직원이 수사기관을 사칭하여 피해자에게 전화하게 된다. 사칭하는 수사기관을 보면, 서울중앙지방검찰청 검사와 수사관 사칭(〈사례9〉, 〈사례10〉), 사이버수사대 경찰과 검사 사칭(〈사례11〉), 경찰 및 검사사칭(〈사례12〉, 검사사칭(〈사례13〉) 등이 있다. 수사기관을 사칭하여 전화하는 경우 주로 피해자 계좌가 범죄에 이용되었다고 하였다(〈사례9〉,〈사례10〉,〈사례11〉,〈사례12〉,〈사례13〉).

② 수사목적의 앱 설치나 유선조사 등을 통한 피해자 개인정보 파악

여기서 살펴 본 사례들을 보면, 가짜 검찰청 사이트로 접속하게 하여 실제 사건이 접수되어 수사 중인 것처럼 표시(〈사례9〉), 수사협조의뢰서 발송(〈사례13〉) 등을 통하여 피해자로 하여금 실제 수사기관인 것처럼 믿게 만드는 방법도 이용되었다. 또한 가짜 경찰청 앱 설치(〈사례11〉), 앱 설치 및 공인인증서 발급 후 비밀번호 요구(〈사례12〉), 유선조사를 진행하며, 혐의점 발견시 소환조사나 영장 발부될 수 있음을 언급(〈사례10〉)하는 사례들이 있었다.

이러한 단계를 통해 피해자로 하여금 진짜 수사기관으로 믿게 만들 수 있고, 수사목적의 조사를 빙자하여 피해자의 개인정보를 얻게 된다.

③ 수사(혹은 추가피해 방지)를 빙자하여 피해자 계좌에 있는 돈(혹은 신규 대출,

상품권 핀번호 등) 요구

이 단계를 구체적으로 보면, 신용정보가 조작되어 범죄에 이용되고 있는지를 알아보기 위한 대출 요구(대출이 될 경우 개인정보 유출로 검수가 필요하니 대출금을 현금으로 인출하라고 함)(〈사례9〉), 추가 피해 막기 위한 피해자 명의 계좌 돈 현금 인출 요구(〈사례10〉), 수사재연을 위한 상품권 결제 요구 등이 있다.

한편 피해자의 개인정보를 알아내어 피해자명의로 몰래 대출받은 사례도 있다(〈사례12〉).

④ 피해자 돈 편취

편취방법으로는 수사관 및 금융감독원 직원에게 직접 전달(〈사례9〉), (금융감독위원회 등 명의) 계좌송금(〈사례11〉), 물품 보관함에 보관(〈사례10〉), 상품권 핀번호 요구(〈사례13〉) 등이 있다. 한편 피해자 몰래 대출받은 후 해당 돈을 금융감독원에서 자금 세탁하려는 돈을 찾아내어 피해자 통장에 입금한 것이라고 하면서 피해자로부터 편취한 사례도 있다(〈사례12〉).

현금 대면편취의 경우 현금수거책이 수사관(〈사례14〉), 금융감독원 직원 등을 사칭하여 피해자를 만나며, 시기적으로는 최초 전화한 당일에 이루어진 경우도 있었다(〈사례9〉,〈사례10〉,〈사례12〉). 장소를 보면 대출사기형과 마찬가지로 아파트 부근(〈사례9〉), 택시승강장 앞(〈사례12〉)과 같이 노상에서 이루어졌다. 피해자를 직접 만나는 경우 위조된 금융범죄 금융계좌추적 민원서류를 교부하기도 하였다(〈사례12〉).

⑤ 현금수거책(혹은 현금인출팀)이 보이스피싱 조직에 피해금 전달

계좌송금의 경우 현금인출책이 현금을 인출하여 조직원에 건네고, 이 조직원은 환전소를 통해 보이스피싱 조직원에 송금하였다(〈사례11〉). 현금 대면편취의 경우에는 현금수거책이 보이스피싱 총책이 지정한 계좌로 송금(〈사례12〉)하는 방식으로 피해금이 조직에 전달되었다.

나) 피싱문자 발송후 연락온 피해자에게 수사기관 사칭하여 피해금 편취

① 피싱문자 발송

이 유형의 경우 우선적으로 피해자들에게 (해외)결제 승인문자 등 피싱문자를 발송한다(〈사례14-1〉,〈사례14-2〉,〈사례15-1〉,〈사례15-2〉).[108]

② 피해자가 문자보고 전화하면 수사기관 연결(혹은 대신 신고)해 준다고 함

피해자가 문자를 보고 결제 사실이 없다고 전화하면 KG모빌리언스, 아마존닷컴 직원 등을 사칭하여 개인정보가 유출되었거나 계좌가 범죄에 이용되었을 것이라고 알려준다. 이와 관련하여 수사기관을 연결(혹은 대신 신고)해 준다고 한다(〈사례14-1〉,〈사례14-2〉,〈사례15-1〉,〈사례16〉).

③ 수사기관 사칭하여 전화(개인정보 유출 혹은 계좌의 범죄이용 언급)

수사기관을 사칭하여 피해자에게 전화하는데, 사칭한 수사기관을 보면, 영등포경찰서 수사과장, 서울지방경찰청 수사과장(〈사례14-1〉), 서울지방경찰청, 금융감독원, 검찰청(〈사례14-2〉), 인천서부경찰서 이상화경위(〈15-1〉), 경찰(〈사례16〉) 등이 있다. 한편 일부 사례들에서는 수사기관과 더불어 금융감독원 직원을 사칭하는 경우들이 있었다(〈사례15-1〉, 〈사례15-2〉).

피해자에게 전화하면서 피해자의 개인정보 유출(〈사례14-1〉), 피해자 명의계좌가 대포통장으로 이용(〈사례14-2〉)되었다는 것을 언급한다. 또한 금융감독원 직원을 사칭한 사례들에서는 피해자 명의가 도용되어 많은 피해자들이 발생했고, 이들이 피해자를 고소한 상태라고도 하였다(〈사례15-1〉, 〈사례15-2〉). 이러한 상황을 제시할 경우 피해자의 이성적이고 합리적 판단을 어렵게 만들 수 있을 것이다.

④ 수사목적의 앱 설치 등 요구

수사목적의 앱 설치를 요구하는 경우들이 있다(〈사례14-2〉,〈사례15-1〉). 이러한 앱 설치를 통하여 피해자의 개인정보를 파악하게 된다.

⑤ 수사(혹은 추가피해 방지)를 빙자하여 피해자 계좌에 있는 돈(혹은 신규 대출) 요구

보이스피싱 조직원은 피해자에게 대포통장으로 사용된 계좌의 현금을 인출하여 금융감독원 직원에게 보여주면 일련번호 확인후 다시 입금해 준다고 하거나(〈사례14-2〉), 혹은 추가피해를 막기 위해 돈을 보관(〈사례 14-1〉,〈사례16〉), 신용한도만큼 대출받아 보관(〈사례15-2〉)할 것을 요구한다.

⑥ 피해자 돈 편취

---

108) 우체국 직원을 사칭하여 해외에서 카드사용이 되었다고 하며 전화한 사례도 있는데(〈사례16〉), 수법이 비슷하므로 여기에 같이 포함하였다.

피해자로부터 돈을 편취하는 방법은 다른 유형과 유사하게 현금 대면편취(〈사례14-1〉,〈사례14-2〉,〈사례15-1〉,〈사례15-2〉), 물품보관함에 두게 하고 꺼내어 가는 방법(〈사례16〉) 등이 있다. 현금 대면편취의 경우 현금수거책이 금융감독원 직원 등을 사칭(〈사례14-2〉)하여 피해자를 만나 직접 현금을 받는 방식으로 이루어진다. 현금수거책이 피해자를 만나는 시기는 최초 전화한 당일(〈사례14-2〉), 3일후(〈사례14-1〉), 6일 후(사례15-2〉) 등이었으며, 피해자 접촉 장소는 초등학교 앞(〈사례14-1〉,〈사례15-2〉), 빌라앞 골목길(〈사례14-2〉), 아파트 지하주차장(〈사례15-1〉) 등이었다. 현금 대면편취의 경우 위조된 금융범죄 금융계좌추적 민원서류를 교부하기도 하였다(〈사례15-2〉).

⑦ 현금수거책이 조직원이 지정하는 사람에게 전달

판결문에서 파악된 자료를 보면, 현금 대면편취의 경우 현금수거책이 조직원이 지정한 사람에게 피해금을 전달하였다(〈사례15-1〉,〈사례15-2〉).

2) 가족·지인 사칭형

① 인터넷 메신저를 통해 연락

피해자의 가족이나 지인을 사칭하는 보이스피싱의 경우 인터넷 메신저를 통해 연락하였다(〈사례17〉,〈사례18〉).

② 요청 사항 제시(앱설치 후 개인정보 알려달라고 하거나 대신 결제 부탁)

자녀나 지인을 사칭하는 경우 피해자에게 요청 사항을 제시하는데, 자녀를 사칭하는 경우 휴대폰 단말기 파손으로 보험금 청구하는데 필요하니 휴대폰 원격제어 프로그램 앱을 설치하도록 요청하였다(〈사례17〉). 이 사례의 경우 앱 설치 후 계좌번호와 비밀번호를 알려달라고 하였다. 지인을 사칭한 경우에는 급하게 결제할 곳에 있는데 오류로 되지 않으니 대신 결제를 부탁하였다(〈사례18〉).

③ 피해자가 요청사항 이행(앱설치 및 개인정보 알려주거나 대신 계좌송금)

피해자가 앱설치 후 개인정보를 알려준 경우 보이스피싱 조직원이 피해자의 정보를 이용하여 은행계좌 접속 후 타 계좌(대포통장)로 송금하였다(〈사례17〉). 피해자에게 대신 결제를 부탁한 경우에는 피해자가 직접 대포통장으로 계좌송금을 하였다(〈사례18〉).

④ 현금인출책이 현금인출하여 보이스피싱 조직책에 계좌송금

보이스피싱 조직원은 대포통장에 현금이 입금된 것을 확인한 후 현금인출책에게 현금을 인출하도록 지시한다(대포통장 명의자 체크카드와 비밀번호 이용). 현금인출책은 현금을 인출한 후 보이스피싱 조직책 혹은 조직원이 지시하는 계좌로 송금하게 된다(〈사례17〉,〈사례18〉).

3. 소결

보이스피싱 범행단계별 특성은 판결문과 경찰내부자료, 언론보도자료 등을 토대로 살펴보았다. 보이스피싱 범행준비단계의 경우, 조직 및 물적·인적 구성, 조직원 교육 및 관리 등이 있었고 보이스피싱 총책이 조직을 만들고 사무실 및 집기 등 물적 기반을 마련하게 된다. 물적 기반에는 피해자 개인정보가 담긴 DB, 계좌송금 편취방식의 경우 대포통장 모집, 사례에 따라 변작중계기 등이 포함될 수 있다. 인적 구성을 보면, 총책과 관리자급 조직원, 콜센터상담원(혹은 텔레마케터), 현금인출책(혹은 현금수거책), 환전책 등이 있다. 조직원 가담경로를 보면 텔레마케터와 현금수거책의 경우 주변 사람의 소개도 있지만 다양한 매체의 구인광고를 보고 가담한 경우가 많았다. 조직원에 대한 교육은 구체적인 범행방법이 담긴 매뉴얼을 통하여 이루어지고 있는 것을 확인할 수 있었다.

범행실행단계는 보이스피싱 유형별로 살펴보았으며, 보이스피싱 유형은 대출사기형과 사칭형(기관사칭형, 가족·지인사칭형)으로 구분하였다. 대출사기형의 범행실행단계는 금융기관 직원을 사칭하여 피해자에게 전화해서 저금리 대출 등을 제안→피해자의 개인정보 등을 파악할 수 있는 상담 혹은 휴대전화 앱설치 요구→피해자 대출내역 확인→피해자가 기존에 대출받은 금융기관 직원 사칭하여 전화해서 계약위반, 법위반 등이라고 하며 기존 대출금 상환요구→피해자로부터 피해금 편취(현금수거책이 대면편취 혹은 계좌송금)→현금수거책(혹은 현금인출책)이 조직원이 지정한 계좌로 송금 등으로 이루어진다. 대출사기형 중 저금리대출을 위한 신용도 향상(고금리 대출기록)을 이유로 대출금을 받게 한 후 편취하는 사례도 있었다.

사칭형 중 기관사칭형의 범행실행단계를 보면 수사기관을 사칭하여 피해자에게 전화해서 피해자 계좌의 범죄이용 등을 말함→수사목적의 앱설치 혹은 유선조사 등을

통하여 피해자 개인정보 파악 → 수사(혹은 추가피해방지)를 빙자하여 피해자 계좌에 있는 돈(혹은 신규 대출, 상품권 핀번호 등) 요구 → 피해자 돈 편취(대면편취/계좌송금/물품보관함이용) → 현금수거책(혹은 현금인출책)을 통해 조직원이 지정한 계좌로 송금 등으로 이루어진다. 기관사칭형 중 피싱문자(해외 결제 승인문자 등) 발송을 포함한 사례의 경우 피싱문자 발송 후 연락온 피해자에게 업체 직원 등을 사칭하여 명의도용(계좌범죄 이용)을 언급하며 수사기관을 연결해 주고, 수사기관을 사칭하여 피해금을 편취하는 방식으로 이루어지고 있었다. 가족·지인사칭형은 인터넷 메신저를 이용하며 요청사항(앱설치 및 계좌번호와 비밀번호 요청, 대신 결제 등)을 제시하고 피해자가 이를 이행하면 피해자 정보를 이용하여 피해자 계좌에서 직접 돈을 빼 가거나 피해자가 (대포통장으로) 계좌송금한 것을 편취하는 단계로 이루어지는 것을 확인할 수 있었다.

이상의 범행단계별 특성을 토대로 시사점을 제시해보면, 먼저 범행준비단계와 관련하여 첫째, 개인정보 유출에 대한 엄격한 단속이 필요할 것이다. 이 연구에서 살펴본 판결문에 의하면, 개인정보가 담긴 DB를 불상의 방법으로 취득하여 보이스피싱 범행에 사용하고 있었다. 참고로 개인정보를 범죄조직에 판매한 개인정보 관리자가 검거된 경우도 있다. 2020년 3월 쇼핑몰 상품판매 및 배송, 고객응대 목적으로 수집한 개인정보를 범죄조직에 판매한 개인정보 관리자가 검거되었다. 경찰청 자료에 의하면 우연히 취득한 타인의 개인정보를 범죄조직에 넘긴 경우가 많으나 기업 등에서 고객정보에 접근가능했던 개인정보 관리자, 신용정보를 합법적으로 조회할 수 있었던 대부업자도 있는 것으로 나타났다.[109] 따라서 개인정보 유출에 대한 철저하고 확실한 단속이 필요할 것이다.

둘째, 현금수거책 등 조직원 가담을 막기 위하여 구직사이트 등에 대한 엄격한 관리가 필요할 것이다. 이 연구에서 살펴본 판결문을 보면, 현금수거책은 주로 구직광고를 통하여 보이스피싱범죄에 가담하였다. 참고로 선행연구에서도 보이스피싱 전달책의 가담경로 중 구직사이트가 70.6%로 가장 많았으며, 지인소개가 15.3%, SNS가 6.4% 등이었다.[110] 따라서 구직사이트에 대한 관리가 필요하다. 구직자 입장에서도

109) 경찰청 2022년 7월 17일 보도자료, "2022년 상반기 전화금융사기 발생·검거 현황 분석 (https://police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20220718094502653, 검색일: 2023년 6월 10일).

110) 홍동규·홍순민·김한결, 보이스피싱 전달책의 가담경로에 관한 연구, 경찰학 연구 제20권 제1

일반적인 채용절차를 거치지 않는 경우, 과도한 보상, 현금수거 역할 등을 제안하는 경우 보이스피싱 조직일 수 있다는 점을 인식하고 경계하는 것이 중요하다.

다음으로 범행실행단계와 관련하여 첫째, 예방교육이 중요할 것이다. 이 연구에서 살펴본 판결문에 의하면 수사기관, 금융기관을 사칭하여 전화한 경우, 피싱문자를 발송한 경우들이 주를 이루는데 이에 대한 경각심을 갖고 올바른 지식을 갖도록 교육을 강화하는 것이 중요할 것이다. 앞에서 본 사례들을 보면, 현금수거책이 피해자에게 위조된 대출상환증명서(대출사기형), 금융범죄 금융계좌추적 민원서류(기관사칭형) 등을 교부하고 현금을 편취하는 경우들이 있다. 금융기관이나 수사기관에서 서류를 (노상 등에서) 직접 만나 교부하는 일이 없다는 점, 무작위 대출(지원금)·투자문자는 100% 피싱이라는 점, 자녀나 지인사칭의 경우 목소리를 반드시 확인하는 것이 필요하다는 점, 백신설치 강조, 출처가 불분명한 문자의 URL을 누를 경우 악성앱이 설치될 수 있다는 점, 금융기관이나 수사기관의 전화를 받았다면 직접 전화번호를 검색해서 확인전화해야 한다는 점 등 예방교육이 보다 적극적으로 이루어져야 할 것이다.[111] 참고로 선행연구에 의하면, 보이스피싱을 당할 뻔했으나 당하지 않는 확률에는 재무지식 심화점수가 높은 경우, 금융사기 예방교육을 받은 경우가 정적(+)으로 유의한 영향을 주는 것으로 나타났다.[112] 보이스피싱 피해를 당하지 않기 위해 필요한 지식과 더불어 보이스피싱 유형별·단계별 대응방안을 체계적으로 알려주는 것도 필요할 것이다.

둘째, 피싱문자 근절을 위한 대책이 중요할 것이다. 기관사칭형 유형 중 하나는 피싱문자를 발송한 후 이를 보고 전화한 피해자들을 대상으로 한 사기였다. 이러한 피싱문자 근절을 위하여 금융기관과 공공기관에서 발송한 정상적 문자를 수신자가 확인할 수 있게 하기 위해 안심마크(인증마크+안심문구)표시 서비스를 시범 도입하였다(2022년 10월). 이러한 안심마크표시 서비스에 대해 일반인이 알 수 있도록 홍보하는 것과 더불어 서비스 도입기관이 확대될 필요가 있다.

호, 2020, 114면.

111) 국무조정실 2022년 9월 29일 보도자료, "보이스피싱 범죄근절을 위한 통신·금융분야 대책 발표"((https://www.fsc.go.kr/no010101/78643, 검색일: 2023년 6월 10일).

112) 김민정·김은미, 보이스피싱 피해경험 및 영향요인 분석, 소비자문제연구 제52권 제1호, 2021, 67면.

셋째, 원격조종 앱 설치를 차단할 수 있도록 하는 노력이 중요할 것이다. 이 연구에서 살펴본 사례들을 보면 보이스피싱 조직원이 수사기관을 사칭하여 피해자에게 '팀뷰어 퀵서포트'(TeamViewer QuickSuppor) 앱을 설치하게 한 경우들이 있었다. 휴대전화에 이 앱을 설치할 경우 휴대전화의 아이디가 부여되며 이를 보이스피싱 범죄자에게 알려주면, 범죄자는 이 아이디를 이용해서 피해자 휴대전화를 원격으로 모니터링하고 임의로 파일 전송받는 것 등이 가능하다.[113] 이와 관련하여 금융회사들에서는 금융회사 앱 구동시 원격조정 앱이 연동되는 것을 차단하고 있다. 또한 금융보안원에서는 금융회사들을 대상으로 이러한 내용을 점검하고 있다.[114] 모든 금융기관을 대상으로 금융기관 앱 구동시 원격조정 앱이 차단될 수 있도록 할 필요가 있다. 다만 원격조정 앱도 계속적으로 다양하게 나타나는 점 등을 고려할 때 엄격한 본인승인 절차 등을 거치게 하는 것 등 최소한의 제한도 고려해 볼 필요가 있다.[115]

제3절 | 보이스피싱 범죄 수법 변화 진단

1. 범죄 수법 변화

가. 과거부터 지속되고 있는 유형

보이스피싱은 범죄조직이 전화를 걸거나, SMS등을 발송하여 피해자를 기망,대포통장으로 송금 및 이체하게 하거나, 금융정보를 편취하여 금원을 편취하는 방법이 가장 기본적이고 공통적인 방법이고, 그 당시 시기와 상황에 따라 조금씩 유형과 방식이 바뀌게 된다.[116] 위에서 살펴본 바와 같이, 보이스피싱 발생 초기에는 범행 수법이

113) 김경진·서준배, 앞의 글, 123면.
114) 국무조정실 2022년 9월 29일 보도자료, "보이스피싱 범죄근절을 위한 통신·금융분야 대책 발표" 별표1(https://www.fsc.go.kr/no010101/78643?srchCtgry=&curPage=2&srchKey=cn&srchText=%EB%B3%B4%EC%9D%B4%EC%8A%A4%ED%94%BC%EC%8B%B1&srchBeginDt=&srchEndDt=, 검색일: 2023년 6월 10일).
115) 김경진·서준배, 앞의 글, 124면.
116) 차영민·송영시, "보이스피싱 범죄의 실태와 피해자의 손해보전 방법에 관한 소고", 법학논총 제21권 제2호, 2014, 537면 참조.

많이 알려지지 않아 그 피해가 크게 나타났다. 대부분 보이스피싱 조직원은 피해자에게 전화를 걸어 다양한 기관 또는 지인 등을 사칭하며 피해자를 기망하는 것을 바탕으로 범죄가 이루어졌다. 조직 내부는 총책, 텔레마케터, 수거책, 모집책, 인출책 등으로 구분되어 유기적으로 움직이며 끊임없이 피해를 발생시켰다.

하지만 피해자를 기망해 대포통장으로 금전 송금을 유도하는 가장 기본적인 수법은 정부 및 수사기관의 대응방안을 피하기 쉽지 않았고, 이에 조직원들은 대응방안을 교묘히 빠져나가면서 또, 피해자가 많이 속을 수 있는 새로운 범죄 유형을 계속해서 변화시키며 끊임없이 피해를 양산하고 있다.

나. 최근 발생 및 증가하고 있는 유형

1) 중계기, SIM박스 활용

보이스피싱 전화가 국제전화 또는 070 인터넷 전화로 많이 걸려온다는 사실이 알려지면서, 전화를 받지 않는 사람들이 늘어나자 중계기를 이용해 010으로 전화번호를 변작하여 접근하기 시작했다. '010'번호로 변작해주는 VoIP게이트웨이 장치와 심박스를 사용하여 번호 변작과 함께 국제전화의 고가 요금을 회피하는 용도로 피싱 범죄에 악용된다.[117]

초기에는 단속을 피하기 위하여 중계기를 눈에 잘 띄지 않는 지하실, 공사현장, 산악지대, 주차장 등에 설치하였으며, 여러 장소에 설치해두어 한 장소가 발각되어도 다른 장소에 거치된 심박스를 계속 사용할 수 있도록 했다.[118] 하지만 최근에는 중계기 단속을 최대한 피하기 위해서 이동식 중계기를 설치하여 이를 움직여 줄 운반자를 모집하기 시작했다. 차량 트렁크나 오토바이에 넣고 이동하는 방법부터, "직접 중계기를 들고 다니며 추적을 피하는 '인간 중계기'까지 등장"했다.[119]

"A씨는 '중고 휴대전화를 여러개를 구매해서 지하철을 매일 타고다니면 일당으로

117) 김시윤·이용걸·이범주, "전기통신금융사기 대응 방안에 관한 연구 : 보이스피싱 담당 경찰관의 관점으로", 치안정책연구 통권 57호, 2022, 351면 참조.
118) 김시윤·이용걸·이범주, "전기통신금융사기 대응 방안에 관한 연구 : 보이스피싱 담당 경찰관의 관점으로", 치안정책연구 통권 57호, 2022, 353면 참조.
119) MBN뉴스, "'달리는 오토바이'가 보이스피싱 중계기···수법 기상천외", 2022.10.18. https://www.mbn.co.kr/news/society/4865043 (최종검색일 : 2023. 08. 05.) 참조.

2~30만 원을 주겠다'는 제안을 받고 4개월 동안 지하철로 수도권 전역을 돌아다니면서 중계기를 이동"시켰다.[120] '알뜰폰 통화품질테스트'나 '수신호 업무'라고 안내하며, 단순 업무를 가장한 아르바이트를 모집하는 등 본인이 하는 일이 '인간 중계기' 업무인지 모르고 피싱범죄에 도움을 주는 사람도 많이 발생하고 있다.[121]

중계기 단속으로 발신번호 변작이 어려워진 이후에는 공공기관 또는 금융기관을 사칭해 전화를 거는 사기수법 대신 가족 또는 지인을 사칭하여 SNS로 피해자와 통신하는 메신저 피싱이 증가하는 결과가 발생하기도 했다.[122]

2) 비대면 금융거래를 이용한 수법

① 비대면 중고거래를 활용한 수법 : 코로나19 이후 비대면 중고 거래가 활성화되면서 비대면 결제를 이용한 피싱 범죄도 함께 증가했다. 온라인으로 중고거래를하고, 최대한 먼 지역을 말하며 택배거래와 네이버 안전거래를 제안 한다.[123] 사기범이 보내준 링크로 들어가면 미리 만들어둔 가짜 안전거래 결제 창으로 들어가지고, 여기에 돈을 입금 하도록 유도하는 수법이다.[124]

② 알뜰폰 개통 후 신용카드 발급 수법 : 고금리로 어려워진 서민들에게 '급전을 마련할 수 있는 방법'으로 유혹하여 대출 서류로 신분증, 범용인증서 또는 선불 유심칩 등을 요구하고, 이를 활용해 휴대전화를 개통한 후, 미리 받아 둔 피해자의 개인정보, 새로 개통한 휴대폰을 이용하여 피해자도 모르는 사이에 신용카드 결제를 하거나 대출을 받아 빚더미에 앉게 만드는 수법이다.[125]

코로나19 이후 비대면 금융과 최근 알뜰폰 사용자가 증가하면서 알뜰폰 업체가

---

120) SBSNEWS, "[단독] "보이스피싱 중계기 직접 들고 지하철로 수도권 일주"...신종 수법 '덜미'", 2023.01.05. https://news.sbs.co.kr/news/endPage.do?news_id=N1007034063&plink=ORI&cooper=NAVER (최종검색일 : 2023.08.05.) 참조.

121) 서울동부지방법원 이은미 변호사, 2023.08.14., 보이스피싱 범죄 유형 관련 인터뷰 참조.

122) 최형욱·이상진, "피싱 범죄의 현황과 대응 방안 모색", 치안정책연구 통권 60호, 2022, 117면 참조.

123) YTN, "조직적 중고 거래 사기 '사이트 피싱'...피해규모와 대책은?", 2022.11.14. https://www.ytn.co.kr/_ln/0115_202211141310206433 (최종검색일 : 2023. 08. 26.) 참조.

124) YTN, "조직적 중고 거래 사기 '사이트 피싱'...피해규모와 대책은?", 2022.11.14. https://www.ytn.co.kr/_ln/0115_202211141310206433 (최종검색일 : 2023. 08. 26.) 참조.

125) 서울신문, "비대면의 역설... 명의 도용 대포폰·신용카드로 나도 모르게 '빚더미'", 2023.05.23. https://www.seoul.co.kr/news/newsView.php?id=20230523002004&wlog_tag3=naver (최종검색일 : 2023. 08. 26.) 참조.

많이 증가하면서, “직접 통신사 대리점을 방문하지 않아도 인터넷으로 주문만 하면 유심칩을 받아서 스마트폰을 개통”할 수 있게 되었고, 이는 통신업자까지 범죄에 가담하게 하는 등 보이스피싱이 더 활발하게 이루어지는 결과를 가져오게 되었다.[126]

③ 유튜브 금융직원 사칭 : 유튜브를 통해 정보를 얻는 사람이 증가하면서, 금융정보 관련 채널을 운영하는 유튜버도 함께 늘어났다. 이에 금융직원을 사칭한 유튜버가 ‘많은 이자를 받을 수 있는 금융상품 소개 영상’을 업로드하고 고정댓글로 남겨둔 링크를 통해 피해자들의 개인정보 등을 편취하는 수법이 발생했다.[127]

남녀노소를 불문하고 유튜브 사용자가 증가하고 있으므로, 더 큰 피해가 생기지 않도록 관련 유형에 대한 각별한 주의와 대응방안 마련이 필요할 것으로 보인다.

3) 오픈뱅킹·간편송금을 이용한 수법

2015년 2월 ‘토스’를 시작으로 네이버페이, 카카오페이 등 비밀번호와 지문인증으로 송금할 수 있는 간편송금 서비스 업체가 생겨나기 시작했고, 이용건수는 해가 갈수록 증가하고 있다.[128] 오픈뱅킹을 활용하면 상대방 계좌번호가 필요하지 않은 간편한 송금 방식이 가능하며, 조직원은 피해자를 기망하여 간편송금을 통해 돈을 송금하도록 유도하거나, 수거책 또는 전달책의 계좌로 돈을 먼저 송금받고 간편송금을 이용해 다른 계좌로 피해금을 회수하는 방법 등을 사용하는 등의 ‘편리함을 악용하는 범죄’가 발생했다.[129]

오픈뱅킹·간편송금을 이용한 피싱범죄의 경우, “피해금이 단기간에 다수의 계좌를 거쳐 빠르게 이전되면서 신속한 지급정지가 어렵고, 카카오페이와 같은 선불업자는 금융업자가 아니기 때문에 보이스피싱 관련 의무와 책임을 지니고 있지 않아” 지급정지가 어렵다는 문제가 있다.[130]

---

126) 서울신문, 위의 기사 참조.

127) SBSNEWS, “[친절한 경제] 이젠 유튜브도 신경써서 봐야해?...‘고정댓글 피싱’ 주의”, 2023.02.09. https://news.sbs.co.kr/news/endPage.do?news_id=N1007073359 (최종검색일 : 2023. 08. 29.) 참조.

128) 머니투데이, “폭증하는 간편송금 시장...토스·카카오가 97%장악”, 2018.08.14. https://news.mt.co.kr/mtview.php?no=2018081410305678343 (최종접속일 : 2023.08.15.) 참조.

129) 매일경제, ““편해서 좋았는데”···보이스피싱 타깃된 간편송금, 피해대책 나왔다”, 2023.07.25. https://www.mk.co.kr/news/economy/10793349 (최종검색일 : 2023.07.29.) 참조.

130) 일요서울, “[심층취재]‘신종 보이스피싱’ 오픈뱅킹·간편송금 등 ”돈 되찾기 더 어려워“ 사기수법 지능화”, 2023.08.07. http://www.ilyoseoul.co.kr/news/articleView.html?idxno=477290

4) 소상공인 통장협박 수법

보이스피싱 대응 방안으로 시행된 '지급정지'제도를 악용한 수법으로 최근 발생하기 시작했다. 자영업자는 계좌가 공개되어 있는 경우가 많은데, 사기범은 이와 같이 공개되어 있는 계좌를 이용해서 보이스피싱 피해금을 자영업자 통장에 이체하고, 자영업자에게는 "돈을 잘못 입금했다."라고 기망하여, 금전을 송금 받게 된다. 그 사이에 진짜 보이스피싱 피해자는 경찰에 신고하고, 지급정지를 신청하면서 송금 기록이 있는 자영업자도 함께 지급정지를 당하게 된다. 이후 사기범은 자영업자에게 돈을 보내주면 지급정지를 풀어준다고 협박하면서 금전을 편취하기도 한다.[131]

사기범은 검거의 위험이 있어 대포통장으로 바로 송금을 받는 대신, 타인 명의 계좌를 이용하여 작업하고, 요청한 대로 금원을 송금해도 피해금 환급절차가 종료되는 기간까지 약 3개월 동안 지급정지 절차는 풀리지 않아 자영업자는 영업에 큰 지장이 생기게 된다.[132]

2. 조직원 모집 수법 변화

가. 조직 역할별 모집방법

1) 총책, 텔레마케터

대부분의 총책 및 텔레마케터는 해외에 사무실을 두고 조직을 운영하고 있지만, 한국인을 상대로 범행을 저지르기 때문에 자연스러운 억양과 말투를 구사할 수 있는 한국사람들, 국내에서 중국으로 간 사람들, 특히 조선족 중에서 한국생활 경험이 있는 등의 한국에 대한 이해와 경험이 있는 사람들을 중심으로 구성되어 있다.[133]

(최종검색일 : 2023. 08. 28.) 참조.

131) 금융감독원 보도자료, "제2차 금융분야 보이스피싱 대책 발표", 2023.02.28. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=58200&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=1 (최종검색일 : 2023. 07. 09.) 참조.

132) 금융감독원 보도자료, "제2차 금융분야 보이스피싱 대책 발표", 2023.02.28. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=58200&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=1 (최종검색일 : 2023. 07. 09.) 참조.

133) 서울동부지방법원 이은미 변호사, 2023.08.14., 보이스피싱 범죄 유형 관련 인터뷰 참조.

텔레마케터를 모집하는 방법으로는 주로 인터넷카페, SNS, 구인구직 사이트 등을 통해서 모집하거나, 이미 보이스피싱 조직에 속해 있는 조직원들이 지인으로 있어서 소개로 일을 시작하게 되는 경우도 있으며, 산둥반도, 칭다오 등에 있는 다른 조직에서 스카우트를 해오는 경우도 있다.[134] 대학생들의 경우, '방학동안 중국에 가서 고액 알바하고 오면 큰 돈을 벌 수 있다.'라는 말에 현혹되어 서로 소개를 해주기도 한다.[135]

해외본부에서 일하는 유인책의 경우 금융기관직원, 경찰, 지방대학교수, 군인 등 생각보다 직업이 다양하며, 국내에서 생활하기 어렵거나, 가족의 병원비를 마련하기 위해, 일신에 문제가 생겨 쫓기는 사람 등이 범죄에 가담하게 된 사유라는 것을 살펴볼 수 있었고, 대부분은 과도한 채무가 있다는 것을 알 수 있었다.[136]

이들이 조직원으로 일하기 위해서 중국으로 넘어가면 조직원들은 여권을 뺏고 신원보증을 이유로 미리 받아둔 이력서를 통해 가족 연락처 등을 이용해 협박을 하기도 한다.[137]

2) 인출책, 수거책, 모집책

보통 인출책, 수거책, 모집책은 크게 명품구매대행, 채권추심아르바이트, 단순 배달 업무로 구분할 수 있으며, 보통 신용정보회사나 추심회사를 가장하여 채무자로부터 돈을 받아오는 일을 지시하거나, 단순 서류나 물건을 받아오는 것이라고 하는 경우가 대부분이고, 도박사이트 자금세탁에 대한 지시를 내리기도 한다.[138]

'알바몬' 또는 '벼룩시장' 등에서 단기고액알바 구직자를 모집하고, 초기에는 '시장조사가 필요하니 어느 위치에 가서 간판을 찍어서 보내라' 또는 '필요한 자료들을 수집해서 보내라" 등의 지시를 하고, 미리 제작해둔 홈페이지를 알려주거나 명함을 보내면서 신뢰를 쌓는다.[139]

전문적인 지식이 필요한 업무가 아니기 때문에 연령, 학력, 성별이 굉장히 다양하고, 아르바이트를 한다고 생각하는 학생, 주부, 노인, 지적장애인 등 평범한 이웃이

---

134) 서울동부지방법원 이은미 변호사, 2023.08.14., 보이스피싱 범죄 유형 관련 인터뷰 참조.
135) 인천지방법원 김지수 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.
136) 서울동부지방법원 이은미 변호사, 2023.08.14., 보이스피싱 범죄 유형 관련 인터뷰 참조.
137) 서울남부지방법원 주희양 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.
138) 서울동부지방법원 이은미 변호사, 2023.08.14., 보이스피싱 범죄 유형 관련 인터뷰 참조.
139) 서울남부지방법원 주희양 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.

대부분이었다.[140] 이들을 기망하는 가장 고전적인 방법으로는 회사의 세금 처리를 간편하게 하기 위해서 현금 출납을 부탁하는 방법을 많이 사용되었다.[141]

또 단순가담자들이 수사기관에 검거될 경우를 대비해 처벌을 면하기 위해 '허위 SNS를 조작'하여 준비하거나, 대응 시나리오를 미리 교육시키는 등의 회피기법을 만드는 경우도 있다.

채팅이 가능한 어플이 굉장히 많이 생기면서, 기존에 인터넷 구인구직 사이트를 통해서 모집하는 방법에서 어플을 통해 조직원을 모집하는 경우도 증가하고 있다. 그 중에서도 특히 일반인에게 익숙한 '당근마켓' 또는 '숨고' 등의 어플을 이용하여 단기 고액 아르바이트를 홍보하고 보이스피싱 업무에 끌어들이는 경우가 있어 주의를 기울일 필요가 있다.[142]

나. 조직원 모집 수법의 변화

보이스피싱 범죄에서 놀라운 점은 피해자를 기망하는 수법만 변화하는 것이 아니라, 피싱 범죄를 완성시켜주는 조직원들을 모집하는 방법도 변화하고 있다는 점이다. 초창기 하위 조직원들 충원 방법을 살펴보면 해외 사기단으로부터 범행을 제의받거나, 한국에 가서 일을 도와주면 관광도 시켜준다고 기망하거나, 유학생 신분으로 입국해서 사기단에게 포섭당하였고, 가족을 해친다는 위협 등으로 조직원을 통제했다.[143]

그러나 최근 들어 조직원들은 수사기관에 노출될 위험이 많은 수거책과 모집책의 경우 본부 사정을 알지 못하게 따로 관리하고, 보이스피싱에 가담하고 있다는 사실을 모르게 하기 위해 모집 시나리오를 따로 준비하는 경향을 보이고 있다. 근로계약서 또는 용역계약서를 작성하거나, 회사의 절세를 위한 것이라고 설명하는 등 조직원을 모집하는 수단 및 수법이 다양해지고 있다.[144]

① 단기고액 아르바이트 모집 수법 : 인터넷 구인구직사이트, SNS 등을 통해 '채권

---

140) 서울동부지방법원 이은미 변호사, 2023.08.14., 보이스피싱 범죄 유형 관련 인터뷰 참조.
141) 인천지방법원 김지수 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.
142) 서울중앙지방법원 김효선 변호사, 2023.08.14., 보이스피싱 범죄 유형 관련 인터뷰 참조.
143) 김성언·양연진, "전화 금융사기 범죄의 진화", 한국공안행정학회보 제17권 제3호, 2008, 128-129면 참조.
144) 서울중앙지방법원 김효선 변호사, 2023.08.14., 보이스피싱 범죄 유형 관련 인터뷰 참조.

회수업무', '외근직 사무업무', '배송업무' 등으로 업무자를 모집하거나, 직접 구직사이트에 올려둔 이력서를 보고 연락을 해서 채용하기도 한다.[145] 심지어는 의심하는 구직자를 대비하여 회사 홈페이지도 만들어서 실존하는 회사처럼 보이게 만들기도 한다.[146] 또, 조직원들은 카카오톡 프로필을 회사이름으로 해두거나, 아이 사진으로 설정해두면서 구직자의 의심과 경계를 줄이기 위해 치밀하게 준비하기도 한다.[147]

② 업무를 결합하여 지시하는 수법 : 가장 최근에는 부동산업과 결합시키는 수법이 발생하고 있다. 부동산 조사 업무로 안내하고 조사를 다녀오면 일당으로 2~30만 원을 주면서 먼저 업무에 대한 거부감을 낮추고, 이후 익숙해 진다 싶으면 추가 업무로 피싱업무를 같이 지시하며, 교묘하게 섞어서 아르바이트생을 속이는 수법도 발생하고 있다.[148] 코로나19가 한참 심한 시기에는 인력이 부족하다는 이유로 급히 제주도에 가서 채권추심 업무를 대신 해주는 알바를 구인하고, 이틀 동안 11번 수거를 하는 동안 수거하는 사람도 보이스피싱 업무인지 모르게 진행시킨다.[149]

③ 한국에 온 유학생 대상 모집 수법 : 유학생 사이트에도 고액 아르바이트를 홍보하며 한국 사정이 어두운 유학생을 대상으로 조직원을 모집하는 경우도 다수 발생하고 있다.[150] 유학생의 경우, 외국인이라 국내에서 취업이 어려워 등록금, 생활비 등을 마련하기 위해 가담하는 경우가 많다.[151]

④ 몸캠피싱으로 협박하는 수법 : 단순가담자의 모집 단속과 처벌이 강화되면서 발생한 신종 수법으로, SNS를 이용한 몸캠피싱으로 금원을 요구하고, 요구한 돈을 마련하지 못하는 경우 '현금수거책 역할이라도 하라'고 협박하며, 기존에는 찾아볼 수 없었던 방법으로 가담자를 끌어들이고 있다.[152]

---

145) 김은정, "대면편취형 보이스피싱 범죄의 범행과정 분석 : 범죄스크립트 분석을 중심으로", 범죄수사학연구 통권 제15호, 2022, 39면 참조.
146) 인천지방법원 김지수 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.
147) 인천지방법원 김도윤 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.
148) 인천지방법원 김지수 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.
149) 인천지방법원 김도윤 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.
150) 인천지방법원 김도윤 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.
151) 윤해성·곽대경, "보이스피싱의 예방과 대책마련을 위한 연구", 형사정책연구원, 2009, 30면 참조.
152) 한겨레, "'몸캠 피싱' 협박해 현금숙책 활용...보이스피싱의 '신종 인력 충원'", 2023.01.30.

⑤ 다른 업무로 모집하는 수법 : 처음에는 블로그 댓글 알바 '재택으로 100만 원 벌기' 등으로 광고를 해서 알바를 모집하지만, 연락을 막상 하면 '해당 업무에 지원자가 많아서 일단 다른 업무를 먼저 하면서 대기하면 해당 업무로 바꿔주겠다.'라고 속이는 수법으로 단순가담자를 모집하기도 한다.[153]

이렇게 자신도 모르는 사이에 보이스피싱 범죄에 가담하게 된 사람들을 살펴보면, 대부분 20대 이거나 60대 이상이며, 계속 공장에서 일을 해왔거나, 일용직 일을 하다 체력저하로 벼룩시장에서 일을 구하거나, 탈북민 등 사회생활에 어려움이 있었거나, 분별력이 약화되어 범죄에 가담하고 있다는 것을 인지하기 어려운 사람들이 조직원의 단순 가담자 모집 대상으로 타깃이 된다.[154]

3. 소결

보이스피싱은 첫 발생부터 지금까지 계속해서 진화하고 있다. 점점 더 교묘해지고 다양한 기술과 결합하면서 이제는 남녀노소를 구분하지 않고 피해가 발생하고 있다. 전화로 피해자를 기망하여 금전을 편취하는 보이스피싱이 최초로 발생한 이후, 파밍, 스미싱, 메신저 피싱 등 범죄수법이 진화한 것은 기본이고, 피해자를 기망하는 수법이 계속해서 변화하고 있기 때문에 피해가 끊이지 않고 있는 것이다. 예를들어 빙자형 보이스피싱으로 같은 수법이라도 피해자를 기망할 때 "'세금·보험금 환급 빙자' 수법에서부터 '납치·협박 빙자' → '택배 반송 빙자' 등"으로 수법이 조금씩 변화하고, 이외에도 같은 피싱사이트를 이용한 범죄에서도 금융감독원사이트, 검찰청 사이트, 인터넷에서 바로 팝업창을 이용하여 접속하게 하는 등 수법이 조금씩 변화하고 있는 것을 볼 수 있다. 보이스피싱을 근절하기 위해 정부와 금융기관에서 다양한 대응책을 마련하고 있지만, 조직원들은 또다른 방법을 계획하여 교묘하게 빠져나가고 있다.

심지어 최근에는 수사기관의 단속을 피하기 위해 '2023년 하반기 제조업 중소기업 육성자금 지원 계획 공고' 등의 가짜 우편물을 발송하거나 직접 우편함에 넣어두고

---

https://www.hani.co.kr/arti/society/society_general/1077426.html (최종검색일 : 2023. 08. 20.) 참조.

153) 서울남부지방법원 주희양 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.

154) 서울남부지방법원 주희양 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰 참조.

우편물에 기재되어있는 전화번호로 연락하면 보이스피싱 조직원과 연락이 되는 사례가 발생하고 있다.[155] 또한 검사 사칭 보이스피싱의 경우, "악성 앱 차단 기능이 없는 공기계 휴대전화를 사용하도록 강요하고, 악성 앱을 깔게 한 뒤에 금원을 편취"하거나, 수사절차라는 이유로 피해자를 모텔로 유인하고 감금 및 신체부위를 촬영해 금원을 편취하는 사례도 발생했다.[156]

금융감독원 보도자료를 참고하여 시기별로 유행한 보이스피싱 수법을 정리해 보면 다음과 같다. [표 3-1]을 통해 연도 별로 보이스피싱 수법이 조금씩 변화한 모습을 확인할 수 있다.

[표 3-1] 보이스피싱 연도별 유행 수법 정리

년도	보이스피싱 수법
2006	최초 보이스피싱 발생
2007	피싱 사이트 : 인터넷 뱅킹 홈페이지 모방
2011	- 피싱 사이트 : 검찰청 홈페이지/개인정보 유출을 이유로 금융정보 직접 입력 유도, 금융정보를 이용하여 공인인증서 재발급 및 인터넷뱅킹으로 계좌이체 카드론 대출 증가 피싱 사이트 : 금융위원회 금융감독원 홈페이지 내 e-금융민원센터 가장 사이트 금융감독원 긴급공지 문자로 피싱사이트 연결 유도
2012	금융자산보호 빙자 신종 보이스피싱 개인정보 유출 사고 → 보안승급 필요 피싱사이트 유도 텔레뱅킹을 이용해 피해자의 예금 편취 '전자금융사기 예방서비스' 가입 요청 문자로 피싱사이트 유도
2013	파밍에 의한 신종 보이스피싱 반복적 발생 주요은행 및 방송사 해킹사고 빙자 보이스피싱 신용카드 이메일 명세서를 이용한 피싱 금융회사 사칭 : '국민행복기금'을 빙자한 보이스피싱 인터넷 실행과 동시에 팝업창 게시하여 피싱사이트 유도 대포통장이 아닌 정상계좌를 이용한 피싱 스피어피싱을 통한 무역대금 사기 발생
2014	카드사 고객정보 유출사고를 이용한 피싱 피싱사이트 내 실시간 채팅창으로 인터넷뱅킹 추가인증 정보 편취하는 수법 '명의도용방지서비스' 가입 유도 신종 피싱 수법
2015	메르스 관련 공공기관 사칭 정부지원금 입금 피싱 레터피싱 : 검찰청 직원 사칭한 가짜 출석요구서 송달 실제 금감원 실장의 실명을 사칭한 피싱

155) 서울경제, "하다하다 이젠 '가짜 우편물까지···치떨리는 보이스피싱", 2023.08.30. https://www.sedaily.com/NewsView/29TLWS81AJ (최종검색일 : 2023. 08. 30.) 참조.
156) 서울경제, "하다하다 이젠 '가짜 우편물까지···치떨리는 보이스피싱", 2023.08.30. https://www.sedaily.com/NewsView/29TLWS81AJ (최종검색일 : 2023. 08. 30.) 참조.

년도	보이스피싱 수법
2016	취업난을 이용하여 가짜 공문서로 접근 및 취업사기 후 신분증 등 개인정보 요구 금융회사 재직증명서를 위조한 피싱 대검찰청 공식 홈페이지 악용한 피싱 대출빙자형 : 기존의 보증료, 신용등급 상향비 요구 수법과는 다르게 고금리대출을 받으면 저금리대출로 바꿔준다고 기망하는 수법으로 변화 가짜 저축은행 홈페이지 이용한 피싱 대포통장 근절대책 이후 : 겨울방학을 맞아 아르바이트생 기망하여 인출책으로 이용하는 사례
2017	전화번호 변작하는 수법 증가 대출금 상환을 사기범 통장으로 유도하는 피싱 금감원 사칭 가짜 이메일 피싱 : '연간 해외송금 한도액 초과 사유에 대한 입증 필요하니 소득증빙 서류 등을 제출하라' 내용 대포통장 근절대책 이후 : 대출을 빙자하여 우선 금전 편취, 이어서 통장까지 가로채 피해자가 대포통장 명의인이 되는 사례 발생 택배 배송 등 사칭 악성코드 URL 문자 발송 가상화폐거래소 가상계좌로 입금을 유도하는 피싱사례 햇살론 등 저금리 서민지원대출 전환을 위해 기존 대출금 대포통장으로 상환 유도하는 피싱 증가
2018	지인사칭 메신저로 금전 요구 피해사례 급증 금감원 사칭 가짜 이메일 피싱 : '유사수신 행위 위반 통보' 조사 위해 주민등록증, 은행통장 준비하여 금감원에 오라는 내용 지인 이름과 프로필 사진 도용하여 사칭 연락 피싱 증가 휴대폰 앱 이용한 신종 피싱 : 피해자 명의 계좌 자금세탁에 이용되어 조치 필요하다고 기망 → 휴대폰에 팀뷰어 프로그램 설치 유도
2019	해외송금 알바를 가장한 보이스피싱 피해금 인출책 모집광고 사례 증가
2020	신종 코로나 바이러스 문자 관련 피싱 코로나19관련 마스크, 손소독제 물품구매 사칭 피싱 소상공인 대상 금융지원을 가장한 피싱 코로나19 정부지원대출 빙자 피싱 신분증, 카드번호를 요구하는 자녀 사칭형 보이스피싱 금융감독원 사칭 : '추가 신규대출은 금융법위반' 이라고 기망하며 자금을 편취하는 피싱
2021	가족·지인 사칭으로 편취한 개인신용정보를 이용하여 피해자 명의의 휴대폰 신규 개통 → 비대면 계좌 개설 및 대출신청
2022	코로나19관련 자가검사키트 공급, 구매 및 정책지원금 안내 사칭 피싱 소상공인 저금리 대환대출, 새출발기금 등 정부지원 대출, 채무조정을 빙자한 피싱 대학입시 및 연말정산 등을 빙자한 피싱 증가
2023	유튜브로 은행직원 사칭해 금융상품 홍보를 가장 및 피싱사이트로 연결하는 피싱 발생 정부 주관 정책자금대출 신청 가능 문자 발송(비대면 대출 신청을 요구) 택배회사 사칭 : 주소 또는 송장번호 불일치 문자 정부기관 사칭 : 방역지원금, 생활안전자금, 근로장려금 등 문자 카카오톡 채널로 시중 은행을 사칭하여 대출 상담을 목적으로 개인정보 요구 소상공인 정책대출을 미끼로 자영업자를 보이스피싱 전달책으로 유인하는 사례 발생

출처: 금융감독원 보도자료 사이트에서 '피싱'을 검색하여 년도별 유행하는 보이스피싱 수법을 정리함. https://www.fss.or.kr/fss/bbs/B0000188/list.do?menuNo=200218 (최종검색일 : 2023. 08. 30.) 참조.

이처럼 최근의 피해 유형은 개인정보를 탈취하는 수법과 연관되어 있는 것을 알 수 있다. 과거 가족 지인을 사칭하여 메신져 피싱을 통해 개인정보를 탈취한 것에서부터 문자나 카카오톡 등에서 지인으로 사칭하여 개인정보 및 인증정보를 요구하는 수법, 대출문자를 받고 개인정보(신분증, 카드)을 송부하도록 하거나 악성 앱을 설치하도록 하는 수법, 그리고 최근 택배, 정부지원금 등 문자를 받고 출처가 불분명한 URL 클릭하도록 하는 수법, 금융 상품 거래 확인서 피싱과 같이 투자성 금융 상품 거래내역을 가공하거나 거래 관련 고객센터 전화번호로 전화를 유도하는 수법 등 교묘해지고 대담해지는 것을 알 수 있다. 피해자는 본인의 개인정보를 전송하거나, 휴대폰 인증번호 송부, 휴대폰 내 악성앱을 설치하도록 강요받고, 사기범은 피해자 피해자 명의 비대면계좌를 개설하거나, 오픈뱅킹 가입, 대출(카드론, 보험대출)을 실행하고 있는 등 다양한 수법이 동원되고 있다.

제4절 | 정부의 대책 진단

1. 범행단계별 총평

국무조정실 보도자료[157]에 의하면 2022년 보이스피싱 피해발생은 16년 만에 큰 폭으로 감소했는데, 발생건수와 피해금액이 30% 대폭 감소하여 그동안 정부의 강력한 조치들이 성과를 내었다고 밝혔다. 정부는 특히 범행단계별 대응 전략을 예방과 차단, 그리고 수사와 홍보강화 등으로 세분화하여 체계적으로 추진한 결과라고 평가하고 있다.

먼저 철저한 사전 예방으로는 피싱사이트 및 변작기 탐지, 불법거래 게시물 탐지, 삭제를 강화하고 대포폰 개통 가능한 회선수 제한, 단말기 자체 국외 발신번호 표시 개선 등의 예방조치를 들었다.[158] 이밖에 과기정통부는 안심마크 표시 서비스를 18개

157) 국무조정실, 2023년 2월 1일자 1면 보도자료에 의하면, 범죄발생건수는 2021년 30,982건에서 2022년 21,832건으로, 피해금액은 2021년 7,744억에서 2022년 5,438억으로 감소하였다.
158) 국무조정실, 2023년 2월 1일자 2면 보도자료.

공공 및 금융기관에서 시범운영하였으며, 고용노동부와 경찰은 구직 사이트 관계자들의 민관 협업으로 현금수거책 알바 모집 광고를 차단하기도 하였다.[159]

범죄수단 신속 차단으로는 경찰은 악성앱, 문자, 대포폰과 통장 등 생성에서 유통까지 전방위적 단속을 실시하고 민관 협업으로 범행수단을 적극 차단하여 큰 성과를 거두었다고 평가하고 있다.[160] 한편, 각 통신사 역시 보이스피싱 범죄 이용 중지 뿐만 아니라 변조 및 발신하는 변작 중계기에 대해서도 사용을 차단하였다고 한다.[161] 또한 금융위를 중심으로 비대면 계좌개설시 본인 확인 등의 절차를 강화하고 피해발생시 피해자가 본인명의의 계좌를 일괄 선택 및 제한할 수 있도록 계좌통합관리서비스 시스템도 시작하였다고 밝혔다.[162]

[표 3-2] 전기통신금융사기 범죄이용 각종 범행수단 차단현황 ('22년, 경찰청)

구분	전화번호	악성앱	카카오 계정	변작 중계기
차단 건수	168,047개	5,982개	6,964개	14,910개

출처: 국무조정실, 2023년 2월 1일자 3면 보도자료.

관계기관 긴밀한 협업 수사와 관련하여 주요 조직원에 대한 대대적인 수사를 통해 보이스피싱 총책 등 상부조직원 657명을 검거하면서 전년 대비 25% 가량 증가라는 성과를 올렸다.[163] 경찰청은 2022년 해외 총책 등 전화금융사기 범죄조직 집중검거 기간을 운영하여 조직 상선 검거에 주력하는 한편, 국내외 전화금융사기 특별 자수 및 신고 기간을 운영하여 대검찰청, 금융감독원, 고용노동부, 관세청은 물론 인터폴, 경찰 주재관, 코리안데스크 등을 통해 외국 법집행기관과 협업한 결과, 조직 상선 검거에 큰 성과를 거두었다. 아울러 정부합동수사단을 2022년 7월 출범하여 보이스피싱 국내외 총책은 물론 대포통장 유통총책 등 111명을 입건하고 24명을 구속하였다[164]고 밝혔다.

159) 국무조정실, 2023년 2월 1일자 2면 보도자료.
160) 국무조정실, 2023년 2월 1일자 2면 보도자료.
161) 국무조정실, 2023년 2월 1일자 2면 보도자료.
162) 국무조정실, 2023년 2월 1일자 3면 보도자료.
163) 국무조정실, 2023년 2월 1일자 3면 보도자료.
164) 국무조정실, 2023년 2월 1일자 3면 보도자료.

[표 3-3] 2022년 역할별 검거 현황

구분	검거인원 합계	역할별 검거 인원			
		상부 조직원	하부 조직원	기타(통신업자 등)	계좌명의인
2022년	25,030	657	14,511	5,016	4,846

출처: 국무조정실, 2023년 2월 1일자 3면 보도자료 및 2022년 경찰청 역할별 검거 현황

국무조정실 보도자료에 의하면 중국 거점에서 보이스피싱 콜센터를 결성하여 금융기관을 사칭한 범죄조직 총책 등을 검거하였고, 필리핀을 거점으로 저금리 대출 명목으로 금융기관을 사칭한 총책 등을 검거하였다[165]고 한다. 이밖에 대포통장과 유심을 유통한 보이스피싱 조직 총책, 모집책, 명의자 등을 검거하였다.[166] 합동수사단에 의하면 조직폭력배와 마약사범 등이 연루된 보이스피싱 조직이 있다고 밝혀 충격을 주기도 하였다.[167]

이처럼 보이스피싱 범죄조직의 근절을 위하여 정보 수사기관 및 외교부 등은 인터폴과 국제기관 및 중국, 필리핀 등 주요 거점국과 핫라인을 구축하는 상시 협업체계를 마련하여 수사역량을 집중해 왔으며,[168] 범정부적 다양한 홍보를 실시하고 있다고 보도하고 있다.

아울러 보이스피싱 사기범죄를 엄정하게 처벌하기 위하여 2023년 11월부터 시행예정인 법제도가 있다. 즉, 기존 통신사기피해환급법상 구성요건화되지 않았던 대면편취형도 사기에 포함하게 되었고 더불어 그동안 세금환급형의 경우 형법상 사기죄가 적용되려면 처분행위에 대한 인식이 있어야 하는데 다행히 2017년 전원합의체 판결에 의하여 처분행위에 대한 인식이 없더라도 형법상 사기죄로 의율이 가능하였다. 그러나 동법에 세금환급형의 경우와 같이 처분행위에 대한 인식이 없어도 처벌할 수 있도록 동법에 명문화 되었으며 처벌도 형법의 사기죄보다 형량이 높다는 점에서 의의가 있다.[169] 이는 보이스피싱의 정범 뿐만 아니라 방조범도 처벌을 강화할 필요가 있다는 각 부처의 의견과도 일치하고 있다. 한편 금융대책과 관련하여 가장 필요한 대책으로

165) 국무조정실, 2023년 2월 1일자 3면 보도자료.
166) 국무조정실, 2023년 2월 1일자 3면 보도자료.
167) 국무조정실, 2023년 2월 1일자 3면 보도자료.
168) 국무조정실, 2023년 2월 1일자 3면 보도자료.
169) 앞으로 2023년 11월 시행될 법에는 1년 이상으로 규정되어 있어서 방조범이라고 6개월의 실형을 선고받을 수 있게 된다.

는 비대면 편취형 보이스피싱 범죄를 방지하기 위해서는 무엇보다 신원의 진위를 안면시스템 등을 통하여 확인할 수 있는 고객확인제도가 필요하다는 점이다. 반면, 가장 아쉽거나 보완이 필요한 대책으로는 지급정지와 관련된 부분으로 비대면 거래제한시 전자 금융거래임에도 불구하고 중고사기, 투자사기 등 보이스피싱 범죄가 아니더라도 각종 지급정지를 요구하고 있어 금융당국에 혼란을 부추긴다는 의견이다. 현재 금융당국의 경우 수사권이 없어 이를 확인할 수도 없다고 한다. 따라서 금융당국에 특사경과 같은 제도 보완이 필요하거나 수사권이 아니더라도 조사권을 신중하게 고려해 볼 수 있다.

2. 대포통장 개설 제한과 신종수법 대응

가. 대포통장 개설 제한

1) 단기간 다수계좌 제한과 거래목적 확인제도

그동안 보이스피싱 범죄와 관련해서 초창기부터 거론되고 있는 것이 바로 대포통장이었다. 보이스피싱 범죄의 시작에는 항상 대포통장이 자리잡고 있었다. 이유는 초창기 대포통장에 대한 거래의 제한이 없다보니 누구나 손쉽게 대포통장을 개설하여 범죄목적으로 사용하였기 때문이다. 그러던 중 대포통장의 개설을 제한하자 노숙자들을 통하여 대포통장을 만들게 하는 등 대포통장은 보이스피싱 범죄에 있어서 꼭 필요한 범행수단이었다. 이를 위해 정부는 전자거래법 등 관련 법들을 개정하였다. 그리고 금융권에서는 '단기간다수계좌'를 제한하거나 '거래목적확인'제도를 시행하여 대포통장의 개설을 규제하였다. 이러한 정부의 노력을 큰 결실을 맺는 것으로 전문가 자문회의 등을 통하여 확인되었다. 다만 신속한 금융처리나 기타 다른 은행업무를 보는 것에 있어서 사실상 국민의 불편함이 초래된 부분이 있었다. 그럼에도 불구하고 현재 이 두 제도는 대포통장을 근절하고 보이스피싱 범죄를 예방하는데 큰 효과가 있는 것으로 판단된다.

2) 본인확인 강화

비대면 계좌개설시 본인확인을 강화하기 위한 방안으로 생체인식을 도입하여 본인이 아니면 계좌개설에서 입금, 이체를 할 수 없도록 하기 위하여 기술적으로 ATM기에 지문, 홍채 등 생체인식을 통해서 사용하는 방안을 고려해 볼 수 있다. 한편, 대출과 같은 악용사례를 방지하기 위해서 비대면 계좌개설시 금융당국(금융위원회 및 금융감독원)의 앱을 통해서 본인을 확인할 때 비로소 계좌를 개설할 수 있는 시스템을 고안해야 한다. 앱을 통해서 신분증진위확인을 하여 보이스피싱 사기범죄자가 위변조를 하지 못하도록 하기 위해서 또는 위변조시 금융결제원과 연결된 행안부나 경찰청 등 관련 부처와의 연결을 통해서 이를 즉각적으로 확인할 수 있어야 한다. 도용과 관련해서는 안면 인식시스템을 통해서 생체인식 정보를 토대로 동일인임을 바로 확인할 수 있도록 해야 한다. 빠르면 내년 1월부터 시행인 고객본인확인제도가 정착된다면 많은 비대면 보이스피싱 범죄사기로부터 예방될 수 있다고 판단하고 있다. 다만 금융당국의 앱을 통해서 신분증진위확인과 안면인식시스템이 이루어지는데 향후 금융당국의 앱을 모방한 피싱범죄가 예상되는 만큼 이에 대한 보안과 검증시스템이 수반되어야 할 것이다. 가령 금융당국의 앱을 일반적으로 인터넷 상에서 어떤 제한없이 다운받는 것이 아닌 은행에서의 본인확인의 인증을 거치도록 하거나 은행에 직접 방문해서 본인 절차를 걸친 다음 은행의 허락하에 앱을 다운받을 수 있도록 하는 방안, 최초 은행에서 생체정보를 인식한 다음 그 생체정보만으로 거래를 하도록 하는 방안 등을 다각적으로 고려해 보아야 한다.

물론 은행직원과의 대면을 통한 거래시에는 이러한 부분을 완화하여 고객의 불편함을 최소화하여야 할 것이다. 다만 비대면으로 ATM기를 사용할 경우에는 대면이 아닌 이상 본인을 인증할 수 있는 형태를 고려하여 사용할 수 있는 방안을 고려해야 한다. 최근 대포폰 방지를 위해 M세이퍼를 사용해야 한다는 주장이 나오고 있다. 현재 사용하는 휴대폰 이외에 다른 통신사에 휴대폰을 개설하지 않을 것이라고 소비자가 의사표현할 수 있도록 하는 제도이다. 사용자 본인이 직접 신청해야 등록이 가능하므로 대포폰 예방에 큰 도움이 될 것으로 보인다.

나. 신종수법 대응

1) 원격조정 앱과 가상자산

최근 금융보안원에서는 금융회사 앱이 가동될 때 보이스피싱 범죄자들이 원격조정 앱을 사용시 이를 차단되도록 하는 조치를 시행하고 있다. 그럼에도 불구하고 대표적인 앱을 점검하여 차단하고 있을 뿐 다른 버전이 계속 만들어지고 있고 다크웹을 통하여 유통하고 있으므로 한계가 있다고 한다. 따라서 금융회사 앱이 가동될 때에는 다른 원격조종앱이 접근하지 못하도록 방화벽을 강화해야 하며 금융보안원 뿐만 아니라 KISA 등 민간보안업체에서도 문제가 있는 원격조종앱의 경우 신고를 받고 이를 바로 차단할 수 있도록 해야 한다. 아울러 지속적인 모니터링을 통하거나 문제가 있는 원격조정 앱이나 피싱사이트 등을 AI와 같은 기술을 이용하여 차단하는 방안을 고민해야 할 것이다.

문제는 보이스피싱 범죄자들이 최근 피해금액을 가상자산으로 이체하거나 받고 있는데 가상자산의 종류도 많고 국내의 거래소가 아닌 해외 거래소도 상당히 많기 때문에 사실상 추적하기도 힘들고 피해자가 지급정지를 해도 현재의 법제도상으로는 환급하기도 힘들다는 점이다. 현재 가상자산은 국내 거래소의 경우 피해금액이 이체된 후에 본인이 확인된 경우 72시간 지연제도를 시행하고 있으며, 금융감독원과 금융위원회에서 단속과 규제하고 법제도를 마련하고 있지만 가상자산의 특성상 변동률이 심해 지급정지를 해도 시가변동이 어제와 오늘, 그리고 내일 변동 폭이 워낙 크다보니 사실상 환급이 실무적으로 불가능하다는 지적이다. 보이스피싱 피해금액이 엄연히 있는데 금액이 넘어서거나 줄어드는 경우가 크기 때문에 그 금액에 맞는 환급을 할 수 없고, 더욱이 국내의 5대 거래소의 1년치의 자금추적을 한 결과 96%가 해외거래소로 이동했기 때문에 사실상 자금을 추적하기도 힘들어 법제도를 마련하는 것도 어렵고 실효성면에서 의문을 제시하고 있다. 가상자산과 관련해서는 별도의 다른 방안이나 정책을 모색해야 할 필요가 있어 보인다. 법제도 측면에서 보면 보이스피싱의 경우 가상자산을 이용한 경우 자금 추적을 통해 범인을 검거하고 이러한 자금을 환수하는 측면에서 보면 자금세탁방지법에서 규제하는 것이 타당해 보이며, FIU와의 긴밀한 협조가 필요하다. 보이스피싱 사기범죄의 지급정지와 환수와 관련해서는 시가변동

이 심하고 환급이 사실상 실무상 불가능한 점에서 보면 뒤에서 살펴볼 기금이나 보험 제도를 활용하여 피해자에게 보상을 해주는 방안을 고려해 볼 수 있다.

2) 정부의 신종수법 대응

현재 보이스피싱 범죄 신종수법이 발견되었을 경우에 긴급대응체계를 현재 갖추고 있다. 국무조정실을 중심으로 신종수법을 각 부처별로 전파하여 각 부처가 할 수 있는 방안을 홍보 및 대응하게 하고 있다. 중요한 것은 국무조정실이 상위기관이고 이를 총괄할 수 있는 기관임에는 틀림없으나 국무조정실에서 모든 보이스피싱 범죄를 우선적으로 파악할 수 있는 것은 아니라는 점이다. 보이스피싱 범죄의 신종수법은 최초 경찰이나 금융위원회에서 적발하는 것이 대부분이다. 따라서 최초 접수된 신종수법의 경우 국무조정실을 통하여 신종수법의 유형을 각 부처별로 알려주고 이에 대한 대응책 마련을 하기 위한 범정부 차원의 TF 마련을 통하여 신속한 대응책을 마련해야 한다. 아울러 각 부처는 보이스피싱 범죄의 신종수법이 발생한 경우 지체없이 국무조정실에 알려서 신종수법 범죄의 대응에 신속하게 대응할 수 있는 체계를 마련하는 것도 고심할 필요가 있다.

초기 보이스피싱 범죄의 경우 각 부처별과 전문가로 구성된 범정부 대응 TF를 상설적으로 운영하고 이에 대한 세미나 등을 통하여 대책 마련에 고심하였으나 현재는 이러한 TF나 전문가 자문회의 등이 예전같이 않다는 평가가 많았다. 보이스피싱 수법의 경우 과거의 범죄수법이 재반복 내지 순환하고 있고 경우에 따라서는 신종범죄와 융합하여 새로운 범죄가 나타나기도 한다. 이러한 경우 정부는 부처별, 또는 전문가 그룹으로 구성된 TF를 통해서 꾸준히 보이스피싱 범죄에 대처하고 예방하는 것이 필요하다. 일시적이고 간헐적인 TF가 아닌 정기적 또는 상설적으로 필요에 따른 범정부 대응 TF를 운영할 필요가 있으며, 각 수법에 따른 전문가를 구성하여 발빠른 대응이 이루어질 필요가 있다.

3. 통신과 금융 대책

가. 통신

1) 대포폰 근절

대포폰과 관련해서 과학기술정보통신부의 경우 보이스피싱 악용 대포폰의 대량유통을 막기 위하여 2022년 9월 대포폰 근절을 위해 동일 명의로 전체 이통사 대상 신규 개통 가능한 회선수를 150개 회선[170]에서 30일 단위로 3개 회선수로 대폭 제한하고,[171] 대면 편취 후 범죄이용계좌의 지급정지, 오픈뱅킹 이체제한 등의 제도를 마련하였다. 먼저 통신대책으로 대표적인 것인 대포폰, 악성문자와 같은 범죄 수단을 차단하는 방안이 있으며,[172] 대포폰을 불법적으로 사용한 행위자나 명의자의 경우 일정기간 동안 신규개통을 차단하는 방안도 고려되고 있다. 아울러 부정개통에 연루된 사업자에 대해서도 엄정 대처한다는 입장이다. 한편 2023년 2월부터 대포폰 보이스피싱 등 불법행위 이력이 있는 명의자의 정보를 이동통신사간 공유하도록 하고 휴대전화 신규개통을 1년간 제한하는 정책을 실시하고 있다.[173]

2) 피싱문자 및 전화번호 변조

피싱문자 근절을 위해 안심마크 표시 서비스 도입[174], 불법전화번호 목록을 문자사업자 간에 공유하도록 하여 문자 발송을 차단하거나 국제전화사칭 근절을 위해 통신사, 단말기 제조사의 국제전화 안내 의무를 강화하기도 하였다. 2023년 1월부터 대량문자 발송 인터넷 문자 서비스의 악용을 방지하기 위하여 불법 전화번호 목록(보이스피싱, 불법스팸, 발신번호 거짓표시, 스미싱 등으로 신고되어 이용중지된 번호)을 문자중계업자에 공유 및 추가 발송을 차단하도록 하였고,[175] 미끼문자와 같은 블랙리스트

---

170) 종전에는 약 50개 업체에 각 3회선으로 총 150개 회선이 개통 가능하여 대포폰을 손쉽게 언제든 개통할 수 있었다고 함.
171) 과학기술정보통신부, 2023년 6월 29, 보도자료 1면.
172) 과학기술정보통신부, 2023년 6월 29, 보도자료 1면.
173) 과학기술정보통신부, 2023년 6월 29, 보도자료 1면.
174) '안심마크'제도란 보이스피싱 예방을 위해 문자 수신시 안심마크가 나오도록 한 것으로 현재 29개 기관만 가입되어 있어 적용기관의 추가가 필요하다는 지적이다. 그리고 공공기관 및 금융기관 등 추가 적용을 통해 시범운영을 할 필요가 있다.
175) 과학기술정보통신부, 2023년 6월 29, 보도자료 1면.

를 만들어 공식적으로 신고 들어온 번호를 리스트화하고 있다. 그리고 블랙리스트는 경찰청에서 KISA로 매일 1회 보내주고 있다고 한다. 현재 중계기를 통한 전화 변작의 경우, 경찰 소관 업무이며, 경찰이 문제의 중계기를 단속하고 있지만, 관련 기관(과기부나 KISA, 방송통신심의위원회)이 이러한 문자중계업자를 모니터링하여 차단하거나 경찰에 신고하는 시스템을 고려해 볼 수 있다.

한때 국제전화의 경우 단말기에 표시하도록 하여 보이스피싱 근절에 효과를 보인 적이 있었다. 그러나 전화번호를 변조 및 발신하는 변작중계기를 사용하면서, 국제전화라도 국내전화로 표시되기 때문에 사실상 중계기의 통신사용을 차단할 방안을 모색해야 한다. 이에 과학기술정보통신부와 한국인터넷진흥원은 SKT, KT, LGU+와 함께 국제전화를 악용한 보이스피싱 범죄 피해를 예방하기 위해 국제전화 수신시 음성으로 국제전화임을 안내하는 서비스를 2023년 7월부터 제공한다고 밝혔다.[176] 또한 삼성, 애플 제조사 등과 협조하여 신종 보이스피싱 피해방지를 위한 휴대폰의 국외발신표시 제도를 개선하였는데, 휴대폰 발신 표시를 개선하여 과거에는 저장된 번호와 전화번호 뒷자리만 일치해도 저장된 이름으로 표기되었던 반면, 국외발신 전화 수신시 본인 연락처에 저장된 번호와 동일한 번호만 저장된 이름으로 표기될 수 있도록 하였다.[177]

또한 가족사칭을 예방하기 위하여 개인정보 유출로 개인정보 유출되면 범죄자들이 그 정보를 가지고 있는데, 해외에서 그 번호로 변작하여 보내면 +82가 찍혀서 표기되도록 하였고, 7월 부터는 “국제전화입니다”라는 음성안내멘트가 나오도록 기술적 조치를 취하고 있다.[178] 더불어서 범죄조직이 국내에 있는 이용자의 전화번호를 도용하여 해외 로밍 형태로 전화번호를 거짓 표시하여 가족을 사칭하는 보이스피싱 행위를 예방하기 위해 국내에 있는 것이 명확한 경우 해당번호의 정상로밍 여부 등을 확인한 뒤 국제전화 수신을 차단할 계획[179]이라고 한다. 한편 보이스피싱 간편 신고를 단말기에서 바로 신고할 수 있도록 하고 있는데 이 또한 보이스피싱이라고 생각될 여지가 많기 때문에 스팸신고창이나 피싱문자 신고채널이 잘 활용되지 않을 수 있다. 따라서 사용자가 신고하기 보다는 방통위, 통신사 등에서 직접 차단하는 방안을 고려해야

176) 과학기술정보통신부, 2023년 6월 29, 보도자료 2면.
177) 과학기술정보통신부, 2023년 6월 29, 보도자료 1면.
178) 과학기술정보통신부, 2023년 6월 29, 보도자료 2면.
179) 과학기술정보통신부, 2023년 6월 29, 보도자료 2면.

한다. 이에 2023년 2월부터 보이스피싱 의심문자 수신시 즉시 휴대폰에서 쉽고 간편하게 신고가 가능하도록 한 서비스를 시행하고 있다.[180] 삼성과 협의하여 삼성폰에서는 해당 기능이 탑재되도록 하고 출고하도록 준비 중에 있으며, 애플의 경우 협의가 어려우므로 해당 기능이 없으나, 현재 KISA가 운영 중인 앱(불법스팸 간편신고)을 이용한 신고가 가능하다고 한다.

한편, 과학기술정보통신부는 최근 문제되고 있는 URL관련 차단 대책으로는 우선 사용자가 절대 클릭하지 않도록 홍보하는 것이 최선책이라고 하며, URL 관련 신고가 들어오면 KISA가 모두 체크하여 통신사에 차단 요청을 하도록 해야 한다. KISA의 경우 접수 후 차단 요청까지 3일 정도의 기간이 소요되는 만큼 가능한 빨리 신고를 해야 보이스피싱을 방지할 수 있다는 것이다. 카카오톡 메시지를 통한 스미싱 등 불법메세지의 경우 이용자가 앱내 신고하는 경우 카카오 사내로 신고되지만 개인정보보호 문제로 인하여 KISA로 연계가 안된다는 문제점이 있다. 이에 개인정보보호를 완화하거나 카카오 사내로 신고를 받는 즉시 카카오 측에서 KISA로 공유하도록 하는 정책을 할 필요가 있다. 과기부에 의하면 문자는 블랙리스트로 관리하며 차단하고 있는데, 향후 음성전화에 대해서도 이러한 관리대책을 마련 중이라고 한다.

보이스피싱 사기의 경우 문자든 전화든 차단조치라는 것은 한 달간의 기간동안만 차단하는 것이고, 대부분의 불법적인 이용자번호는 최대 일주일만 사용하고 계속 바꾸는 수법을 사용한다고 한다. 이에 대하여 주의를 요하며, 설마 내 번호가 도용되어 불법문자에 이용되는 것을 차단하는 서비스, 즉 '번호도용문자차단서비스'가 현재 시행중에 있는데(통신사 통해 가입 가능), 이 서비스에 대해 모르는 경우가 많아 홍보를 통해 가입할 필요가 있다.

나. 금융대책

1) 정부의 다양한 정책

금융대책과 관련하여 대면편취형의 경우 통신사기피해환급법상 구성요건이 결여되어 있었는데, 수사기관이 현장에서 검거, 즉시 금융회사에 지급정지를 할 수 있도록

180) 과학기술정보통신부, 2023년 6월 29, 보도자료 1면.

법이 개정되어 2023년 11월부터 시행예정이다. 그리고 카드, 통장을 사용하지 않는 ATM 현금입금 한도를 축소하였는데 이는 여러 가지 불편함을 안겨주고 있는 것이 사실이나 효과는 있는 것으로 나타났다. 한편, 금융회사에서 소비자 경고를 수시로 보내거나 언론 홍보를 통한 보이스피싱 최근 수법을 소개하는 것이 국무조정실에서 각 부처별로 홍보하고 대응하는 것보다 효과가 빠르다는 지적이 있었다. 또한, 지연인출제도와 단기간 다수 계좌개설 제한, 거래 목적 확인제도, 보이스피싱 피해 발생시 피해자의 본인 명의로 된 금융기관의 계좌를 일괄 또는 선택 정지할 수 있는 시스템이 구축되어 시행하고 있다.

한편, ATM기를 이용하는 경우에는 노인을 포함하여 속수무책으로 당할 여지가 있다. 이에 청원경찰이나 보안요원으로 하여금 보이스피싱 예방에 대한 교육을 통하여 ATM기에 접근하는 사람들을 주의깊게 관찰하고 도움을 주는 것도 고려해야 한다. 특히 현금수거책의 경우 여러 번 나누어서 현금을 인출하고 모자나 안경 등을 착용하거나 수상한 낌새가 있으면 경찰에 신고하거나 현장에서 검거할 수 있도록 해야 할 것이다. 최근에는 알바몬, 벼룩시장 등 고액 아르바이트 모집을 빙자하여 이력서를 업로드하도록 하고 정식업체인 듯 가장하여 현금책이나 수거책 등을 모집하고 있다. 따라서 처음 가담자의 경우 보이스피싱인지 모르는 경우도 있으나 알면서도 처벌이 안 되는줄 알았다는 경우가 상당하므로 이에 대한 경계문구를 ATM기나 광고 등에 삽입하여 남의 돈을 함부로 입금하는 것이 보이스피싱 범죄 가담자가 될 수 있고 처벌될 수 있다는 주의 문구를 홍보할 필요가 있다. 이를 통해서 보이스피싱 방조자라고 할지라도 미필적 고의를 인정하여 처벌을 강화, 경각심을 높일 필요가 있다. 또한 2023년 11월부터는 처분행위의 인식이 결여된 경우 형법상 사기죄가 2017년 전원합의체에 의하여 처벌될 수 있었으나 전기통신사기피해 환급법에서도 처분행위를 인식하지 못한 세금환급형의 경우 처분행위를 인식하지 못하였더라도 기존 형법상 사기죄보다 높게 처벌할 수 있도록 법을 개정, 시행하게 되었다.

2) 이상거래징후 시스템

금융회사 자체적으로 피해를 탐지하는 시스템을 통하여 예방 정책들을 시행하고 있는 것을 확인할 수 있었다. 간혹 각종 매스컴이나 신문, 뉴스 등에서 “은행 직원의

도움으로 보이스피싱 범죄를 막았다"또는 "범인을 검거하였다" 등의 내용을 접할 수 있다. 따라서 금융회사 자체적인 노력이 얼마나 중요한지는 새삼 알 수 있는 대목이다. 문제는 이러한 이상거래징후 시스템은 원래의 목적은 자금세탁방지법에 의하여 보이스피싱이나 전세사기, 투자사기 등의 자금을 추적하는데 있지만 은행의 경우 이러한 법제상의 포괄적인 행위 유형을 포섭하기 힘들다. 그래서 은행마다 그동안의 보이스피싱의 경험칙을 바탕으로 시나리오를 구성한 후 시스템에 탑재하여 이상 징후시 경고음이 발생하여 은행 자체적으로 판단하여 보이스피싱 범죄에 사용되거나 사용될 계좌를 정지하거나 경찰에 신고하는 경향이라고 한다. 차후 금융보안원에서 은행마다 이상거래징후시스템을 공유하고 있다고는 하지만 은행마다 대응하는 이상거래징후시스템의 노하우가 다르고 시스템도 달라 통일적이지는 않다는 평가이다.

3) 은행의 대응방안

은행의 경우 보이스피싱 사고 접수시 개인정보 유출 및 피해 상황에 대해 정확히 파악하고, 비밀번호 변경, 인증서 폐기, 보안매체 재발급, 개인정보노출자 등록 등 사고접수 및 관련 업무처리를 하고 있는 실정이다. 지급정지 해제와 관련해서는 본인 요청에 의한 지급정지 등록은 본인요청에 의해 해제가 가능하며, 개인정보유출에 의할 경우에는 본인 요청 지급정지 계좌 확인시 지급정지 해제전 조치사항 안내 및 자필 확인이 필요하다고 한다. 은행 업무처리시 유의사항으로는 전기 통신 금융사기에 해당하는지 확인을 하거나 유선신고 여부 및 사건사고사실확인원(경찰서 발급) 지참 여부를 확인하고, 사기 이용 계좌 당/타행 여부를 확인한다고 한다. 또한 업무처리 불편 사항으로는 당/타행 계좌에 따른 업무처리 방법이 상이하고, 은행, 경찰서 등 피해처리가 가능하도록 기관의 일원화, 혹은 처리 방법 연동이 필요하다는 의견을 제시하였다. 이유는 피해 처리를 위한 기관 방문으로 처리 지연 문제가 발생하고, 피해자가 피해 사실을 인지한 시점에 기 발생된 금융거래에 대한 복원 방법이 없다는 것이다.

이에 은행에서 제시한 피싱 피해 예방법으로는 안심뱅킹서비스[181], 악성앱 구동

181) 현재 은행에서 제공되는 서비스로 실물 OTP 고객의 모바일 OTP 발급을 제한하여 피싱 및 정보탈취 사기의 피해를 예방하고 있다.

시 금융앱 동작이 불가하도록 금융앱을 개선하거나 금융 피해 사실이 명백하게 확인되면 사기로 발생한 거래에 대해 취소 및 정정이 가능한 방안을 모색 또는 금융 사고 처리 프로세스 간소화하여 처리 지연으로 인한 2차 피해가 없도록 해야 한다는 의견을 제시하였다.

4) 피해 상황 대응

보이스피싱 사기범죄 관련 현재 피해상황을 보면 피해자가 신분증을 유출 및 분실 시 신분증을 새로 재발급받아야 하며, 휴대폰 악성 앱이 본인 휴대폰에 설치된 경우에는 가까운 서비스센터에 방문해야 한다. 신분증을 유출 및 분실했다면 혹시나 보이스피싱 범죄에 사용될 가능성을 염두하여 가까운 동사무소 내지 문화센터에 신고하여 다른 곳에서 신분증이 사용될 경우 이를 포착하는 시스템을 고려해 볼 수 있다. 또한 현재의 시스템이라면 휴대폰에 악성 앱이 설치될 경우 가까운 서비스센터에 방문해야 하는 번거로움이 있다. 그리고 휴대폰에 악성 앱이 설치되었는지도 모르는 경우가 상당할 것으로 보인다. 따라서 휴대폰 자체적으로 악성 앱이 설치되었는지를 자체 점검하는 프로그램이 내장되어 있어야 할 것이다. 그렇지 않다면 은행방문시 은행원이나 청원 경찰 등이 요청시 휴대폰 악생 앱이 설치되었는지, 설치되었다면 그 자리에서 바로 삭제할 수 있도록 교육이 필요하다.

현재 개인정보가 유출되었다면 경찰청, 금융감독원, 금융기관 콜센터에 신고하여 피해상황에 대응하도록 하고 있다. 또는 비대면 계좌개설여부를 확인하려면 계좌정보통합관리서비스를 통해 확인할 수 있으며, 대포폰 가입 여부를 확인하려면 명의도용서비스 사이스를 조회하여 알 수 있다. 이를 표로 정리하면 다음과 같다.

내용	방법
개인정보 유출 신청	경찰청, 금융감독원, 금융기관 콜센터
비대면 계좌개설 여부	계좌정보통합관리서비스(www.payinfo.or.kr) 조회
대포폰 가입여부 확인	명의도용방지서비스(www.msafer.or.kr) 조회

문제는 이러한 홍보가 제대로 되어 있지 않아 많은 사람들이 잘 모르는 경우가 많다는 점이다. 그리고 개인정보 유출시 경찰청, 금융감독원, 금융기관 콜센터에 신고

하도록 되어 있으나 각각의 유관기관이 제각각이다 보니 정보공유나 대응이 신속하지 않다는 지적이다. 비대면 계좌개설과 대포폰 가입여부의 확인도 사이트가 다르다 보니 불편함이 적지 않다는 지적도 있었다. 보이스피싱 범죄와 관련되었는지를 한번에 확인 및 신고할 수 있는 사이트를 마련하고 신속하게 대응할 수 있는 시스템을 마련하는 것도 필요해 보인다.

4. 해외 공조 수사 및 관계기관 협업수사

가. 해외 공조 수사

1) 총책 검거의 필요성

대부분 보이스피싱 범죄단체는 점조직 형태로 이루어지고 운영하고 있기 때문에 수사하는데 상당한 애로점이 있다. 더구나 총책이 해외에 거주하고 있기 때문에 총책을 검거하지 않는한 말단 조직원을 가벼운 처벌에 그치고 있다. 총책의 경우 중국은 물론 베트남 및 필리핀 등 동남아시아에 주로 본거지를 마련하고 있다. 따라서 보이스피싱 범죄단체의 경우 해외에서 결성된 뒤에 국내에서 범행을 범하고 있기 때문에 이러한 조직원을 검거하기 위해서는 외교부, 인터폴과 중국공안 등과의 해외공조가 필요하다.[182] 특히 총책을 검거하기 위해서는 무엇보다 관계기관 긴밀한 협업수사를 통하거나 해외 공조가 필수적이다. 최근의 수사사례를 비추어 볼 때, 한국의 수사기관이 중국 공안과의 친밀한 관계를 유지하거나 중국 내 거주하면서 총책이나 운영책을 검거한 사례가 있다. 이처럼 수사기관과의 긴밀한 협력관계를 통하여 총책을 검거할 필요가 있다. 또한 정부합동수사단은 22년 7월 출범 이래 약 5개월 간의 합동수사로 보이스피싱 조직의 국내외 총책, 대포통장 유통총책 등 총 111명을 입건하고 24명을 구속하였다.[183] 이처럼 보이스피싱 범죄의 총책과 관련 인물을 검거하기 위해서는 정보 수사기관 및 외교부 등 관계부처와의 협업과 해외 공조가 뒷받침되어야 한다.

---

182) 국무조정실 보도자료에 의하면 국내말단 조직원부터 해외 총책 등 주요 조직원에 대한 대대적인 수사를 통해 보이스피싱 총책 등 상부 조직원 657명을 검거하면서 전년 대비 25%가량 증가하는 성과를 올렸다고 밝혔다(국무조정실, 보도자료, 2023. 2월 1일 배포, 3면).

183) 국무조정실, 보도자료, 2023. 2월 1일 배포, 3면.

〈주요 검거 사례〉[184)]

◇ 중국 거점 8개 보이스피싱 조직 95명 검거, 40명 구속〈경찰청〉
- 중국 칭다오 · 광저우 등지에 보이스피싱 콜센터를 결성, 금융기관을 사칭해 피해자 442명으로부터 34억 원 상당을 편취한 8개 범죄조직 총책 등 95명 검거

◇ 필리핀 거점 최대규모 보이스피싱 조직 39명 검거, 10명 구속〈경찰청〉
- 필리핀 마닐라에 보이스피싱 범죄조직(민준파) 결성 후, '17. 12월~'21. 12월까지 금융기관을 사칭하여 저금리 대환대출 등 명목으로 피해자 562명으로부터 108억 원 상당을 편취한 총책 등 39명 검거

◇ 대포통장 · 유심 유통 보이스피싱 조직 168명 검거, 12명 구속〈경찰청〉
- 통신 판매점 5개소를 개설한 후 '20. 1월부터 '22. 8월까지 인터넷 등으로 명의자를 모집해 개통한 대포유심 1,716개와 명의자 동의 없이 개설한 증권계좌 417개를 전화금융사기 조직에 유통한 범죄조직 총책 · 모집책 · 명의자 등 총 168명 검거

◇ 조직폭력배와 마약사범 등이 연루된 보이스피싱 조직 수사〈합수단〉
- 단순 현금수거책만 불구속 송치된 사건을 전면 재수사하여 마약사범과 조직폭력배('동방파' 두목, '칠성파' 행동대원)가 연루된 보이스피싱 조직이 '13. 9.~'22. 6. 피해자 23명으로부터 약 9억 5,000만원을 편취한 전모를 규명하여 국내외 총책 등 총 30명을 입건하고 9명 구속

이상의 검거사례를 보면 총책을 비롯하여 관련자를 검거하기 위해서는 중국, 필리핀 등 주요 거점국과 핫라인을 구축하는 등 상시 협업체계를 구축하거나 인터폴 등 국제공조를 통하는 방법 등 국내외 정보 수사역량을 집중한 것을 알 수 있다. 더구나 최근의 경향은 외국인, 마약사범, 조직폭력배와 연루된 보이스피싱 범죄가 이루어지고 있기 때문에 연루범죄에 대한 수사도 필요한 상황이다. 이를 위해서는 해외 네트워크망이 필요한데 국가정보원이 해외 네트워크망이 잘 되어 있으므로 국정원의 협력 역시 필요하다. 보이스피싱 범죄의 경우 무엇보다 경찰의 수사의지가 중요하다. 중국 공안은 물론 주요 동남아시아국의 협조를 얻기 위해 자체적인 네트워크망을 형성하여 수사 협조를 이끌어야 할 것이다. 그리고 보이스피싱 범죄와 연계된 다른 범죄를 예방하고 대응하기 위해서라도 주기적인 해외 수사 네트워크망을 구성 및 유지하여 보이스피싱 범죄 뿐만 아니라 이와 연계된 범죄 역시 일망타진해야 할 것이다.

2) 법집행기관간 협업체계 및 네트워크 도모

국가간 협업을 유도하기 위해서는 워킹그룹에 참여하거나 관련 TF 협의체 기구

184) 국무조정실, 보도자료, 2023. 2월 1일 배포, 3면.

등에 참여 또는 해외 수사 기관과의 협력약정(MOU) 체결을 통하여 법집행기관간의 협업체계와 네트워크를 도모하는 방안도 고려해 볼 수 있다. 오늘날 수사기관 간의 공조는 국제회의, 컨퍼런스, 교육훈련, 공동수사 등을 바탕으로 국제협력 교류가 활성화된다는 점을 고려해야 한다. 또한 수사기관간 직접적으로 협업체계를 구축하는 방안도 고려해 볼 수 있다. 즉 국제사법공조의 경우 주로 외교부를 거치는데 이러한 과정을 생략하고 경찰 대 경찰, 검찰 대 검찰 등 법집행기관이 자체적으로 친밀한 관계를 맺고 공조를 요청하는 방안이다. 이러한 기관간의 협업체계가 활성화된다면 신속한 대응과 피해구제가 가능하게 된다. 나아가 동남아시아를 기반으로 한 보이스피싱 범죄가 활성화되고 있으므로 유럽의 유러폴과 같이 동아시아폴과 같은 기구를 마련하는 것도 의미가 크므로 해당국들 사이에 실질적인 도움이 될 수 있는 시스템을 장기적으로 고려해야 할 것이다.

나. 관계기관 협업

1) 신속한 지급정지의 개선

2011년 전기통신금융사기피해방지 및 피해금환급에 관한 특별법 시행 이후 보이스피싱 사기 범죄의 경우 가해자가 피해자에게 입금하려고 하는 계좌의 경우 입금을 하면 바로 지급정지를 경찰에 신고시 함께 할 수 있도록 제안했었고 시범적으로 운영하였었다. 즉 사기이용계좌에 입금된 순간부터 약 20분 안에 현금수거책이 현금으로 빼내가기 때문에 가능한 빨리 신속하게 계좌를 지급정지해야 하기 때문이다. 경찰에 신고하면 경찰이 보이스피싱 사기범죄를 접수하면서 동시에 금융당국으로 연결하여 신속하게 사기이용계좌를 지급정지라는 시스템이었다. 그러나 금융당국에 의하면 홍보가 부족해서인지, 아니면 무슨 이유인지 경우에 따라서는 그러한 제도는 현재 잘 활용되지 않고 다시 예전처럼 은행에 신고하고 은행에서 지급정지를 하도록 하고 경찰에게 별도의 수사요청을 해야 한다는 것이다. 전기통신금융사기피해방지 및 피해금환급에 관한 특별법상 가장 핵심적인 부분이 지급정지를 신속하게 하고 신속하게 피해자에게 피해금을 구제할 수 있도록 하는 제도였으나 부처별로 하는 역할과 소관업무가 다르고 상호 협조는 물론 정보 공유가 이루어지지 않는 점에서 이러한 문제가

발생한다고 본다.

금융당국 관계자에 의하면 현재 지급정지의 환급율은 약 30%라고 한다. 은행에 신청해서 구제를 별도로 하는 순간 지급정지를 하기도 전에 피해자의 금원은 범죄자의 손으로 들어갈 것은 뻔하다. 역시 관계 기관 내지 부처의 협업이 필요한 시점이라고 판단된다. 지급정지도 마찬가지로 수사기관이 신청을 받으면 그 즉시 수사에 착수하고 금융당국에 바로 요청하여 지급정지를 할 수 있도록 해야 한다. 아울러 금융당국과 관계 유관부처는 보이스피싱 범죄에 함께 대응할 수 있는 시스템을 구축해야 한다. 그렇지 않다면 현재의 상황에서는 금융기관에게 요청된 지급정지를 하면서 바로 수사에 착수하려면 금융당국에 수사권을 주는 것이 효과적일 것이다.

과학기술정보통신부에 의하면 경찰이나 보이스피싱합동수사단과 협업하여 통신사에 대한 합동 검사로 불법대출에 이용되는 보이스피싱 사기가 매달 몇십만 건에 이르던 신고건수가 천건단위로 줄었다는 경험으로 미루어 볼 때, 대응차원에서 보면 검찰 및 경찰과의 협업이 효과적이었다고 한다. 경찰은 수사대상에 대한 압수수색을 진행하고, KISA는 점검을 진행하여 통신사를 통해 불법정보를 많이 보내는 이용자의 계정을 차단할 수 있었다고 한다. 따라서 관련 부처의 유기적인 협업과 지속적인 단속이 보이스피싱 사기에 효과적인 것을 알 수 있다.

2) 통합신고센터의 원스톱 운영

2023년 7월부터 통합신고 대응센터가 마련되어 시행될 예정이다. 각 유관 기관별 업무 분야의 차이가 있기 때문에 경찰 주도의 통합 운영에 대하여 우려하는 시선이 있다고 한다. 금융감독원에 의하면 계좌지급정지나 피해 규제 상담 등의 업무를 처리하고 있는데 통합신고센터에서는 사건처리에 대한 상담 인력만이 있기 때문에 피해구제에 있어서 효과적인 대응이 어렵다는 것이다. 이에 반해 경찰청에서는 피해 구제 방법 등에 대해서도 상담이 이루어지고 있다는 입장이다. 아울러 전화번호 이용 중지에 대한 협의가 안 된 상황이다 보니 자체적으로 전화번호를 중지할 수도 없고 다시 방통위에 연락하여 중지하는 체계이다. 통합신고 대응센터가 원스톱으로 운영되려면 사고처리 및 피해구제, 대응 등 종합적이고 유기적인 연계가 필요하다. 일원적인 신고체계만 갖추는 것이 아닌 신고를 통하여 보이스피싱을 종합적으로 대응하고 피해구제

를 할 수 있는 시스템을 마련해야 한다. 그러기 위해서는 112신고센터가 아닌 별도의 통합신고대응센터를 마련하고 각 부처의 전문가를 상주하게 하고 할 수 있는 일은 바로 그 자리에서 대응 및 피해구제를 하고 그렇지 않은 일은 부처로 연락하여 해결하도록 해야 할 것이다.

3) 보이스피싱 통계의 일원화 및 통합

통계와 관련해서 전체적이고 통합적인 통계 수집이 현재로서는 어렵다는 것이다. 각 부처에서 하는 업무가 다르기 때문에 그 일에 한해서 통계수집이 가능하다는 것이다. 가령 금감원에서는 통신사기 환급법에 해당하는 통계만 수집하고 있고 경찰은 사건처리의 통계, 방통위에서는 전화번호 변작 및 이용중지 등 각각의 통계를 관리하고 있어 전반적인 통계의 통합이 사실상 어렵다. 따라서 효과적인 보이스피싱 범죄를 예방하고 대응하기 위해서는 기본적이고 통합적인 통계가 필요한 만큼 관련 법제도를 손질하여 보이스피싱 관련 통계를 통합적으로 수집 및 관리해야 한다. 가능하다면 통합신고 대응센터에서 모든 보이스피싱 신고를 접수받는 만큼 여기서 통계를 수집 및 관리하는 방안도 고려될 수 있다.

5. 소결

보이스피싱과 관련하여 정부는 새로운 수법이 나타날 때 마다 일선에 빨리 알리고 신속하게 대응할 수 있는 프로세스를 제시하였다. 한 때 국민에게 문자를 통하여 보이스피싱을 예방할 수 있게 하였지만 이는 비용이 드는 문제도 있을 뿐만 아니라 큰 효과를 담보하지도 못하였기 때문에 현재는 답보상태이다. 금융감독원 등은 내부적 평가를 통하여 가령 소비자 보호실태 평가 등을 통하여 보이스피싱에 정부의 대책이 어느 정도 효과가 있는지 자체평가를 하지만 그럼에도 불구하고 보이스피싱 범죄는 수법을 바꾸거나 새로운 수법이 나타나면서 금융당국을 당혹하게 만들고 있다.

특히 현재 인터넷이 등장하고 가상자산이 활용되면서 보이스피싱과 같은 범죄는 대응하기 어렵다는 분석도 나오고 있다. 이유는 가상자산은 자금을 추적하기 힘들뿐더러 자금을 세탁하기 위한 것인데 기술적으로 가상자산이 보이스피싱 범죄에 연루되었다고 하면 사실상 현재의 지급정지의무는 무용지물이라는 것이다. 다시 말해서 보

이스피싱 범죄자들이 가상자산으로 돈을 입금하라고 하면 이를 담당하는 거래소에 지급정지를 해봤자 지급정지가 될 수 없다는 것이다.

또한 형평성과의 문제도 주장되고 있는데, 현재 주식의 경우 지급정지 대상이 아닌데, 가상자산을 지급정지 대상에 포함시키는 것도 사실상 형평성에 어긋난다는 것이다. 따라서 보이스피싱의 경우 가상자산으로 입금하지 말아야 하는 대대적인 홍보가 필요하며 거래소에서는 자체 지침을 통하여 내부적으로 보이스피싱 범죄 관련 이상징후 포착 등의 교육을 통하여 금융회사처럼 자체적으로 대응할 필요가 있다. 그리고 금융위원회가 가상자산을 담당하고 있으므로 수시로 거래소 점검 및 단속을 통하여 보이스피싱 피해에 만전을 기하여 할 것이다. 은행직원이든 거래소 직원이든 보이스피싱의 예방과 대응과 관련하여 보이스피싱 피해를 방지하거나 범죄자를 검거할 경우 별도의 인센티브나 인사고과에 반영하는 방안도 고려될 수 있다.

한편, 부처간 업무도 상이하고 관할도 다르다. 금융감독원의 경우는 사칭형(메신져, 비메신져)과 대출빙자형을 담당하고 있으며, 전화번호이용중지의 경우는 방송통신위원회가 담당하고 있고 가상자산의 경우는 금융위원회에 담당하고 있다. 또한 전화번호나 변작신고는 인터넷 진흥원(KISA)가 담당하고 있듯이 각 부처의 역할도 서로 다른 것을 확인할 수 있었다. 사실상 현재 상황에서는 신고가 들어와도 부처의 업무가 아닌 이상 다른 곳으로 신고를 해야 한다. 사정이 이렇다 보니 통합신고센터를 만들어서 대응해야 한다는 목소리도 커지고 있는 상황이다. 그러나 통합신고센터를 만든다고 해서 보이스피싱 범죄나 피해구제에 과연 효과가 있는 것인지는 다시 한번 고려해야 한다. 어차피 업무가 다른 이상 신고만 통합되었다고 한들 이곳에서는 일반적 상담만 할 뿐이며 정보의 접근 자체도 어렵고 대응하는 기관도 다 다르기 때문에 금융당국 내지 방통위로 다시 들어올 수밖에 없는 구조인 것이다. 통합신고센터가 통합신고ㆍ대응센터로 명실상부한 보이스피싱 대응 및 피해구제 기관으로 거듭나려면 상담은 물론 신속한 대응과 피해구제도 함께 가능해야 한다는 점을 염두해야 한다. 그러려면 국무조정실 아래 보이스피싱 합동 대응단을 마련하거나 경찰청 아래 합동수사단을 마련하여 FIU, 금감원, 금융위, 방심의 등 보이스피싱 범죄의 대응에서 피해구제까지 한꺼번에 해결할 수 있도록 하는 방안을 고려해야 한다.

오래전부터 전문가들은 통합신고 대응센터를 마련해야 한다고 주장했었다. 보이스

피싱 범죄가 다양하고 한 부처만으로는 대응이 힘들기 때문에 112 통합신고 · 대응센터를 마련하고 각 유관부처의 인원이 파견을 나와서 함께 공동으로 대응을 해야 하지만, 비용과 인력, 여러 가지 사정을 원인으로 현재까지 이루어지지 않고 있었다. 대표적으로 경찰에 신고하고 동시에 금융기관으로 연결하여 지급정지를 하도록 하는 것도 그러한 일환이었다. 현재 정부에서 제시한 통합신고센터의 기능을 보면 신고는 물론 신고데이터를 집적, 분석하여 수반되는 절차를 동시에 처리하고 수사 및 행정처분 자료로 활용한다는 입장이다. 이를 위해서는 여러 가지 보이스피싱 범죄의 문제를 해결할 수 있는 장비와 시설, 그리고 인력이 필요하다. 형식적인 신고만이 아닌 신고에서 원스톱으로 어느 정도의 대응을 할 수 있는 하나의 센터 내지 기관이 필요하다.

나아가 어느 정도의 적절한 대응을 할 수 있지만 전문적인 대응을 할 수 있는 허브기관이 되어야 한다. 가령 국제조직과 연계된 보이스피싱 범죄 신고시 통합신고센터에 신고가 접수된 다음 통합신고대응센터의 경찰 내지 합동수사단의 검경이 이를 인수인계 받고 초동조치를 취한 후에 본청 내지 대검찰청에 연락하여 중국 공안 내지 인터폴의 협조 아래 검경이 합동으로 수사를 하는 것이다. 또한 국가정보원의 해외 네트워크망을 활용하여 정보를 받고 국제공조수사를 할 수 있도록 해야 한다.

정부의 대책 가운데 한 가지 아쉬운 점은 현재 보이스피싱 정부 합동 수사단을 설치 운영하겠다는 것인데 이 역시 오래전에 전문가들이 주장한 대안이었다. 이제야 대검찰청, 경찰청, 관세청, 국세청, 금융감독원, 방송통신위원회 등 정부 기관들로 구성된 합동수사단을 마련한다는데 늦은감이 있다. 다만 합동수사단이 경찰청 아래에 편성을 할 것인지 아니면 국무조정실 아래에 편성될 것인지는 다시 한번 논의해야 할 것으로 보인다. 중요한 것은 경찰청 아래 합동 수사단이든, 국무조정실 아래 합동대응단이든 간에 보이스피싱 관련 정부부처로 이루어진 만큼 중요한 것은 보이스피싱 정부 합동 수사단 및 합동 대응단과 112 통합신고 · 대응센터는 별도의 기관이 되어서는 안 된다는 점이다.

보이스피싱 합동 수사단 아래 112 통합신고 대응센터가 위치하여 함께 협업할 수 있는 환경이 구축되거나 국무조정실 아래 합동 대응단을 마련하여 신속하게 112 통합신고 대응센터와 밀접하고 유기적으로 협업이 이루어질 필요가 있다는 것이다. 다만 통합신고 대응센터와 수사기관 간이 유기적인 협력이 필요한 만큼 신고 대응센터에서

확보한 데이터를 분석 및 종합하여 수사기관에 제공함으로써 유기적인 협력이 이루어지게 할 필요가 있다. 보이스피싱 범죄는 하나의 독립된 범죄가 아닌 여러 가지 속성과 특성을 가지고 있기 때문에 각 부처가 별개로 이루어서 대응하기란 사실상 의미가 없을 수도 있기 때문이다. 함께 하나의 보이스피싱 범죄 대응이라는 목표아래 일사천리로 대응하고 전파하고 예방하는 시스템이 함께 이루어질 필요가 있다.

보이스피싱 범죄는 대표적인 서민범죄에서 지금은 전 국민을 노리는 범죄인 만큼 피해자 큰 것이 사실인 만큼 보이스피싱 범죄에 대한 정부의 대책은 계속 현재 진행중이다. 2023년 7월 초부터는 개인정보가 노출자 시스템을 도입하여 간편송금제도를 보완 및 수정한 일괄지급제도를 시행할 예정이다. 정부의 대책대로 지급정지는 보이스피싱을 근절하기 보다는 피해자 구제 차원에서 획기적인 대책으로 평가되고 있었다.

그러나 최근 이러한 전체 지급정지가 오히려 선의의 피해자에게는 피해를 주는 제도가 되고 있는 만큼 정부는 전체지급정지제도에서 부분지급정지제도로 변환하거나 특정은행에 한하여 지급정지를 추진하는 것도 의미가 있다. 아울러 보이스피싱 범행에 가담하지 않게 하기 위해서는 현금수거책이나 그 외 방조범에게도 전반적으로 형량의 구형을 높일 필요가 있으며, 법원은 보이스피싱 방조범에게 범죄단체의 미필적 고의를 확대해석하여 실형을 선고할 필요가 있다.

보이스피싱 범죄피해자에 대한 피해구제방안

김 계 환

제4장

보이스피싱 범죄피해자에 대한 피해구제방안

보이스피싱 범죄피해자에 대한 법적 피해구제방안과 관련하여서는 우선 현행 법체계 하에서 피해자가 취할 수 있는 법적 구제절차와 그 문제점 및 개선 방향을 살펴보고, 아울러 새롭게 도입할만한 제도에 대하여 살펴보고자 한다.

제1절 | 민사상 손해배상청구

1. 금융회사 등에 대한 손해배상청구

가. 지급정지 미이행시 손해배상

전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법(이하 '통신사기피해환급법'으로 약칭한다)은 금융회사가 대출신청이나 금융상품 해지와 같은 금융거래시 본인확인조치를 하지 않음으로써 이용자에게 손해가 발생한 경우(제2조의4 제2항)와 피해자의 피해구제신청 또는 피해구제신청을 받은 금융기관의 지급정지 요청, 수사기관 또는 금융감독원으로부터 사기이용계좌로 의심된다는 정보제공이 있는 경우임에도 지급정지를 이행하지 않아 이용자에게 손해가 발생한 경우(제4조 제3항) 그 손해를 배상하도록 하고 있다.

이와 관련하여 현행 통신사기피해환급법은 금융회사의 금융거래 시 본인확인조치 미이행과 지급정지 사유가 있음에도 미이행 시에 한하여 손해배상책임을 지도록 하고 있어 이 법에 따라 피해자가 손해배상을 받을 수 있는 경우가 거의 없다고 보는 견

해[185]도 있다. 그러나 위와 같이 본인확인조치를 이행하도록 하고, 미이행시 손해배상책임을 지운 결과 사기범이 피해자의 명의로 대출을 받거나 적금을 해지하여 인출하는 등의 피해(이러한 유형이 피해자별 피해금액이 상대적으로 크다)는 상당히 줄어든 긍정적인 효과가 있었다. 또한 피해금을 사기범이 인출하기 전에 금융회사로 하여금 신속한 지급정지 조치를 하도록 강제함으로써, 피해금 환급을 통한 피해구제의 실효성을 높이는 효과도 있음을 부정할 수 없다.

[그림 4-1] 보이스피싱 유형별 건수(경찰청)

출처: 금융위원회 2023. 2. 21.자 보도참고자료

보이스피싱의 유형별 건수를 보더라도, 계좌이체형은 계속 감소하여 2018년 30,611건 에서 2021년 3,362건으로 3년 사이 거의 10분의 1 수준으로 줄어든 반면, 대면편취형은 2018년 2,547건에서 2021년 22,752건으로 3년 사이 거의 10배가 늘어났는데, 이는 위와 같은 조치가 영향을 주었을 것으로 보인다.

그리고 실제로 통신사기피해환급법에 따라 금융회사의 손해배상책임이 인정된 사례들도 찾아볼 수 있다. 예컨대, 금융분쟁조정위원회는 금융회사가 잘못된 업무매뉴얼(금융회사가 적극적으로 송금 또는 이체 여부를 확인하지 아니하고 피해자가 이체 날짜와 이체금액 등을 특정하여 요청하는 경우에만 다른 금융회사에 대해 지급정지를

185) 현새롬, "보이스피싱 범죄수법의 진화와 제도적 대응방안에 관한 연구", 고려대학교 정보보호대학원 정보보호학과 석사학위논문(2021. 8.), 96페이지

요청하도록 되어 있는 업무매뉴얼)에 따라 다른 금융회사에 대한 지급정지 요청을 지연하여 발생한 손해에 대하여 배상하도록 결정한바 있고, 해당 금융회사는 업무메뉴얼을 개정한바 있다.[186] 이외에도, 최근 법원이 금융회사의 본인확인조치나 임시조치의무가 미흡하였음을 이유로 손해배상책임을 인정한 사례들을 찾아볼 수 있다.

먼저, 서울중앙지방법원 2017. 1. 25. 선고 2015가단5300687 판결[187]은 보이스피싱 사기범이 원고의 금융정보를 탈취하여 원고의 피고 은행 정기예금 계좌를 해지하고 해지된 정기예금에서 보통예금계좌로 입금된 47,857,150원을 자신들이 지배하는 다른 계좌로 이체해간 사안에서, 피고 은행의 손해배상책임을 인정하였다. 위 판결은 통신사기피해환급법 제2조의4 제1항 제2호에 의하면, 금융회사는 이용자가 저축성 예금 등 금융상품을 해지하는 경우에 통신사기피해환급법 시행령 제2조의3 제1항 각호에서 정한 방식, 즉 전화, 대면 등의 방법으로 본인확인조치를 하여야 하는데, 피고가 공인인증서를 이용한 이 사건 예금계약 해지의 거래지시를 수신하고 계좌번호, 비밀번호, OTP 응답값 등 접근매체에 관한 정보의 일치 여부의 확인을 통한 본인확인에 더하여 전화, 대면 등의 방법으로 본인확인조치를 하지 않았다는 이유로 본인확인조치의무위반을 인정하였다. 또한 위 판결은 피고 은행이 정기예금 해지 처리시 통신사기피해환급법 제2조의4에서 정한 본인확인조치를 취할 의무를 명백하게 위반하였을 뿐만 아니라 해지되어 입금된 돈의 이체 처리와 관련하여 임시조치를 취할 의무(제2조의5) 등 선량한 관리자로서 금융거래가 안전하게 처리되게 하여 전기통신금융사기를 방지할 의무를 위반하였다고 판단하였다(다만, 피고의 손해배상 책임 범위를 40%로 제한).

서울중앙지방법원 2023. 4. 11. 선고 2021가단5243198 판결[188] 역시 사기범이 메신저피싱을 통해 편취한 원고의 개인정보 등을 이용해 원고를 사칭하여 피고 보험회사로부터 5,000만 원의 약관대출을 받아 편취한 사안에서, 피고 보험회사의 손해배상책임을 인정하였다. 위 판결은 피고 보험회사가 휴대전화를 통한 SMS인증과 공동인

186) 금융감독원 2022. 11. 1.자 보도자료

187) 위 판결에 대하여는 원, 피고 쌍방이 항소하였으나 항소가 모두 기각되었고, 상고심에서도 심리불속행 기각이 되었다.

188) 위 판결에 대하여는 피고가 항소하여 현재 항소심(서울중앙지방법원 2023나21565)이 진행 중이다.

증서를 통한 본인확인절차를 거친 것만으로는, 비대면 전자금융거래 방식으로 이루어진 보험계약대출약정에 따른 대출을 실행함에 있어 이용 명의자의 피해방지를 위하여 전자금융거래법 및 통신사기피해환급법에서 정하고 있는 비대면 전자금융거래시 금융회사 등이 취해야 할 본인확인절차 및 전기통신금융사기에 의한 피해방지를 위한 노력을 제대로 하지 아니하였다고 보고, 원고가 보험계약대출로 인하여 입은 피해에 대하여 이를 배상할 책임이 있다고 판단하였다(다만, 피고의 손해배상 책임 범위를 대출금액의 50%로 제한).

위와 같이 통신사기피해환급법상 손해배상책임을 명시한 본인확인조치의무위반의 경우뿐 아니라, 이용자계좌에 대한 임시조치의무(제2조의5)에 위반한 경우까지 금융회사의 손해배상책임을 인정하는 근거가 될 수 있다는 측면에서 보더라도, 현행 통신사기피해환급법이 보이스피싱 피해 구제로서 실효성이 없다고 단정하기는 어렵다.

나. 피해구제 측면에서의 보완

현행 통신사기피해환급법 등은 금융회사의 책임 및 책임범위와 관련하여 보이스피싱 피해 구제에 한계가 있는 것도 사실이다. 피해구제의 측면에서 좀 더 보완되어야 하는 부분을 살펴보면, 다음과 같다.

첫째, '본인확인조치' 등 피해방지의무를 통신사기피해환급법상 은행업[189]을 수행하는 금융회사와 자본시장법상 금융기관 및 보험회사에만 지우고 있다는 점이다. 신용카드회사, 할부금융회사와 같은 여신전문금융회사, 대부업체는 제외되고 있다. 이로 인해 보이스피싱범이 부정하게 취득한 피해자의 개인정보 및 금융정보로 피해자의 인증서 등을 발급받아 신용카드사나 대부업체로부터 대출을 받아 가로채는 경우 해당 신용카드사나 대부업체가 본인확인조치를 소홀히 하더라도 통신사기피해환급법상 손해배상책임이 인정되지 않는다. 실제로 대법원 2018. 3. 29. 선고 2017다257395 판결은 「대출신청의 경우, 휴대전화 등을 이용한 본인확인절차를 거치도록 한 '전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법' 제2조의4 제1항의 규정은 대부

189) 은행법 제2조 제1항 제1호는 "은행업"을 「예금을 받거나 유가증권 또는 그 밖의 채무증서를 발행하여 다수인으로부터 채무를 부담함으로써 조달한 자금을 대출하는 것을 업(業)으로 하는 것」으로 정의하고 있다. 즉, 수신과 여신을 하는 업으로 정하고 있다.

업자에게 적용되는 규정이 아니므로, 이 규정을 근거로 피고들이 휴대전화 등을 이용한 본인확인절차를 거쳤어야 한다고 보기도 어렵다.」고 판단한바 있다. 따라서 '본인확인조치'의무가 적용되는 범위에 신용카드사 등 여신전문금융업체와 대부업체도 포함되도록 개정할 필요가 있다.

둘째, 손해배상책임이 인정되는 사유에 있어 '본인확인조치'와 '지급정지'를 제대로 하지 않은 경우뿐 아니라, 그 외에도 금융회사 등의 피해 방지의무를 좀 더 구체적으로 정하고, 이에 따른 손해배상책임을 명문화할 필요가 있다. 예컨대, 통신사기피해환급법 제2조의5(이용자계좌에 대한 임시조치) 제1항은 금융회사의 자체점검을 통하여 이용자의 계좌가 전기통신금융사기의 피해를 초래할 수 있는 의심거래계좌(피해의심거래계좌)로 이용되는 것으로 추정할만한 사정이 있다고 인정되면 해당 이용자 계좌의 전부 또는 일부에 대하여 이체 또는 송금을 지연시키거나 일시 정지하는 조치(임시조치)를 하도록 의무화하고 있다. 그러나 위와 같이 피해의심거래계좌로 추정할만한 사정에 대하여는 구체적으로 정하고 있지 않고, 나아가 이에 위반한 경우에 대한 제재규정(과태료 부과 등)이 따로 없으며, 손해배상책임 규정도 없다. 앞서 살펴본 바와 같이, 법원이 통신사기피해환급법 제2조의5에 따른 임시조치의무를 위반한 경우 역시 금융회사의 손해배상책임을 인정하는 근거로 삼고는 있으나, 이를 판단할 수 있는 세부규정이 마련되지 않는 한 사실상 선언적인 것에 그칠 가능성이 있다. 따라서 의심거래계좌로 추정할만한 사정에 대하여는 시행령이나 고시로 위임하는 규정을 두고, 하위 법령에서 이를 구체적으로 정할 필요가 있다.

한편, 앞서 예로 든 서울중앙지방법원 2017. 1. 25. 선고 2015가단5300687 판결은 해당 사안의 이체 거래(약 1시간 30분 동안 18차례 다수 계정으로 이체)와 관련하여, 금융위원회가 2014. 6. 마련한 '금융회사 정보기술(IT)부분 보호업무 이행지침'에서 금융회사에게 이상금융거래탐지시스템을 구축·운영하도록 하면서 이상금융거래의 예시로 들고 있는 사유(동일 단말에서 단시간 동안 다수의 계정으로 전자금융거래가 발생하는 경우)에 해당함을 이유로 피고가 임시조치의무를 위반한 것으로 판단한바 있다. 세부기준에 대한 법령의 위임이 없었음에도, 과실 유무 판단의 근거로 사용되었다는 점에서 의미가 있다.

셋째, 대면편취형 보이스피싱의 경우에도, 금융회사의 피해 방지 책임이 인정되는

예시규정을 둘 필요가 있는지 검토할 필요가 있다. 현행 통신사기피해환급법은 금융회사의 피해 방지 책임과 관련하여 대출 신청이나 금융상품 해지시 본인확인조치의무(제2조의4)와 피해의심거래계좌에 대한 임시조치의무(제2조의5)와 같이 주로 비대면편취형 보이스피싱을 염두에 둔 경우에 대하여만 규정하고 있다. 그러나 금융회사를 활용한 기존의 비대면편취형 보이스피싱이 어려워지자 최근에는 피해자와 직접 현장에서 만나 피해금을 건네받는 대면편취형 보이스피싱이 증가(2019년 3,244건, 2020년 15,111건, 2021년 22,752건, 2022년 14,053건)하는 추세[190]이고, 이때에도 경우에 따라서는 금융회사의 고객보호의무가 인정될 수 있기 때문이다. 예컨대, 통신사기피해환급법 제2조의4 제1항 각호의 경우 일상적인 입출금 거래가 아니고, 계약 단계에서부터 금융소비자 보호를 위하여 다소 까다로운 절차를 거치도록 하는 금융상품이다{대출성 상품의 경우는 금융소비자 보호에 관한 법률에 따른 적합성원칙(제17조), 적정성원칙(제18조)이 적용되고, 예금성 상품의 경우도 계약의 해지·해제에 대하여 설명의무 대상으로 하고 있다(제19조 제1항 제1호 다목, 같은 법 시행령 제13조 제5항}. 즉, 피해자가 보이스피싱 사기범에게 속아 사기범(현금수거책)에게 교부할 돈을 마련하기 위해 대출을 받거나, 정기적금을 해지하는 경우로서 이상금융거래로 의심될만한 사정이 있는 경우를 생각해 볼 수 있다. 이런 경우 은행 창구에서 피해자에게 대출을 받으려는 이유나 적금을 해지하는 이유를 물어보고(대출신청서나 해지신청서 양식에 누군가로부터 전화를 받고 방문하였는지 기재하도록 하는 방법도 있다), 의심스러운 정황이 없는지 생각할 시간을 버는 것만으로도, 피해발생을 줄일 수 있다(아래 예시로 든 기사 참조). 제한적으로나마 위와 같은 거래시 금융회사가 조치해야 할 최소한의 사항만이라도 정할 필요가 있는 이유다.

- 경남신문 2023. 7. 31. 기사 “김해서부서, 보이스피싱 막은 경남은행 직원에 감사장” : 은행을 찾은 한 고객이 같은 날 수백만원의 현금 인출과 다른 은행의 계좌를 해지하고 이체한 5200만원을 인출하려고 하자 적극적인 상담과 설득 끝에 신속하게 지급을 정지하고 112 신고로 보이스피싱 피해를 막은 사례.
- 중부일보 2023. 7. 12. 기사 “안양동안경찰서, 보이스피싱 막은 은행 직원에 감사

190) 금융위원회 ‘제2차 금융분야 보이스피싱 대응방안(2023. 2. 28)’, 1페이지

장·포상금 전달" : 은행을 방문한 30대 남성이 여자친구 프로포즈 비용을 마련해야 한다며 만기되지 않은 적금을 해약하고 그 중 1천500만 원을 성급히 다른 계좌로 송금하려하고, 또 그의 휴대전화로 '검사'라고 표기된 문자메시지가 계속 수신되는 것을 보고 피해자를 설득, 송금을 제지시킨 사례.

- 경남도민일보 2023. 3. 23. 기사 "양산경찰서 보이스피싱 막은 은행 직원 감사장" : 피해자가 급하게 3,000만 원을 신용으로 대출받아 가려는 점을 수상하게 여기고 경찰에 신고한 사례.

한편, 최근 대면편취형 보이스피싱 피해자에 대하여도 지급정지와 피해금환급의 구제절차가 가능하도록 '전기통신금융사기'의 정의에 자금을 교부받거나 교부하도록 하는 행위(제2조 제2호 다목)를 포함시키는 내용의 통신사기피해환급법 개정(2023. 5. 16. 법률 제19418호)이 되기는 하였다. 그리고 이와 관련하여 금융위원회는 대면편취의 경우 자금의 송금·이체 기록이 없어 피해자가 사기이용계좌를 특정할 수 없으므로 경찰이 범죄현장 검거 등 수사과정에서 계좌를 특정하여 지급정지를 신청할 수 있다고 설명[191]하고 있다. 그러나 대면편취형의 경우 사기범이 현금을 교부받아가는 방식이지 계좌를 이용하는 것이 아니기 때문에, 이러한 지급정지 및 피해금환급 절차를 통한 피해구제를 기대하기는 어렵다. 따라서 대면편취형 보이스피싱 피해자의 경우에 대하여는 앞서 언급한 바와 같은 별도의 피해방지조치가 필요하다.

2. 가해자에 대한 손해배상청구(형사절차상의 피해구제 절차 포함)

가. 현금수거책, 인출책

보이스피싱의 경우 인출책이나 수거책이 검거되는 경우는 종종 있으나, 사기범행의 주범들이 검거되지 않는 경우가 많다보니, 관련 민사상 손해배상 청구 소송은 거의 대부분 인출책이나 수거책 또는 사기이용계좌 예금주를 상대로 한 경우에 국한되고 있다. 이와 관련하여, 최근 하급심에서 보이스피싱과 관련하여 선고된 판결례들을 예로 들어 보면 아래 표와 같다. 아래 표에서 볼 수 있듯이, 대면편취형 보이스피싱이

191) 금융위원회 2023. 2. 21.자 보도참고자료, 2페이지

늘면서 현금수거책이 검거되는 사례가 증가하였고, 이와 더불어 보이스피싱 가담 사기범을 상대로 한 민사소송도 증가하였지만, 대부분 현금수거책 또는 사기이용계좌 예금주를 상대로 한 사건들이다.

[표 4-1] 보이스피싱 사기범을 상대로 한 최근 손해배상 소송 판결례

사건	피고의 가담유형	선고결과(원금만 표시)
고양지원 2021가단4348	위조된 금융위원회 위원장 명의 공문을 피해자에게 제시하고 피해자로부터 현금 4,000만 원 교부받음(수거책)	피고는 원고에게 4,000만 원 지급(원고 전부 승소)
고양지원 2021가단9602	피해자에게 금융기관 직원으로 행세하여 피해자로부터 현금 3,300만 원을 수거하여 전달(수거책)	피고는 원고에게 3,300만 원 지급(원고 전부 승소)
장흥지원 2022가단5858	피해자로부터 현금 9,872만 원을 교부받아 전달(수거책)	피고는 원고에게 59,233,000원 지급(원고 일부 승소-책임제한 40%)
서울남부지방법원 2021가단249586	은행직원을 사칭하여 피해자로부터 현금 2,000만 원을 교부받아 송금(수거책)	피고는 원고에게 1,600만 원 지급(원고 일부 승소-책임제한 20%)[192]
서울남부지방법원 2021가단255581	피고 B : 돈을 받고 보이스피싱범에게 접근매체 대여, 피해자로부터 위 피고 계좌로 피해금 25,800,000원 입금(사기이용계좌 예금주) 피고 C : 보이스피싱에 이용되는 줄 모르고 환전에 이용되는 것으로 생각하고 자신의 계좌로 보이스피싱 피해금 입금받아 전달(사기이용계좌 예금주)	피고 B는 원고에게 1,032만 원 지급(원고 일부 승소-책임제한 60%) 피고 C에 대한 청구는 기각
서울중앙지방법원 2020가단5042343	피고들 계좌로 보이스피싱 피해금이 3,170만 원 및 2,200만 원 각 입금(사기이용계좌 예금주)	원고 청구 기각
서울중앙지방법원 2021가단5344800	수사기관 소속 직원으로 사칭하여 피해자로부터 47,092,000원을 교부받음(수거책)	피고는 원고에게 32,964,400원 지급(원고 일부 승소-책임제한 30%)
수원지방법원 2021가합11865	금융감독원 직원을 사칭하여 피해자로부터 현금 7,000만 원을 교부받음(수거책)	피고는 원고에게 4,900만 원 지급(원고 일부 승소-책임제한 30%)[193]
수원지방법원 2022가단552137	위조된 금융위원회위원장 명의 공문서를 피해자에게 교부하고, 현금 5,000만 원을 교부받음(수거책)	피고들은 원고에게 2,200만 원 지급(원고 일부 승소-책임제한 30% 및 형사합의금으로 받은 1,300만 원 공제)
수원지방법원 2021가단75125	금융위원회 직원을 사칭하여 피해자로부터 현금 3,500만 원을 교부받음(수거책)	피고는 원고에게 3,500만 원 지급(원고 전부 승소)-피고는 책임제한 주장을 하였으나, 받아들이지 않음

또한 손해배상 청구 소송을 통해 승소판결을 받더라도, 대부분 인출책이나 수거책을 상대로 한 경우가 대부분인데, 이들은 자력이 없는 경우가 거의 대부분이어서 실제 소송을 통해 배상을 받은 사례는 많지 않다. 그럼에도, 별도의 민사소송을 통해 손해배상을 받으려면 적지 않은 소송비용과 시간이 소요된다. 따라서 보이스피싱 범죄에 가담한 가해자에 대한 손해배상 청구의 실효성을 높일 수 있는 제도적 보완장치가 필요하다.

나. 신속한 재판을 받을 제도적 장치

피해자들의 소송비용 부담을 덜어주고, 신속한 재판을 받을 수 있도록 하는 제도적 장치가 필요하다. 이와 관련하여 현행법상 활용할 수 있는 제도로는 ① 범죄피해자 보호법상 형사조정제도(제41조)와 ② 소송촉진 등에 관한 특례법(이하 '소촉법'으로 약칭한다)상 배상명령제도(제25조)가 있다. 그런데, 형사조정제도의 경우 조정이 성립되더라도 민사판결과 같이 강제집행 권원이 되지 못한다는 한계가 있고, 배상명령제도의 경우 실무상 법원이 실제로 배상판결을 하지 않는 경우가 여전히 많다는 한계가 있다. 위 두 제도의 실효성 확보와 활성화를 위한 제도적 보완이 필요하다.

그동안 이와 관련한 제도개선을 논하는 연구논문은 상당수 나왔으나, 현 시점에서는 각 제도를 따로 따로 놓고 개선하기 보다는 일련의 절차로 연계하여 구제하는 방안을 논의할 필요가 있어 보인다. 위 두 제도는 모두 별도의 민사소송 절차를 거치지 않고 피해자의 피해회복을 신속하게 하려는 것으로서 사법기관이 그 운영주체라는 점에서 공통됨에도, 현재 두 제도는 서로 다른 법령에서 규율하고 있고, 이를 운영하는 주체와 절차도 별개로 진행하고 있다. 형사조정절차가 완료된 후 의무이행을 강제할 방법이 없고, 그 이행을 담보할 장치가 없다는 형사조정제도의 근본적인 한계 역시 양 절차가 연계되지 않고 분리·절연되어 있다는 점에서 기인하는 측면이 있다. 그럼에도 아래에서 보는 바와 같이 최근 배상신청 건수와 배상신청 인용 비율은 현저히 늘어난 바 있다.[194] 배상명령이 기재된 유죄판결서 정본은 민사집행법상 집행력 있는

192) 당초 원고는 위 2,000만 원 외에도, 1,170만 원도 피고에게 교부하였고, 이에 대하여도 손해배상청구를 하였으나, 법원은 이에 대하여는 기각함.

193) 당초 원고는 보이스피싱 피해로 입은 전체 손해에 대하여 손해배상청구를 하였으나, 법원은 피고가 형사처벌을 받은 위 7,000만 원 건에 대하여만 배상책임을 인정함.

민사판결 정본과 동일한 효력이 있어(소촉법 제34조 제1항), 이러한 집행력이 부여되지 않는 형사조정제도에 비하여 더 유용하다. 그러나 배상명령 역시 유죄판결의 선고와 동시에 하여야 하기 때문에, 결국 형사재판이 끝날 때까지 장시간이 소요되고, 법원이 여전히 배상신청을 각하하는 비율이 높기 때문에 그 이용률 증대에 한계가 있다.

[표 4-2] 연도별 배상명령 사건 처리 현황

	2015	2016	2017	2018	2019	2020	2021
접수건수	6,799	9,245	8,181	9,826	14,873	26,581	43,437
처리건수	6,176	8,887	8,125	8,914	13,598	18,247	36,176
인용건수	1,820	2,278	2,758	3,699	6,254	9,116	14,945
기각건수	3,962	6,211	4,974	4,820	6,957	8,365	20,124

출처: 사법연감, '기타' 및 '취하 · 기타'는 생략함

[표 4-3] 배상신청 각하 사유 분석표

사 건	배상신청 각하 이유	가담 형태
대구지방법원 2022고합483 등	배상신청인들에 대한 손해배상책임은 책임제한 가능성이 있어 피고인의 배상책임의 범위가 명백하다고 보기 어려움	수거책
대구지방법원 2023고단485	배상신청인과 합의하였고, 현금수거책으로 활동한 것이므로, 배상신청인에 대한 배상책임의 유무 및 범위가 명백하지 아니함	수거책
대전지방법원 2022고단3607	배상신청인과 합의하는 한편 편취금액 전액 이상을 이체하여 지급하였으므로, 배상책임의 유무 또는 범위가 명백하지 않음	수거책
부산 서부지원 2022고단2454	소송촉진 등에 관한 특례법 제32조 제1항 제3호(합의)	수거책
서울북부지방법원 2023노180	피해자와 합의하였고, 이에 따라 배상책임의 유무 및 범위가 명확하지 않게 됨	?
서울중앙지방법원 2023고단542	소송촉진 등에 관한 특례법 제32조 제1항 제3호(피고인이 배상신청인과 합의하였으므로)	수거책

194) 최근 이와 같이 배상명령의 신청 건수와 인용율이 급격히 증가한 원인을 명확히 알 수는 없지만, 그 시기에 특별한 법 개정이나 사법행정 차원의 다른 특별한 시도가 없었다는 점을 고려하면, 이런 현상은 배상명령제도에 대한 근본적인 인식 변화에서 기인한 것은 아니고 배상명령이 쉽게 인정되는 특정한 종류의 사건이 우연히 이 시기에 많이 발생한 것 때문으로 추측된다는 견해도 있다(박성은, "배상명령제도 활성화를 위한 절차 개정안-독일의 부대소송제도에 대한 검토를 중심으로-", 법학논고 제81집(2023. 4.), 208페이지).

사 건	배상신청 각하 이유	가담 형태
전주지방법원 2023고단491	피고인이 배상신청 대상 각 범행에 가담한 동기와 경위, 수행한 역할 및 가담한 정도, 범행으로 취득한 이익 등에 따라 과실상계 또는 책임제한이 고려될 수 있는 등 배상책임의 범위가 명백하지 않을 뿐 아니라, 피고인이 해당 피해자와 합의를 하거나 피해액 중 일부를 공탁하기까지 하여 배상명령을 하는 것이 타당하지 않음	수거책
창원지방법원 2023고단100	피고인이 범행에 가담한 경위 및 정도, 사기 피해가 발생한 경위 등에 비추어 배상책임 범위가 명백하지 아니함	수거책

위 각 표에서 볼 수 있는 것처럼, 배상명령의 경우 신청건수도 2021년 연간 4만 3천여 건으로 증가하였을 뿐 아니라, 그 인용률도 2017년까지는 불과 20~30%대에 불과하다가 그 이후로는 40%~50% 가까이 높아졌다. 매우 고무적인 현상이다. 소송촉진 등에 관한 특례법상 배상명령제도와 범죄피해자 보호법상 형사조정제도가 연계될 경우 집행력 확보와 신속한 피해구제라는 두 가지 문제점을 보다 실효적으로 해결할 수 있다는 기대를 할 수 있는 것도 이러한 배경을 바탕으로 한다.

다. 제도의 실효성 도모

1) 형사조정 기간의 확대

형사조정 절차를 기소 전 단계까지로만 한정하지 않고, 기소 후 공판절차 진행 중일 때까지 진행할 수 있도록 하여야 한다. 기소 후에는 별도의 형사조정 절차가 없다보니 피해자는 피의자의 인적사항이나 연락처를 알지 못하여, 반대로 피의자 역시 피해자와 따로 연락할 수 없거나 피해자가 피의자와 접촉하기를 꺼려하여 당사자간 합의진행이 어려운 경우도 많다. 현행 제도 하에서는 기소 후에는 당사자간(또는 대리인인 변호사와 변호인을 통해) 사적 합의를 한 후 형사재판에서 합의서를 제출하는 방식으로 진행할 수밖에 없다. 그리고 앞서 살펴본 것처럼, 당사자간 합의가 된 경우 오히려 배상신청은 '배상명령을 하는 것이 타당하지 아니하다고 인정되는 경우'(소촉법 제32조 제1항 제3호)로 보아 각하되고 있다. 실무상 형사절차에서 합의하는 경우 피해금액의 전부가 아닌 일부를 지급하는 조건으로 처벌불원의 의사표시가 담긴 형사합의만 하고 나머지 손해배상채무는 잔존하는 형태의 합의(민·형사 분리 합의)나 전체 배상할 금액을 합의하고 이중 일부를 일시금으로 나머지는 추후 분할하여

지급하기로 하는 형태의 합의도 많이 이루어지고 있는데, 이처럼 당사자간 합의가 되었음에도, 오히려 배상신청은 각하되는 아이러니한 상황이 발생하고 있는 것이다. 피의자 입장에서는 감형사유로 삼기 위해, 피해자는 피해회복을 위해 합의를 원하는 수요가 있음에도, 오히려 절차가 이를 뒷받침하지 못하는 실정이다. 이런 이유로 범죄피해자 보호법상 설치된 형사조정위원회의 형사조정 대상 사건의 범위와 형사조정기간을 수사단계 이후 공판절차 종료시까지 확대할 필요가 있다.

2) 형사조정이 성립된 경우 합의된 내용을 법원에 송부하여 배상명령 신청 또는 공판조서로 작성

형사조정이 성립된 경우 검사는 해당 사건을 기소하는 경우에는 기소시 공소장과 함께, 기소유예시에는 기소유예 처분 즉시 법원에 형사조정결정문[195]을 송부하고, 피해자를 위하여 배상신청을 할 수 있도록 하고, 법원은 공판이 개시되기 전이라도 배상명령을 별도로 할 수 있도록 할 필요가 있다. 이미 형사조정 절차에서 당사자간 합의가 된 경우이기 때문에 법원으로서는 형사조정 성립 후 배상명령시까지 사이에 피고인(또는 피의자)이 조정사항을 이행한 부분(즉, 피해변제를 한 부분)이 있는지 확인 후(민사소송에서 답변서를 제출하는 것처럼, 일정기한을 정하여 의견서를 제출받는 방식 등) 배상명령을 하면 된다.

3) 기소되어 공판이 개시된 후의 형사조정과 형사소송 절차에서의 화해 제도 활용

기소 후에도 피고인 또는 피해자는 법원에 형사조정회부를 신청할 수 있도록 하고, 그 신청이 있는 경우 법원은 형사공판 절차 진행과는 별개로 형사조정위원회 조정회부를 할 수 있도록 하면 된다. 그리고 기소 후 진행된 형사조정절차에서 조정이 성립되면, 형사조정결정문을 법원에 송부하고, 법원은 소촉법 제36조(민사상 다툼에 관한 형사소송 절차에서의 화해) 제1항[196]에 따른 신청이 있는 것으로 보아 형사조정결정문 내용을 공판조서에 기재하면 된다. 이 경우 그 공판조서는 확정판결과 같은

---

195) 범죄피해자 보호법 시행규칙 별지 제25호 서식

196) 제36조(민사상 다툼에 관한 형사소송 절차에서의 화해) ① 형사피고사건의 피고인과 피해자 사이에 민사상 다툼(해당 피고사건과 관련된 피해에 관한 다툼을 포함하는 경우로 한정한다)에 관하여 합의한 경우, 피고인과 피해자는 그 피고사건이 계속 중인 제1심 또는 제2심 법원에 합의 사실을 공판조서에 기재하여 줄 것을 공동으로 신청할 수 있다.

효력을 가지게 되어 집행력이 있게 된다(소촉법 제36조 제5항, 민사소송법 제220조). 수사단계에서 형사조정이 결렬된 경우라도, 기소 후에도 1차례에 한하여 형사조정을 신청할 수 있도록 하되, 형사공판과는 별개로 진행함으로써 재판절차 지연을 막으면서, 동시에 형사조정제도의 활성화와 집행력 확보라는 목표를 달성할 수 있다.

4) 의무이행 정도를 양형에 반영

위와 같이 형사조정이 성립된 경우 판결선고 전 피고인이 조정사항을 이행하였는지 여부를 확인한 후 이를 양형에 반영함으로써, 그 실효성을 높일 필요가 있다. 또한 사실심 판결 당시 형사조정이 성립되었고, 그러한 점이 양형에 반영되었으나 피고인이 조정사항을 이행하지 않는 경우에 대비할 필요도 있다(다만, 이에 대하여는 검토할 사항이 너무 많고, 보이스피싱 피해구제에 한정된 주제가 아니므로 일단 향후 연구과제로 남기기로 한다).

라. 집단소송이나 단체소송 고려

이외에도, 피해자 개개인이 소송을 하는데 따른 비용부담과 보이스피싱 범죄가 조직적으로 이루어지고 있어 다수의 피해자가 발생하는 점을 고려할 때, 집단소송이나 단체소송을 도입하는 방안도 검토할 필요가 있다(현행법상 집단소송으로는 증권관련 집단소송법상 집단소송이 있고, 개인정보보호법상 단체소송(제51조)이 있다). 보이스피싱 가해자에 대한 형사사건에서 형사조정 및 배상명령 제도를 활용하는 것은 조직적 범죄로서 다수의 피해자가 발생하는 보이스피싱 범죄의 특성상 한계가 있다. 특히 다수의 피해자가 배상명령을 신청하는 경우 형사절차에서 각 피해자별로 합의 여부나 손해배상범위까지 판단하는 것이 쉽지 않기 때문에, 형사재판 절차에서 배상명령을 하는 것이 자칫 본래의 재판인 형사재판에 지장을 줄 우려가 있다(이런 이유로 소촉법 제32조 제1항 제3호에 기해 각하될 가능성이 높다).

다만, 이는 보이스피싱 범죄의 경우뿐만 아니라, 다단계 사기범죄 등과 같이 조직적 사기범죄 사건에서의 피해구제와 관련하여 공통되는 문제이고, 그동안의 수많은 논의에도 불구하고, 현재까지 극히 일부 영역에만 도입된 현실을 고려할 때, 좀 더 장기적인 검토 과제로 보아야 할 것이다.

제2절 | 범죄피해자 구조 대상의 확대 및 피해회복위원회 설치 방안

1. 범죄피해자 보호법

범죄피해자 보호법은 구조대상 범죄피해를 받은 사람(이하 '구조피해자'라 한다)이 피해의 전부 또는 일부를 배상받지 못한 경우나 자기 또는 타인의 형사사건의 수사 또는 재판에서 고소·고발 등 수사단서를 제공하거나 진술, 증언 또는 자료제출을 하다가 구조피해자가 된 경우에 한하여 범죄피해 구조금을 지급하도록 하고 있다(제16조). 그리고 "구조대상 범죄피해"에 대하여는 대한민국의 영역 안에서 또는 대한민국의 영역 밖에 있는 대한민국의 선박이나 항공기 안에서 행하여진 사람의 생명 또는 신체를 해치는 죄에 해당하는 행위로 인하여 사망하거나 장해 또는 중상해를 입은 것으로 정의하고 있어, 보이스피싱과 같은 재산범죄 피해자는 그 대상에서 제외하고 있다. 따라서 보이스피싱 피해자의 경우 범죄피해자 보호법에 따른 구조금 지급 대상에 포함시킬 것인지가 논의될 수 있다.

2. 보이스피싱 피해자를 구조금 지급 대상

보이스피싱 피해자를 구조금 지급 대상에 포함시킬 것인지의 논의는 다른 재산범죄와의 형평성 문제 및 헌법 제30조와의 관계, 구조금 재원을 어떻게 마련할 것인지, 나아가 구조금 지급범위는 어떻게 할 것인지의 문제로 연결된다.

가. 먼저, 다른 재산범죄와의 형평성 문제에 대하여는 다른 재산범죄는 배상명령제도를 통해 해결할 수 있는 방안이 있지만 상대적으로 검거율이 낮은 보이스피싱 범죄는 가해자가 검거되지 않는다면 피해회복을 할 수 있는 방법이 사실상 없고, 따라서 가해자 검거가 되지 않은 범죄피해자에 대해서는 개정을 통해 지급될 수 있는 방안을 모색해야 한다는 견해가 있다.[197] 그러나 보이스피싱 범죄의 경우 가해자가 검거되어

197) 이동임, "보이스피싱범죄 대응 및 피해회복 방안", 피해자학연구 제18권 제2호(2010. 10.), 280

가해자를 상대로 손해배상 청구 소송에서 판결을 받거나 형사사건에서 배상신청을 하더라도, 거의 대부분 가해자가 무자력이거나 이미 재산을 빼돌려 강제집행이 어렵다. 가해자가 검거되지 않는 피해자에 대하여만 구조금을 지급하게 될 경우 오히려 가해자가 검거된 경우 실제 손해배상을 받지 못하였더라도 구조금을 지급받지 못하는 불균형이 발생한다. 또한 가해자가 장시간 검거되지 않았다가 검거되는 경우는 어떻게 할 것인지도 문제다. 보이스피싱 피해자의 경우 가해자 검거 여부를 기준으로 구조대상에 포함시킬지 여부를 결정할 수 없는 이유다.

범죄피해자 보호법은 헌법 제30조(타인의 범죄로 인하여 생명·신체에 대한 피해를 받은 국민은 법률이 정하는 바에 의하여 국가로부터 구조를 받을 수 있다)에 근거하고 있고, 이에 구조금 지급대상범죄를 생명 또는 신체를 해하는 범죄에 한정하는 것으로 보인다. 그러나 범죄피해자를 구조하여야 하는 국가의 의무는 반드시 생명·신체에 대한 범죄에 한정되는 것은 아니므로, 범죄피해자 보호법이 구조대상 범죄의 범위를 일부 재산범죄로 확대한다고 하여 위헌의 소지를 갖게 되는 것은 아니라고 본다. 국가는 신체장애자 및 질병·노령 기타의 사유로 생활능력이 없는 국민에 대하여 보호의무가 있으므로(헌법 제34조), 국민이 재산범죄로 인해 생활능력이 없게 되었다면, 국가는 그 국민에 대하여도 보호할 의무가 있다. 또한 범죄피해자 보호법의 목적은 궁극적으로는 '범죄피해자의 복지 증진'에 기여하는데 있다. 따라서 보이스피싱 범죄 등 일부 재산범죄로 인하여 생활능력에 지장을 받게 된 피해자를 구조대상에 포함시켜 구조하는 것은 헌법 및 범죄피해자 보호법의 취지에도 부합한다.

그리고 재산범죄간 형평성의 관점에서 보면, 보이스피싱 범죄에 한하여 범죄피해자 보호법상 구조대상에 포함시킬지를 논의할 것은 아니다. 재산범죄 중 어떤 유형의 범죄를 어떠한 기준으로 구조대상범죄에 포함시킬 것인가의 관점에서, 보이스피싱 범죄피해자의 경우 구조대상에 포함되는 것이 적절한 것인가의 논의가 이루어져야 할 것이다. 이에 구조대상범죄에 포함시킬지 여부의 판단기준으로 제시해 볼 수 있는 것으로는, 피해자의 경제적 능력, 피해의 정도, 타 구제절차에 의한 피해회복 가능성 등이 있다.

페이지

나. 다음으로 보이스피싱 범죄피해자 등 일부 재산범죄 피해자들을 범죄피해자 보호법에 따른 구조금 지급대상으로 할 경우 늘어나게 될 구조금의 재원 마련을 어떻게 할 것인가의 문제이다. 현행 범죄피해자보호기금법은 범죄피해자보호기금의 조성 재원으로 ① 형사소송법 제477조 제1항에 따라 집행된 벌금의 100분의 8(위 법 시행령 제2조 제1항)에 해당하는 금액, ② 범죄피해자 보호법 제21조 제2항에 따라 대위하여 취득한 구상금, ③ 정부 외의 자가 출연 또는 기부하는 현금, 물품, 그 밖의 재산, ④ 기금의 운용으로 인하여 생기는 수익금을 정하고 있다. 그러나 이외에도, 법 개정을 통해 범죄피해자보호기금 조성 재원으로 고려할 만한 것이 더 있다고 본다. 예컨대, 벌금의 일부만 그 재원으로 할 것이 아니라, 범죄자 등으로부터 몰수·추징한 재산의 일부도 고려해 볼 수 있다.

다. 마지막으로 보이스피싱 범죄피해자에게 구조금 지급을 할 경우 그 지급범위를 어떻게 할 것인가의 문제가 있다. 범죄피해자 보호법은 구조금액과 관련하여, 피해자의 전 손해를 구조하는 것이 아니라, 월 실수입액 또는 평균임금에 일정 개월 수를 곱한 금액으로 정하고 있다. 즉, 실 손해의 정도를 고려하되, 일정범위 내로 한정하고 있다. 이는 한정된 범죄피해자보호기금을 고려한 것으로 불가피한 것으로 보인다. 재산범죄의 경우 역시 실제 손해의 규모를 고려하되, 일정범위를 초과하지 않는 것으로 그 기준을 정할 필요가 있다. 특히 재산범죄의 경우 그 손해범위가 천차만별이기 때문에, 실제 손해액 전보에 초점을 맞출 경우 재원 마련의 어려움이 있고, 또한 전 손해에 대한 구조금 지급을 할 경우 잠재적 피해자로 하여금 피해예방을 위한 노력을 하지 않도록 할 우려가 있다. 따라서 구조금 지급 범위의 경우 일정한 상한액의 범위 내에서 전 손해가 아닌 손해액의 일정 비율로 한정할 필요가 있다고 본다.

3. 피해회복위원회 설치 방안

별도의 피해회복위원회를 검찰청 내에 설치하여 검찰에서 사건을 마무리 하고나면 바로 피해회복위원회에서 지급심의를 할 수 있도록 하자는 견해도 있다. 위 견해는 아울러 피해회복이 어려운 노인, 빈곤층 등에 대하여 피해회복위원회에서 심의를 거

쳐 피해금액의 30~50%를 차등 지급하는 안도 제시하고 있다.[198]

충분히 고려해 볼만한 견해이나, 위 견해는 피해구제를 위한 자금을 어디서 충당할 것인지 등에 대하여는 제시하지 않고 있고, 단지 피해회복을 위한 절차적 기구를 제시하는데 그친 점에서 아쉽다. 보이스피싱 범죄피해자를 위하여 별도의 피해회복위원회 설치를 하거나, 피해회복을 위한 기금을 따로 만들기보다는 앞서 살펴본 범죄피해자 보호법상 구조대상범죄에 포함시킬 것인지의 논의와 함께 검토되는 것이 바람직할 것으로 사료된다.

제3절 | 보이스피싱 보험 활성화

1. 보이스피싱 보험의 활성화

가. 보험제도

현실적으로 보이스피싱 범죄피해자의 피해구제에 가장 신속하고 효율적인 방안은 보험제도이다. 다만, 현재 운용 중인 보이스피싱 보험의 경우는 보상금액이 300~500만 원 수준, 최대 보장한도 1,000만 원 수준으로 피해금액에 비하면 턱없이 미흡하고[199], 임의가입이다 보니, 실제로 보험혜택을 볼 수 있는 피해자도 많지 않은 한계가 있다.

정부의 2020. 6. 보이스피싱 척결 종합방안에서도 보이스피싱 피해 구제 지원을 위한 보험상품의 보장 범위를 확대하고 판매채널 등도 확대할 수 있도록 추진(특히 기본 보험 판매 채널 뿐 아니라 통신대리점, 은행 등 금융회사 창구 등에서 다양하게 해당 상품을 안내)하는 방안을 발표한 바 있다.

198) 이동임, "보이스피싱범죄 대응 및 피해회복 방안", 피해자학연구 제18권 제2호(2010. 10.), 276~277페이지

199) 현새롬, "보이스피싱 범죄수법의 진화와 제도적 대응방안에 관한 연구", 고려대학교 정보보호대학원 정보보호학과 석사학위논문(2021. 8.), 99페이지

나. 책임보험 제도의 도입 고려

위와 같이 보이스피싱 보험상품의 임의가입 형태로는 가입률을 높이는데 한계가 있고, 보장범위 역시 너무 제한적이다. 이런 측면에서 자동차손해배상책임보험, 원자력손해배상책임보험, 근로자재해보상보험, 재난배상책임보험, 개인정보 손해배상책임 보장제도 등과 같은 책임보험 제도를 도입하자는 견해는 경청할만하다.[200] 그러나 위 견해 역시 구체적인 보험운영 방식에 대하여는 전혀 언급하지 않고 있다. 무엇보다도, 보이스피싱 관련 보험 상품이 있다는 것조차 홍보가 제대로 되어 있지 않다는 것이 더 문제이다. 결국 보험가입률을 어떻게 높일 것인지와 보험가입금액과 보장범위를 어떻게 현실화할 것인가의 문제로 귀결된다.

다. 보험가입률 증대 방안

1) 타 상품과의 결합판매 또는 부가서비스 판매 방안

이와 관련하여, 보이스피싱 보험 판매 활성화를 위한 대안으로 타 상품과의 결합판매를 제안하는 견해[201]를 경청해 볼만하다. 이 견해는 휴대폰 분실파손 보험과의 결합판매를 그 예로 들고 있는데, 위 보험은 가입자가 천만 명에 육박할 뿐만 아니라, 모바일 진단 기술의 발전으로 향후 높은 성장성이 예상되기 때문이다.

보이스피싱 보험을 단독으로 판매할 경우 그 가입률에 한계가 있을 수밖에 없는 점을 고려하면(더구나 현재는 보험사들이 그 판매를 적극 광고하고 있지도 않다), 위와 같이 타 보험상품과의 결합판매 방안 외에도, 신용카드 회원가입시나 정기적금 등 금융상품 판매시에도 보이스피싱 보험상품을 안내하거나, 아예 그 부가서비스에 가입시키는 방법으로 보이스피싱 보험과 같은 보장을 제공하는 방안도 적극 활용할 필요가 있다. 사실 국내 보험사들이 판매하는 보험상품은 거의 대부분 보이스피싱 전용 보험이 아니라 피싱 및 해킹 등 금융사기를 보험사고로 하는 보험이다. 금융회사

---

200) 현새롬, "보이스피싱 범죄수법의 진화와 제도적 대응방안에 관한 연구", 고려대학교 정보보호대학원 정보보호학과 석사학위논문(2021. 8.), 99페이지

201) 장주성, "금융소비자 보호를 위한 보이스피싱 대응방안 연구-통신사, 제조사, 금융사, 플랫폼 사업자와의 협업을 통한 단계별 대응방안 제안-", 금융감독연구 제9권 제1호(2022. 4.), 147페이지

들로서는 특히 비대면 보이스피싱 사고 발생시 피해자인 고객과의 불필요한 법률분쟁을 줄일 수 있는 이점도 있기 때문에 부가서비스나 보이스피싱 보험에 가입하도록 권유할 실익도 있다. 그리고 실제로 신용카드사의 경우 신규 신용카드 회원을 피보험자로 하는 단체계약(신용카드 무료 단체보험 부가서비스 등) 형태로도 체결하고 있고[202], 또한 신용카드사의 부가서비스 중 하나인 '피싱 및 해킹 금융사기보상'서비스 역시 일종의 보이스피싱 보험 기능을 하고 있다. 예컨대, 신한카드의 경우 '피싱안심' 부가서비스는 '보이스피싱 차단서비스' 외에도 '피싱 및 해킹 금융사기보상' 등을 제공하고 있는데, '피싱 및 해킹 금융사기보상'은 "이용자"의 서비스 가입기간 중 대한민국 내에서 발생한 피싱(Phishing) 또는 해킹(Hacking) 금융사기(스미싱, 파밍, 메모리해킹을 포함)로 인하여 "이용자"의 계좌에서 예금이 부당 인출(사기에 의한 부당 송금 및 이체 포함)되어 "이용자"가 입은 금전적 손실액을 연간 300만 원 한도로 보상하는 서비스이다.[203] 위 부가서비스 이용료는 개인형(1인)의 경우 월 700원(부가세 포함)으로 저렴한 편이나 대신 보상한도가 너무 낮은 단점이 있다. 이에 신한카드는 보상범위를 확대한 '피싱안심Together' 부가서비스도 제공하고 있는데, 위 부가서비스는 1인당 연간 2,500만원 한도로 보상하고, 이용료는 개인형(1인)의 경우 월 6,900원(부가세 포함)이다.[204] 부가서비스의 경우 실효성이 있을 정도로 보상범위를 늘릴 경우 이용료가 비싸다는 단점이 있어 이를 보완할 필요가 있다.

2) 의무보험화 또는 설명의무화 방안

전기통신금융사기와 관련한 보험의 의무보험화나 설명의무화 방안도 고려할만 하다. 특히 비대면 전자금융거래가 급증하여 왔고, 이제는 필수적인 거래방식이 된 상황에서 누구나 전기통신금융사기와 해킹 등으로 인한 사고 발생 위험에 노출되어 있다고 해도 과언이 아니다. 따라서 비대면 전자금융거래를 이용하려는 경우 보험가입을 일정 부분 필수적인 것으로 제도화하거나(예컨대, 1일 이체한도가 3천만 원 이상인 경우 인터넷뱅킹 이용시 보상한도가 1일 이체한도의 1/3이상인 보험에 가입하도록 하는 것), 금융상품 판매자인 금융회사에게 금융상품 판매시 고객에게 피싱 및 해킹

202) 디비손해보험(주) '피싱 · 해킹 금융사기보상보험' 사업방법서 참조
203) 피싱안심 서비스 이용약관 제4조 제1항 제4호
204) 피싱안심Together 이용약관 제4조 제4항

관련 보험상품(앞서 소개한 피싱안심 부가서비스와 같은 부가서비스 포함)에 대한 설명을 하도록 의무화하는 방안도 고려해볼 수 있다. 의무보험화는 다수 국민들의 거부감이 있을 수 있으므로 당장 도입이 쉽지 않을 것으로 보이나, 금융회사의 설명의무에 포함시키는 것은 금융소비자 보호에 관한 법률 제19조(설명의무) 제1항 제4호(그 밖에 금융소비자 보호를 위하여 대통령령으로 정하는 사항)의 위임을 받아 제정된 같은 법 시행령 제13조(설명의무) 제8항 각호에 추가하는 것만으로도 가능하다.

다만, 설명의무 대상으로 하는 경우 피싱 및 해킹 관련 보험상품 설명을 하지 않았을 경우 금융회사의 손해배상책임(금융소비자 보호에 관한 법률 제44조 제2항)과 과태료 부과(위 법률 제69조 제1항 제2호)가 되는 문제가 발생한다. 이 때문에 금융회사들로서는 그 도입에 반대할 가능성이 높다. 그러나 피싱 및 해킹 관련 보험상품 설명을 하지 않은 사실과 피싱이나 해킹으로 인한 손해의 발생 사이에 인과관계가 인정되기는 어려울 것이기 때문에(설명을 듣지 못하여 보이스피싱 보험에 가입하지 않아 발생한 손해는 보이스피싱으로 인한 손해가 아니라 그 손해회복이 안 된 경우에 불과하다), 실제로는 금융회사들이 위 보험상품 설명을 하지 않은 사실만으로 배상책임을 질 가능성은 높지 않다고 사료된다. 그리고 과태료 부과의 경우 현행 금융소비자 보호에 관한 법률 제69조 제1항(1억 원 이하) 제2호, 같은 법 시행령 별표4(과태료의 부과기준)에 따를 경우 과태료가 7천만 원(법인) 내지 3,500만 원(개인)으로 피싱 및 해킹 관련 보험상품에 대한 설명을 하지 않은 것에 대한 과태료치고는 지나치게 과다한 측면이 있으므로, 위 시행령 별표 기준을 별도로 마련할 필요가 있다(예컨대, 과태료 1,000만 원[205] 이하).

라. 보험가입금액과 보장범위의 현실화 방안

최근 보이스피싱 현황을 살펴보면, 계좌이체형을 기준으로 피해자 1인당 피해금액은 2018년 910만 원, 2019년 1,330만 원, 2020년 1,290만 원, 2021년 1,270만 원, 2022년 1,130만 원으로, 2019년 이후 1,100만 원을 초과하는 높은 수준을 유지하고 있다.[206] 지급정지를 통한 환급률을 고려하더라도, 최근 환급률(환급액÷피해금액)이

205) 금융소비자 보호에 관한 법률 시행령 별표4에서 가장 낮은 과태료 수준이 1,000만 원인 점을 감안

26.1%[207]까지 낮아진 상황임을 고려하면, 실제 1인당 피해금액은 평균 1,000만 원 가까이 될 것으로 추정된다. 그리고 이는 어디까지나 1인당 평균적인 피해금액이므로, 실제 피해액은 수천만 원 이상인 경우도 있다. 이에 반해 현재 판매되는 전기통신금융사기 관련 보험의 보험가입금액은 300~500만 원 수준, 최대 보장한도 1,000만 원 수준임을 고려하면, 피해구제에는 미흡한 상황이다. 따라서 보장한도인 보험가입금액을 1,000만 원 이상 수준으로 현실화할 필요가 있다.

그리고 현재 판매되고 있는 전기통신금융사기 관련 보험상품들을 살펴보면, 대면편취형 보이스피싱의 경우 보험사고에 포함되지 않는 경우(즉, 보장범위에서 제외)가 많다. 아래 표에서 보는 바와 같이 삼성화재 '금융사고보상보험(Ⅲ)'의 경우 통신사기피해환급법상 전기통신금융사기로 인한 손해를 보험사고로 하고 있고, '피싱'의 정의규정에서도 개인정보 및 금융정보를 부당하게 얻거나 자금을 송금·이체하도록 하는 등의 수법과 보이스피싱을 포함하도록 규정하고 있어, 대면형과 비대면형 보이스피싱 피해 모두 보장범위에 포함된다. 이에 반하여, 디비손해 '피싱·해킹 금융사기 보상보험', 메리츠화재 '전자금융사기보상보험', KB손해보험 '피싱·해킹금융사기보험(Ⅱ)'의 경우 보험사고를 예금 부당 인출(송금, 인출)과 신용카드 부당사용의 경우로 한정하고 있고, '피싱'의 정의규정에서도 개인정보 및 금융정보를 부당하게 얻어 재산상 이익을 취득하는 행위로만 규정하고 있으며, 그 외 보이스피싱까지 포함하는 내용이 없다. 이런 경우 자금 이체나 송금을 하지 않는 대면편취형 보이스피싱(현금을 특정 장소에 두고 가도록 한 후 수거책이 이를 가져하는 유형도 포함)의 경우 보험사고에 포함되지 않아 보험보상이 되지 않게 된다. 따라서 보험사고에 관한 약관규정을 삼성화재 '금융사고보상보험(Ⅲ)'의 경우와 같이 규정함으로써, 대면편취형 보이스피싱 등에 대하여 보험보장이 될 수 있도록 보장범위를 확대할 필요가 있다.

위와 같이 보험가입금액을 늘리고, 보장범위를 확대할 경우 결국 보험료 인상이 불가피해진다.

---

206) 금융감독원 2023. 4. 20.자 보도자료
207) 금융감독원 2023. 4. 20.자 보도자료

[표 4-4] 현재(2023. 8. 기준) 판매되고 있는 보이스피싱 관련 보험상품의 보험사고 예시

보험회사	상품명	보험사고(보상하는 손해)
삼성화재	금융사고보상보험(Ⅲ)	전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법 제2조(정의)에 따른 전기통신금융사기를 말하며, 피싱, 해킹, 스미싱, 파밍 및 이와 유사한 금융사기를 포함함 * 피싱 : 전화, 전자우편, 휴대전화 문자메세지 등을 사용해서 공공기관, 금융기관, 수사기관, 피보험자의 지인 등 신뢰할 수 있는 사람이나 기업이 보낸 것처럼 피보험자를 기망(欺罔), 공갈(恐喝)함으로써 계좌번호, 비밀번호 등과 같은 개인정보 및 금융정보를 부당하게 얻거나 자금을 송금•이체하도록 하는 등의 수법을 말하며, 보이스피싱(Voice phishing)을 포함(단, 몸캠피싱은 제외).
디비손해	피싱·해킹 금융사기 보상보험	“피싱(Phishing) 또는 해킹(Hacking) 금융사기”(스미싱, 파밍, 메모리해킹을 포함)로 인하여 피보험자 명의의 계좌에서 예금이 부당 인출(사기에 의한 부당 송금 및 이체 포함)되거나 신용카드(직불카드, 현금카드 등 포함)가 부당하게 사용되어 피보험자가 입은 금전적 손해 * 피싱 금융사기 : 사기의 의도를 가진 자가 전화, 인터넷 전자우편 또는 메신저(모바일 메신저 포함) 및 모바일 메세지 등을 사용해서 공공기관, 금융기관, 수사기관, 피보험자의 지인 등 신뢰할 수 있는 사람 또는 기업이 보낸 것처럼 타인을 기망(欺罔)· 공갈 (恐喝)함으로써 비밀번호, 카드 정보와 같이 기밀을 요하는 개인정보 및 금융정보를 부당하게 얻어 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하게 하는 행위를 말하는 것으로, 스미싱(Smishing) 등으로 인한 금융사기를 포함
메리츠화재	전자금융사기 보상보험	“전자금융사기”{피싱(스미싱 포함), 해킹(파밍, 메모리해킹을 포함), 휴대폰 분실 부당결제피해}로 인하여 피보험자 명의의 계좌에서 예금이 부당 인출(사기에 의한 부당 송금 및 이체 포함)되거나 신용카드(직불카드, 현금카드 등 포함)가 부당하게 사용되어 피보험자가 입은 금전적 손해 * 피싱 : 사기의 의도를 가진 자가 전화, 인터넷 전자우편 또는 메신저(모바일 메신저 포함) 및 모바일 메세지 등을 사용해서 공공기관, 금융기관, 수사기관, 피보험자의 지인 등 신뢰할 수 있는 사람 또는 기업이 보낸 것처럼 타인을 기망(欺罔)·공갈(恐喝)함으로써 비밀번호, 카드 정보와 같이 기밀을 요하는 개인정보 및 금융정보를 부당하게 얻어 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하게 하는 행위
KB손해보험	피싱·해킹 금융사기 보상보험(Ⅱ)	“피싱 또는 해킹 금융사기”(스미싱, 파밍, 메모리해킹을 포함)로 인하여 피보험자(계약자의 고객 및 고객의 배우자, 미혼자녀) 명의의 계좌에서 예금이 부당 인출(사기에 의한 부당 송금 및 이체 포함)되어나 신용카드(직불카드, 현금카드 등 포함)가 부당하게 사용되어 피보험자에게 발생한 금전적 손해 * 피싱 : 사기의 의도를 가진 자가 전화, 인터넷 전자우편 또는 메신저(모바일 메신저 포함) 및 모바일 메세지 등을 사용해서 공공기관, 금융기관, 수사기관, 피보험자의 지인 등 신뢰할 수 있는 사람 또는 기업이 보낸 것처럼 타인을 기망(欺罔)· 공갈 (恐喝)함으로써 비밀번호, 카드 정보와 같이 기밀을 요하는 개인정보 및 금융정보를 부당하게 얻어 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하게 하는 행위를 말하는 것으로, 스미싱(Smishing) 등으로 인한 금융사기를 포함.

그러나 보험료 인상에 불구하고 위와 같은 조치는 반드시 필요하다. 현재 판매되는 보험상품들이 보이스피싱 피해구제에 미흡하다는 점과 이 상품을 단독으로 판매하기가 쉽지 않다는 점(즉, 수익성이 떨어진다)이 보험가입률을 높이지 못하는 이유로

작용하는 것으로 추정된다. 따라서 피해구제에 미흡한 점을 보완하고, 다른 보험상품이나 금융상품과 결합하여 판매한다면, 보험료 부담도 상대적으로 줄어들고, 보험가입률과 수익성도 높일 수 있다고 본다. 상품성이 없어서 보험가입률이 부진한 것이므로, 상품성을 갖추면 되는 것이다.

이와 비교하여 살펴보면, 민사소송 등에서 소송비용 부담을 하게 된 경우 변호사비용 등 소송비용을 지급하는 보험상품의 경우도 과거에는 그다지 판매가 많이 이루지지 않았으나 현재는 운전자보험과 같이 많이 판매되는 보험상품에 특약으로 포함되어 판매되는 경우가 상당히 늘고 있다. 그 예를 들어보면, 아래 표와 같다. 아래 표에서 보는 바와 같이 소송에서 패소하여 소송비용을 부담하게 되는 손해를 입게 되더라도, 법상 부담하게 되는 소송비용에 준하여 보험금이 지급되는 수준이다. 이러한 예에서 보듯, 보장범위를 현실화하고, 많이 팔리는 보험상품의 특약으로 포함시켜 판매한다면, 앞서 언급한 문제들을 어느 정도 해결할 수 있을 것으로 기대한다.

[표 4-5] 보이스피싱 관련 보험상 및 특약, 보험금 지급 예시

보험회사	보험상품 및 특약	보험금 지급
삼성화재	무배당 삼성화재 운전자보험 레디For레이디(2306.1)-민사소송 법률비용손해 특별약관	변호사보수의 소송비용산입에 관한 규칙에서 정한 변호사비용의 한도 내에서 피보험자가 실제 부담한 변호사 보수액 중 자기부담금 10만 원 초과 금액(1,500만 원 한도)+인지대 및 송달료(500만 원 한도)
디비손해	참좋은라이더+보험2301-민사소송법률비용손해(실손) 특별약관	
현대해상	무배당 뉴하이카운전자상해보험(Hi2304)-법률비용손해(민사소송)보장 특별약관	

2. 분담금 내지 부담금으로 조성한 피해구제기금에 의한 피해구제사업

가. 적합한 모델의 고려

사실 피해구제를 위해 가장 적합한 모델로 고려해 볼 수 있는 것은 자동차손해배상보장법상 의무보험 형태의 책임보험과 연계된 자동차손해배상 보장사업(제30조)과 약사법상 의약품 부작용 피해구제사업(제86조)이다.

나. 자동차손해배상보장법상 보장사업(통상 '정부보장사업'이라 한다)

자동차손해배상보장법상 보장사업(통상 '정부보장사업'이라 한다)은 자동차보유자를 알 수 없는 자동차의 운행으로 사망하거나 부상한 경우, 보험미가입자가 손해배상책임을 지게 되는 경우, 자동차보유자를 알 수 없는 자동차의 운행 중 해당 자동차로부터 낙하된 물체로 인하여 사망하거나 부상한 경우와 같이 가해자를 알 수 없거나 자동차보험을 통해 피해구제를 받을 수 없는 자동차사고피해자에게 책임보험의 보험금 한도에서 그가 입은 피해를 보상하도록 하고 있다(제30조). 그리고 위와 같은 보장사업의 재원은 자동차보험 책임보험 가입자가 내는 책임보험료의 100분의 5 이내에서 대통령령(현행 100분의 1)으로 정하는 분담금으로 마련하고 있다(제37조). 보이스피싱 범죄의 경우 가해자를 검거하지 못하여 손해배상 청구조차 하지 못하는 경우가 대부분인데, 자동차손해배상보장법상 정부보장사업 역시 가해자를 알지 못하는 등의 경우에 대비한 피해구제 제도라는 점에서 유사한 측면이 있다.

한편, 자동차손해배상보장법상 의무보험은 사고발생 위험에 불구하고 자동차운전을 피할 수 없으므로, 사고발생시 피해자 구제를 위해 그 가입을 강제하고, 또한 그 보험료 중 일부를 피해구제를 위한 분담금으로 징수하여 정부보장사업의 재원으로 사용하고 있다(현재 위 사업은 자동차손해배상진흥원에서 담당하고 있다). 그런데, 금융거래 역시 보이스피싱 범죄와 같은 위험에 노출되더라도 일상생활 영위를 하는데 있어 피할 수 없으므로, 보험보호의 필요성이 있다는 점에서는 비슷한 측면이 있다. 다만, 자동차보험의 경우 자동차보유자(보통은 자동차소유자)는 자동차 운행으로 인한 위험을 야기하는 자가 보험료를 부담하는 것이지만, 금융거래의 경우 금융회사나 그 이용자가 사고위험을 야기하는 자는 아니라는 점에서 차이가 있다. 따라서 의무적으로 보험에 가입하게 할 경우 그 보험가입 주체를 누구로 할 것인지와 보험료의 최종 부담은 누구에게 지울 것인지의 문제가 남게 된다. 금융소비자에게 지우든, 금융회사에 지우든 이의를 제기할 수 있는 상황이다.

다. 약사법상 의약품 부작용 피해구제사업

약사법상 의약품 부작용 피해구제사업은 식품의약품안전처장이 의약품의 제조업

자, 품목허가를 받은 자 및 수입자로부터 의약품 피해구제 부담금을 부과·징수하여(제86조의2) 마련한 재원으로, 의약품을 사용한 사람이 그 의약품의 부작용으로 인하여 질병에 걸리거나 장애가 발생하거나 사망한 때 피해구제급여를 지급(제86조의3)하는 제도이다(현재 피해구제사업은 한국의약품안전관리원에서 위탁받아 하고 있다). 약사법은 의약품 판매 등을 통해 이익을 얻는 자에게 의약품 부작용 피해구제를 위한 분담금 지급의무를 지우고 있다. 약사법상 피해구제제도를 고려한다면, 금융거래를 통해 이익을 얻는 주체인 금융회사에게 분담금 지급의무를 두는 것이 금융소비자에게 분담금 지급의무를 지우는 것에 비하여 더 타당성을 가질 수 있을 것으로 보인다.

라. 피해구제사업의 개요

위에서 모델로 삼은 두 가지 피해구제사업의 개요를 살펴보면, 아래 표와 같다.

[표 4-6] 자동차손해배상 보장사업과 약사법상 부작용 피해구제 사업 비교

항 목	자동차손해배상 보장사업	약사법상 부작용 피해구제 사업
제도의 근거	자동차손해배상 보장법 제30조 등	약사법 제86조의3 등
운영 기관	자동차손해배상진흥원	한국의약품안전관리원
피해 보상 기준	책임보험의 보험금 한도	- 진료비 : 2천만 원 이하의 범위에서 본인 부담 금액 - 사망보상일시금 : 최저임금 월환산액의 5년분 - 장애일시보상금 : 1~4급(사망일시보상금의 25~100%) - 장례비 : 국가배상법 시행령 제4조에 따른 평균임금의 3개월치
기금 마련	제37조에 따른 분담금(책임보험료의 1%) 기금의 운용으로 생기는 수익금	기본부담금(전년도 의약품 생산액 및 수입액의 1000분의1) 추가부담금(전년도 해당 의약품으로 인한 피해구제 지급액의 100분의 25)

마. 피해구제사업 모델 제안

위에서 살펴본 제도들은 모두 분담금 또는 부담금으로 조성한 기금을 바탕으로 하고 있고, 일정한 한도 내에서 발생한 손해를 보상해주고 있다. 사실상 손해의 일부만을 보상해주는 기능을 한다. 앞서 살펴본 보이스피싱 보험의 의무보험화를 도입할

경우에도 여전히 보험미가입자가 상당수 발생할 것으로 보이기 때문에(기존 보험의 보장대상에 포함되지 않은 새로운 유형의 전기통신금융사기가 발생할 경우 점까지 감안하면 더더욱), 이 부분 논의는 실익이 있다. 자동차보험과 같이 금융서비스 이용자들로 하여금 의무보험으로 가입하도록 하는 것이 쉽지 않은 상황이고 보면, 보험미가입자로서 가해자로부터 손해배상을 받는 것이 사실상 어려운 상황에 처한 피해자에 대한 구제로서는 위와 같은 제도가 가장 적절할 것이다. 이미 어느 정도 성공적으로 정착된 위 두 가지 제도 모델을 참고하여 피해구제기금을 통한 피해구제사업 모델을 고안하여 보면, 아래와 같다.

[표 4-7] 보이스피싱 피해구제기금 사업 모델 제시

항 목	내 용
제도의 근거	통신사기피해환급법 제13조 이하에 신설하는 방안
운영 기관	채권소멸절차를 주관하는 금융감독원이 적절할 듯
피해 보상 기준	1인당 피해금액을 기초로 정한 한도(예컨대, 1,000만 원[208])의 범위 내에서 손해액의 50~70%[209]를 지급하되, 손해액 산정시 손해 회복이 된 채권소멸절차에 의하여 환급받은 금액과 사기범 또는 금융회사 등으로부터 손해배상(책임보험금 포함)을 받은 금액은 제외함이 타당함
기금 마련	1) 현행법상 금융기관이 이용자에 대한 손해배상책임 담보를 위해 가입하는 의무보험(아래 예시 ① 내지 ③)의 보험료 중 일부 ① 전자금융거래법 제9조 제4항 ② 여신전문금융업법 제16조 제4항 ③ 대부업 등의 등록 및 금융이용자 보호에 관한 법률 제11조의4 제2항 2) 보이스피싱 사기범들로부터 몰수 · 추징한 금원의 일부 3) 기부금
구제 신청 절차	현행 통신사기피해환급법은 지급정지 조치를 행한 금융회사가 금융감독원에 채권소멸절차의 개시를 위한 공고를 요청함으로써 시작됨(제5조). 이때, 금융회사가 피해자로부터 피해구제신청을 위임받아 금융감독원에 피해구제신청을 하거나, 채권소멸절차 진행 중 피해자가 별도 신청하는 것도 가능하도록 하면 됨. 채권소멸절차를 통해 피해자에게 환급되는 금액과 잔여 손해액이 특정되면, 피해금 환급 후 피해자에게 피해구제금 지급을 위한 심사를 개시(이때, 피해자로부터 배상을 받았는지 그 내역을 손해액 계산서 등 양식으로 제출하도록 하여야 함), 2~3개월의 심사기간을 거쳐 피해구제금 지급.
피해 구제금 환수	통신사기피해환급법 제11조 각호에 해당하는 사유 및 손해액 계산서 등을 허위로 제출한 경우
형사 처벌	제16조(벌칙) 각호에 거짓으로 피해구제금 신청을 한 자를 추가

제4절 | 소결

현행 통신사기피해환급법은 금융회사에 대하여 금융거래시 본인확인조치의무와 지급정지의무, 임시조치의무를 부과하고 있고, 이를 이행하지 않을 경우 법원은 손해배상책임을 인정하고 있고, 이는 비대면 전자금융거래 방식의 보이스피싱 피해 예방과 피해구제를 위한 실효적인 제도적 장치가 되고 있다. 이와 관련하여, 피해구제의 측면에서 보완되어야 할 부분을 살펴보면, 본인확인조치 등 피해방지의무를 여신전문금융회사와 대부업체까지 확대할 필요가 있다는 점, 금융회사 등의 피해 방지의무를 좀 더 구체적으로 정하고 이에 대한 손해배상책임을 명문화할 필요가 있다는 점, 대면편취형 보이스피싱의 경우에도 금융회사의 피해방지책임이 인정되는 예시 규정을 둘 필요가 있는지 검토가 필요한 점 등을 들 수 있다.

그러나 금융회사의 책임 강화를 통한 피해구제 방식은 비대면 방식의 보이스피싱 예방과 피해구제에는 어느 정도 실효성이 있으나, 금융회사의 개입 정도가 적은 대면편취형 보이스피싱 피해자의 구제에 적합하지 않은 측면이 있다. 또한, 일반인의 입장에서 대기업인 금융회사를 상대로 소송을 통해 피해구제를 받는 것은 쉽지 않고, 소송을 통한 피해구제는 최소 1년에서 수년이 걸린다는 문제가 있다.

보이스피싱 가해자측을 상대로 한 손해배상청구는 대부분 인출책이나 수거책 또는 사기이용계좌 예금주를 상대로 한 경우이다. 그런데, 위와 같은 손해배상청구 소송에서 승소판결을 받아도 가해자측이 무자력인 경우가 많아 강제집행이 어렵고, 소송비용 부담과 소송기간의 문제가 있다. 가해자측의 무자력으로 인한 문제는 근원적인 해결이 어렵지만, 현행 형사조정제도와 배상명령제도를 연계하는 방식의 제도 개선으로 가해자측의 임의변제를 유도하고, 소송비용 부담을 줄이고 신속한 재판이 이루어지도록 하는 것은 가능할 수 있다. 또한 조직적 범죄인 보이스피싱 사기범죄의 특성상 피해자가 다수일 가능성이 높고, 이런 경우 집단소송이나 단체소송을 도입하는 방안

208) 2022년 1인당 피해금액이 1,130만 원 정도이고, 최근 비슷한 수준임을 감안(금융감독원 2023. 4. 20.자 보도자료).

209) 손해액 전액을 지급하는 경우 피해자가 피해확대를 방지하기 위한 지급정지 신청 등 조치를 소홀히 할 우려가 있고, 또한 보이스피싱 예방을 위한 노력을 기울이지 않을 가능성이 높아질 우려가 있기 때문임.

도 검토되어야 한다.

범죄피해자 보호법상 구조대상에 재산범죄가 포함되어 있지 않은데, 보이스피싱 피해자를 구조대상에 포함시킬 것인지는 다른 재산범죄와의 형평성 문제, 구조금 재원 마련 문제 등과 연계하여 검토되어야 하고, 쉽게 결정할 수 없는 문제이다. 구조대상에 보이스피싱 피해자를 포함시키더라도, 그 대상이 생활능력이 없는 자 등으로 제한적이어야 하고 그 재원을 확대할 필요가 있다. 또한 구제절차가 중복되지 않도록 앞서 살펴본 피해구제기금에 의한 피해구제제도 도입 문제와 연계하여 논의가 되어야 한다.

보이스피싱 보험은 다른 피해구제 제도와 비교하면, 피해구제에 가장 신속하고 효율적인 방안이 될 수도 있다. 그러나 현재 판매되는 보이스피싱 관련 보험상품은 보장한도가 낮고, 가입률이 저조하다는 한계가 있다. 따라서 가입률을 높이기 위해 타 상품과의 결합판매나 부가서비스 방식의 판매를 늘릴 필요가 있다. 또한 보이스피싱 보험의 의무보험화나 금융상품 가입시 금융회사의 설명의무를 도입하는 것도 검토되어야 한다. 그리고 보험가입금액을 1인당 평균적인 피해금액에 비추어 최소한 1,000만 원 이상으로 확대하고, 대면편취형도 보장범위에 포함시켜 피해구제에 빈틈이 생기지 않도록 현실화하여야 한다.위와 같은 현행 피해구제 제도와 방법의 단점과 개선책을 요약해보면, 아래 표와 같다.

[표 4-8] 현행 피해구제 제도의 단점 및 개선책

피해구제 방식		단 점	개선책
손해배상 청구	금융회사 상대	- 비대면 금융거래에 대하여 제한적 실효성 - 대면편취형 보이스피싱 구제에 부적절 - 소송을 통한 구제의 한계	- 피해방지의무를 여신전문금융회사 및 대부업체까지 확대 적용 - 본인확인조치와 지급정지의무 외에 임시조치 등 피해방지 조치 사유를 구체화 - 대면편취형 보이스피싱의 경우도 피해방지 책임이 인정되는 사유를 명문화하는 방안 검토 필요
	가해자 상대 - 민사소송 - 형사조정 - 배상명령	- 범인이 검거되지 않는 경우가 많고, 무자력인 경우가 많아 제한적 실효성 - 민사소송은 소송비용 및 소송경제 측면에서 구제에 한계 - 형사조정은 집행력이 없어 미	- 형사조정제도와 배상명령제도를 연계하여, 형사조정 기간(수사기간→공판까지)의 확대, 형사조정 사항에 대한 법원의 배상명령, 형사소송 절차에서의 화해제도 활용, 조정사항 의무이행 유무의 양형 반영 등 필요 - 집단소송이나 단체소송 도입 검토 필요

피해구제 방식	단 점	개선책
	이행시 강제집행 불가 - 배상명령은 유죄판결 선고시에 이루어져 장시간 소요되고, 각하 비율이 높음	
범죄피해자 보호법상 범죄피해자 구조	- 보이스피싱 피해자는 구조대상에 포함시키느냐의 문제는 다른 재산범죄와 형평성, 구조금 재원 마련 등의 난해한 문제가 있음	- 보이스피싱 피해자를 구조대상에 생활능력이 없는 자 등으로 제한하고, 재원을 확대하는 방안 - 피해구제기금에 의한 피해구제와 연계하여 검토 필요
보이스피싱 보험	- 보상금액이 300~500만 원 수준으로 피해구제에 미흡 - 임의가입으로 가입률 저조 - 대면편취형 보이스피싱은 보장범위에서 제외된 경우도 있음	- 타 금융상품 혹은 보험상품과 결합판매 또는 부가서비스 판매 - 의무보험화 또는 설명의무화 - 보험가입금액과 보장범위를 확대하여 현실화할 필요

결국, 현행 피해구제 제도의 한계를 고려할 때, 피해구제를 위해 가장 적합한 모델로 고려해 볼 수 있는 것은 자동차손해배상보장법상 의무보험 형태의 책임보험과 연계된 자동차손해배상 보장사업과 약사법상 의약품 부작용 피해구제사업이다. 이러한 모델을 기초로 보이스피싱과 같은 전기통신금융사기 피해자의 피해구제를 위한 피해기금을 마련하여 피해구제를 함으로써, 통신사기피해환급법상 피해환급절차와 금융회사 내지 가해자를 상대로 한 손해배상 청구 등을 통해서도 회복되지 않는 피해자의 손해를 신속하게 보상해주는 제도가 절실히 필요하다.

결 론

윤 해 성

제5장

결 론

이상의 내용을 정리 및 요약하고 시사점을 제시하면서 결론에 갈음하고자 한다. 경찰 통계를 통해서 최근 발생건수를 보면 2018년 34,132건에서 2019년 37,667건으로 증가하였으나 이후 감소하는 경향을 보이고 있다(2022년 21,832건). 피해액은 2018년 4,041억원에서 2021년에 7,744억까지 증가하였으며 2022년에는 감소하여서 5,438억원에 이르고 있다. 다만 2022년의 피해액은 2018년에 비해 많다는 것을 알 수 있다. 보이스피싱 유형별 발생현황을 보면 기관사칭형은 대체로 증가하는 반면 대출사기형은 감소하는 경향을 나타내고 있다. 편취수법별로 보면, 2018년의 경우 계좌이체 비율이 89.7%로 상당히 높았으나 큰 폭으로 감소하여서 2022년에는 9.9%였다. 반면 대면편취의 경우 같은 기간 7.5%에서 64.4%로 증가하였다.

보이스피싱은 전화로 피해자를 기망하여 금전을 편취하는 보이스피싱이 최초로 발생한 이후, 파밍, 스미싱, 메신저 피싱 등 범죄수법이 진화한 것은 기본이고, 피해자를 기망하는 수법이 계속해서 변화하고 있다. 같은 수법이라도 피해자를 기망할 때 '세금·보험금 환급 빙자' 수법에서부터 '납치·협박 빙자'에서 '택배 반송 빙자' 등으로 수법이 조금씩 변화하고, 이외에도 피싱사이트를 이용한 범죄에서도 금융감독원 사이트, 검찰청 사이트, 인터넷에서 바로 팝업창을 이용하여 접속하게 하는 등 수법이 조금씩 변화하고 있다. 특히 최근 보이스피싱 유형은 크게 대출사기형과 기관사칭형으로 분류될 수 있다. 대출사기형의 경우 범행대상이 미끼문자 등을 통한 불특정 다수인 유형과 개인정보 탈취 후 송금을 유도하는 특정 유형이다. 특히 문제되는 유형은 피해자에게 대출 신청서 앱을 송부하고 카카오톡 친구를 맺은 다음 악성 앱을 다운로드 하도록 유도, 악성 앱이 설치되면 전화기의 모든 권한이 범죄자에게 넘어가 강제로 수신 및 발신할 수 있게 되어 스마트폰상의 모든 개인정보가 범죄자에게 넘어

가게 되는 등 기술에 발전에 따라 보이스피싱 범죄수법도 계속적으로 진화하고 있다.

한편, 범행 수단이 다양화됨에 따라 주요 범행 수단이 4개 범행 수단에서 8개로 늘어나게 되었는데, 1. 대포통장, 2. 대포폰, 3. 전화번호 변작 중계기, 4. 자금세탁 행위, 5. 악성 앱 제작·유포 행위, 6. 불법 데이터베이스 유출·유통 행위, 7. 각종 미끼문자·자동 응답 시스템 전화 발송 행위, 8. 사회관계망서비스(SNS) 대포 계정 생성이다. 따라서 이를 차단할 수 있는 방안들이 다각적으로 모색되어야 한다. 대포폰 규제의 경우 유심칩을 통제하여야 하는데 이때, 보이스피싱 범행 시작 단계인 미끼문자 발송업체를 단속하여 미끼문자를 차단할 필요가 있다. 아울러 대포유심과 대포증권계좌를 단속하여야 하기 위해서는 경찰 등 관련 유관부처와 통신업체와의 협업을 통해 지속적인 단속을 해야 한다.

보이스피싱 대응과 관련해서 미끼문자의 경우, "정부지원금을 준다." "2% 낮은 금리로 준다"는 문자가 발송하는데 이러한 경우 보이스피싱으로 의심하고 전화를 하면 안 된다라는 홍보가 우선되어야 한다. 설령 전화를 하였다고 해도 절대 카카오톡 친구를 맺어선 안 되고 대출 신청서를 다운로드 받으면 안된다라는 홍보가 대대적으로 이루어질 필요가 있다. 정부에서는 새로운 신종범죄 수법을 인지할 경우 국무조정실을 중심으로 각 부처에 알려야 하며 특히 금융기관과 통신업체를 통해 미끼문자에 대한 대대적인 홍보를 할 필요가 있다. 대표적으로 "택배 수령이 안 된다." "계좌가 개설되었다." "해외직구에 얼마 결제되었다"등의 이상한 문자가 온다면 무시하는 것이 가장 좋은 방법이나 이를 걸러낼 수 있는 시스템을 마련하는 것도 고려해야 한다. 혹시나 URL 사이트가 있다면 절대 접속해서는 안 된다. 아울러 발신번호 변작 중계소를 대대적으로 단속하고, 의심있는 문자나 번호의 경우 차단할 수 있도록 해야 한다.

최근 대금을 입금받을 계좌번호를 가게 문이나 주차장 앞에 게시하는 경우가 빈번한데 이러한 상황을 악용하여 게시된 계좌번호를 대포통장으로 사용한 뒤 지급정지를 풀어주는 조건으로 돈을 요구하는 수법도 나타나고 있다. 그러므로 가급적 계좌번호를 게시하거나 공개하지 않도록 지속적인 홍보가 요청된다. 이를 위해 경찰이나 지자체의 공무원의 경우 순찰이나 단속시 계좌번호를 알려주지 않도록 하는 등 교육을 통하여 경각심을 심어줄 필요가 있다.

보이스피싱과 관련하여 정부는 새로운 수법이 나타날 때마다 일선에 빨리 알리고

신속하게 대응할 수 있는 프로세스를 제시하였다. 한때 국민에게 문자를 통하여 보이스피싱을 예방할 수 있게 하였지만 이는 비용이 드는 문제도 있을 뿐만 아니라 큰 효과를 담보하지도 못하였기 때문에 현재는 답보상태이다. 금융감독원 등은 내부적 평가를 통하여 가령 소비자 보호실태 평가 등을 통하여 보이스피싱에 정부의 대책이 어느 정도 효과가 있는지 자체평가를 하지만 그럼에도 불구하고 보이스피싱 범죄는 수법을 바꾸거나 새로운 수법이 나타나면서 금융당국을 당혹하게 만들고 있다.

특히 현재 인터넷이 등장하고 가상자산이 활용되면서 보이스피싱과 같은 범죄는 대응하기 어렵다는 분석도 나오고 있다. 이유는 가상자산은 자금을 추적하기 힘들뿐더러 자금을 세탁하기 위한 것인데 기술적으로 가상자산이 보이스피싱 범죄에 연루되었다고 하면 사실상 현재의 지급정지의무는 무용지물이라는 것이다. 다시 말해서 보이스피싱 범죄자들이 가상자산으로 돈을 입금하라고 하면 이를 담당하는 거래소에 지급정지를 해봤자 지급정지가 될 수 없다는 것이다. 또한 형평성과의 문제도 주장되고 있는데, 현재 주식의 경우 지급정지 대상이 아닌데, 가상자산을 지급정지 대상에 포함시키는 것도 사실상 형평성에 어긋난다는 지적이다.

보이스피싱의 경우 가상자산으로 입금하지 말아야 하는 대대적인 홍보가 필요하며 거래소에서는 자체 지침을 통하여 내부적으로 보이스피싱 범죄 관련 이상징후 포착 등의 교육을 통하여 금융회사처럼 자체적으로 대응할 필요가 있다. 그리고 금융위원회가 가상자산을 담당하고 있으므로 수시로 거래소 점검 및 단속을 통하여 보이스피싱 피해에 만전을 기하여 할 것이다. 은행직원이든 거래소 직원이든 보이스피싱의 예방과 대응과 관련하여 보이스피싱 피해를 방지하거나 범죄자를 검거할 경우 별도의 인센티브나 인사고과에 반영하는 방안도 고려해야 한다.

한편, 부처간 업무도 상이하고 관할도 다르다. 금융감독원의 경우는 사칭형(메신져, 비메신져)과 대출빙자형을 담당하고 있으며, 전화번호이용중지의 경우는 방송통신위원회가 담당하고 있고 가상자산의 경우는 금융위원회에 담당하고 있다. 또한 전화번호나 변작 신고는 인터넷 진흥원(KISA)가 담당하고 있듯이 각 부처의 역할도 서로 다른 것을 확인할 수 있었다. 사정이 이렇다 보니 통합신고센터를 만들어서 대응해야 한다는 목소리도 커지고 있는 상황이다. 그러나 통합신고센터를 만든다고 해서 보이스피싱 범죄나 피해구제에 과연 효과가 있는 것인지는 다시 한번 고려해야 한다.

어차피 업무가 다른 이상 신고만 통합되었다고 한들 이곳에서는 일반적 상담만 할 뿐이며 정보의 접근 자체도 어렵고 대응하는 기관도 다르기 때문에 금융당국 내지 방통위로 다시 들어올 수밖에 없는 구조라는 것이다. 통합신고센터가 통합신고ㆍ대응센터로 명실상부한 보이스피싱 대응 및 피해구제 기관으로 거듭나려면 상담은 물론 신속한 대응과 피해구제도 함께 가능해야 한다는 점을 염두해야 한다.

나아가 어느 정도의 적절한 대응을 할 수 있지만 전문적인 대응을 할 수 있는 허브기관이 되어야 한다. 가령, 국제조직과 연계된 보이스피싱 범죄 신고시 통합신고센터에 신고가 접수된 다음 통합신고대응센터의 경찰 내지 합동수사단의 검경이 이를 인수인계 받고 초동조치를 취한 후에 본청 내지 대검찰청에 연락하여 중국 공안 내지 인터폴의 협조 아래 검경이 합동으로 수사를 하는 것이다. 또한 국가정보원의 해외 네트워크망을 활용하여 정보를 받고 국제공조수사를 할 수 있도록 해야 한다.

정부의 대책 가운데 한 가지 아쉬운 점은 현재 보이스피싱 정부 합동 수사단을 설치 운영하겠다는 것인데 이 역시 오래전에 전문가들이 주장한 대안이었다. 이제야 대검찰청, 경찰청, 관세청, 국세청, 금융감독원, 방송통신위원회 등 정부 기관들로 구성된 합동수사단을 마련한다는데 늦은감이 있다. 중요한 것은 보이스피싱 정부 합동 수사단과 112 통합신고ㆍ대응센터는 별도의 기관이 되어서는 안 된다는 점이다. 보이스피싱 합동 수사단 아래 112 통합신고 대응센터가 위치하여 함께 협업할 수 있는 환경이 구축되어야 한다.

2023년 7월 초부터는 개인정보가 노출자 시스템을 도입하여 간편송금제도를 보완 및 수정한 일괄지급제도를 시행할 예정이다. 정부의 대책대로 지급정지는 보이스피싱을 근절하기 보다는 피해자 구제 차원에서 획기적인 대책으로 평가되고 있었다. 그러나 최근 이러한 전체 지급정지가 오히려 선의의 피해자에게는 피해를 주는 제도가 되고 있는 만큼 정부는 전체지급정지제도에서 부분지급정지제도로 변환하거나 특정 은행에 한하여 지급정지를 추진하려고 한다. 아울러 보이스피싱 범행에 가담하지 않게 하기 위해서는 현금수거책이나 그 외 방조범에게도 전반적으로 형량의 구형을 높일 필요가 있으며, 법원은 보이스피싱 방조범에게 범죄단체의 미필적 고의를 확대해석하여 실형을 선고할 필요가 있다.

피해구제와 관련하여 현행 통신사기피해환급법은 금융회사에 대하여 금융거래시

본인확인조치의무와 지급정지의무, 임시조치의무를 부과하고 있고, 이를 이행하지 않을 경우 법원은 손해배상책임을 인정하고 있고, 이는 비대면 전자금융거래 방식의 보이스피싱 피해 예방과 피해구제를 위한 실효적인 제도적 장치가 되고 있다. 이와 관련하여, 본인확인조치 등 피해방지의무를 여신전문금융회사와 대부업체까지 확대할 필요가 있다는 점, 금융회사 등의 피해 방지의무를 좀 더 구체적으로 정하고 이에 대한 손해배상책임을 명문화할 필요가 있다는 점, 대면편취형 보이스피싱의 경우에도 금융회사의 피해방지책임이 인정되는 예시 규정을 둘 필요가 있는지 검토가 필요한 점 등을 들 수 있다.

그러나 금융회사의 책임 강화를 통한 피해구제 방식은 비대면 방식의 보이스피싱 예방과 피해구제에는 어느 정도 실효성이 있으나, 금융회사의 개입 정도가 적은 대면편취형 보이스피싱 피해자의 구제에 적합하지 않은 측면이 있다. 또한 보이스피싱 가해자측을 상대로 한 손해배상청구는 대부분 인출책이나 수거책 또는 사기이용계좌 예금주를 상대로 한 경우이다. 그런데, 위와 같은 손해배상청구 소송에서 승소판결을 받아도 가해자측이 무자력인 경우가 많아 강제집행이 어렵고, 소송비용 부담과 소송기간의 문제가 있다. 다만, 현행 형사조정제도와 배상명령제도를 연계하는 방식의 제도 개선으로 가해자측의 임의변제를 유도하고, 소송비용 부담을 줄이고 신속한 재판이 이루어지도록 하는 것은 가능할 수 있다. 아울러 조직적 범죄인 보이스피싱 사기범죄의 특성상 피해자가 다수일 가능성이 높고, 이런 경우 집단소송이나 단체소송을 도입하는 방안도 검토되어야 한다. 나아가, 범죄피해자 보호법상 구조대상에 재산범죄가 포함되어 있지 않은데, 보이스피싱 피해자를 구조대상에 포함시킬 것인지는 다른 재산범죄와의 형평성 문제, 구조금 재원 마련 문제 등과 연계하여 검토되어야 하며, 구조대상에 보이스피싱 피해자를 포함시키더라도, 그 대상이 생활능력이 없는 자 등으로 제한적이어야 하고 그 재원을 확대할 필요가 있다.

보이스피싱 보험은 다른 피해구제 제도와 비교하면, 피해구제에 가장 신속하고 효율적인 방안이 될 수도 있다. 보험가입금액을 1인당 평균적인 피해금액에 비추어 최소한 1,000만 원 이상으로 확대하고, 대면편취형도 보장범위에 포함시켜 피해구제에 빈틈이 생기지 않도록 현실화하여야 한다.현행 피해구제 제도의 한계를 고려할 때, 피해구제를 위해 가장 적합한 모델로 고려해 볼 수 있는 것은 자동차손해배상보장

법상 의무보험 형태의 책임보험과 연계된 자동차손해배상 보장사업과 약사법상 의약품 부작용 피해구제사업이다. 이러한 모델을 기초로 보이스피싱과 같은 전기통신금융사기 피해자의 피해구제를 위한 피해기금을 마련하여 피해구제를 함으로써, 통신사기피해환급법상 피해환급절차와 금융회사 내지 가해자를 상대로 한 손해배상 청구 등을 통해서도 회복되지 않는 피해자의 손해를 신속하게 보상해주는 제도가 절실히 필요하다.

참고문헌

1. 국내문헌

강성복·윤종민, 전기통신금융사기 법제에 관한 분석적 고찰, 과학기술과 법 제3권 제2호, 충북대학교 법학연구소, 2012.

고제성, 통신사기피해환급법 제15조의2 제1항에서 말하는 '정보 또는 명령의 입력행위'의 의미, 사법 제36호, 사법발전재단, 2016.

곽대경, "보이스피싱의 실태와 대책에 관한 연구", 형사사법연구 제1권 제1호, 2011.

구길모, 보이스피싱 예방과 단속을 위한 한중공조방안, 비교형사법연구 제16권 제2호, 한국비교형사법학회, 2014.

권성원, 전화금융사기 범죄에 대한 한국 사회의 대응: 대만과의 비교 분석, 형사정책 제22권 제1호, 2010.

김경진·서준배, 보이스피싱 현황과 정책제언, 시큐리티연구 제66호, 2021.

김경찬·정군남·김창준·현송학, "중국 동북지역 한국관련 마약범죄와 보이스피싱범죄의 실태 및 대응방안에 관한 연구", 한국형사정책연구원 연구총서 13-AA-13, 2014.

김기창, "전자금융거래법상 '이용자의 중대한 과실' -대법원 2013다86489 판결의 문제점-", 정보법학 제18권 제3호, 2014..

김대근·임석순·강상욱·김기범, "신종금융사기범죄의 실태 분석과 형사정책적 대응방안 연구-기술적 수단을 사용한 사이버 금융사기를 중심으로-, 한국형사정책연구원 연구총서 16-CB-03, 2016.

김동민, "접근매체를 이용하는 전자금융사기의 범위에 관한 소고", 법학연구 제31권 제2호, 2020.

김민정·김은미, "보이스피싱 피해 경험 및 영향요인 분석", 소비자문제연구 제52권 제1호, 2021.

김민정·김은미, 보이스피싱 피해경험 및 영향요인 분석, 소비자문제연구 제52권 제1호, 2021.

김선복, 詐欺罪에 있어서 處分意思의 必要性, 형사법연구 제13호, 한국형사법학회, 2000.

김성규, 전기통신금융사기의 현상과 그 가벌성, 법학논총 제32집 제2호, 전남대학교 법학연구소, 2012.

김성언, 전화금융사기 범죄에 대한 한국사회의 대응: 대만과의 비교분석, 형사정책학회 발표문, 2010.

김성언·양영진, 전화 금융사기 범죄의 진화: '보이스피싱(Voice Phising)'의 피해구조 분석과 대응, 한국공안행정학회보 제32호, 한국공안행정학회, 2008.

김시윤·이용걸·이범주, "전기통신금융사기 대응 방안에 관한 연구 : 보이스피싱 담당 경찰관의 관점으로", 치안정책연구 통권 57호, 2022.

김은정, "대면편취형 보이스피싱 범죄의 범행과정 분석 : 범죄스크립트 분석을 중심으로", 범죄수사학연구 통권 제15호, 2022.

김재봉, 사기죄와 처분의사, 한국형사판례연구회, 형사판례연구 11, 박영사, 2003.

김혜경, "범죄피해자 구조금 지급의 법적 개선방안-헌법상 범죄피해자구조청구권의 본질과의 상관성을 중심으로-", 형사정책연구 제26권 제1호(통권 제101호, 2015 봄)

김효신·서준배, "로맨스 스캠(Romance Scam) 범죄 현황 및 대응방안에 대한 고찰", 경찰한논총 제14권 제3호, 2019.

박명호·최정욱·정훈, 주요국의 해외금융계좌 신고제도에 대한 비교 연구, 한국조세재정연구원, 2013.

박성은, "배상명령제도 활성화를 위한 절차 개정안-독일의 부대소송제도에 대한 검토를 중심으로-", 법학논고 제81집(2023. 4.)

서준배, "보이스피싱 현황, 유형, 추이와 대응관련 시사점", 통계청 통계개발원 한국의 사회동향, 2022.

송귀채, "범죄피해자 구조금 산출 방법의 문제점 및 개선방안", 한국피해자학회「피해자학연구」제30권 제3호(2022. 12.)

여혜린, "피싱과 스미싱을 주로 한 사이버 사기의 현황 및 입법 제언", KHU글로벌 기업법무 리뷰, 제15권 제1호, 2022.

오영근, 대포통장에서의 현금인출과 전기통신금융사기죄의 성립여부—대법원 2016. 2. 19. 선고, 2015도15101 전원합의체 판결—, 법조 제66권 제2호, 법조협회,

2017.
원혜욱, “범죄피해자 보호 · 지원제도의 개선방안”, 피해자학연구 제25권 제3호(2017. 12.)
윤해성, 보이스피싱 대응방안 고찰, 법학논고 제34집, 경북대학교 법학연구원, 2010.
윤해성, 보이스피싱 사기범죄의 국제적 동향과 법제도적 방향 모색, 형사정책 제25권 제2호, 한국형사정책학회, 2013.
윤해성, "보이스피싱 범죄에 대한 쟁점과 대책", 성신법학 제9호, 2010.
윤해성·곽대경, “보이스피싱의 예방과 대책마련을 위한 연구”, 한국형사정책연구원, 2009.
윤해성·김유근, “보이스피싱 피해유형별 구체적 예방방안에 관한 연구”, 대검찰청 연구용역보고서, 2017.
윤해성·곽대경, 보이스피싱의 예방과 대책마련을 위한 연구, 한국형사정책연구원, 2009.
윤해성·안성훈, 보이스피싱 근절과 피해자 구제를 위한 제도 개선 방안, 한국형사정책연구원, 2012.
이기수, “최근 보이스피싱의 범죄수법 동향과 법적 대응방안”, 범죄수사학연구 제4권 제2호, 2018.
이동임, “보이스피싱범죄 대응 및 피해회복 방안”, 피해자학연구 제18권 제2호(2010. 10.)
이동임, “보이스피싱범죄 대응 및 피해회복 방안”, 피해자학연구 제18권 제2호(2010. 10.)
이봉한, 전화금융사기의 유형과 피해자 분석-한국과 일본의 비교, 한국범죄심리연구 제4권 제2호, 2008.
이세빈·이지오·염흥열, “금융정보를 탈취하는 파밍 악성코드 분석 및 대응방안”, 정보보호학회지 제27권 제3호, 2017.
이유주, “전화금융사기(보이스피싱) 대응책의 현황 및 개선방안”, 국회입법조사처 현안보고서 제34호, 2009.
이은진, “전기통신금융사기 피해자 구제에 관한 연구-피해금 환급 방안을 중심으로-”, 고려대학교 법무대학원 석사학위논문(2018. 6.)
이정훈·김두원, 가상화폐 관련 형사법적 문제에 관한 고찰, 형사정책연구, 2017.

이창섭, 통신사기피해환급법 제15조의2 제1항 위반죄에 관한 고찰, 법학연구 제57권 제4호, 부산대학교 법학연구소, 2016.

장주성, "금융소비자 보호를 위한 보이스피싱 대응방안 연구", 금융감독연구 제9권 제1호, 2022.

장주성, “금융소비자 보호를 위한 보이스피싱 대응방안 연구-통신사, 제조사, 금융사, 플랫폼사업자와의 협업을 통한 단계별 대응방안 제안-”, 금융감독연구 제9권 제1호(2022. 4.)

정대용, “범죄 스크립트 분석을 활용한 몸캠피싱 범죄수법 분석”, 경찰학연구 제21권 제3호, 2021.

정순채, 전화금융사기 등 정보통신망 이용 금융사기 대응방안 고찰, 경희대학교 국제법무대학원, 2012.

정영호·하형준, "메신저피싱 범죄의 실태와 대응방안에 관한 연구", 범죄수사학연구 제8권 제1호, 2022.

정정원, “보이스피싱(Voice Phishing)범죄의 형사법적 검토 및 대응방안”, 가천법학 통권 15호, 2013.

정정원, 보이스피싱(Voice Phishing)범죄의 형사법적 검토 및 대응방안, 가천법학 제6권 제2호, 가천대학교 법학연구소, 2013.

정태진, “팬데믹시대 증가하는 로맨스스캠과 몸캠피싱 : 국내외 동향 및 대응방안”, 한국경찰연구 제20권 제4호, 2021.

차영민·송영시, “보이스피싱 범죄의 실태와 피해자의 손해보전 방법에 관한 소고", 법학논총 제21권 제2호, 2014.

최관·김민지, "한국 보이스피싱 범죄의 진행과정에 관한 연구", 경찰학연구 제15권 제3호, 2015.

최형욱·이상진, "피싱 범죄의 현황과 대응 방안 모색", 치안정책연구 통권 60호, 2022.

하담미, "전자금융거래법상 접근매체 대여에 있어 '대가'의 의미 고찰 -최근 판례들을 중심으로-", 일감법학 제46권, 2020.

허성욱·정세종, 국제전화금융사기에 관한 법적 고찰, 한국경찰연구 제7권 제2호, 2008.

현새롬, “보이스피싱 범죄수법의 진화와 제도적 대응방안에 관한 연구”, 고려대학교 정보보호대학원 정보보호학과 석사학위논문(2021. 8.)

현새롬, “보이스피싱 범죄수법의 진화와 제도적 대응방안에 관한 연구”, 고려대학교 정보보호대학원 정보보호학과 석사학위논문(2021. 8.)

홍동규·홍순민·김한결, 보이스피싱 전달책의 가담경로에 관한 연구, 경찰학 연구 제20권 제1호, 2020.

황석진, "전기통신금융사기 근절을 위한 고찰 -보이스 피싱을 중심으로-", 경찰학연구 제21권 제1호, 2021.

황정익, 전화금융사기사건에 있어서 명의도용 예금통장에 관한 법적 고찰, 한국공안행정학회보 제33호, 2008.

2. 국외문헌

Carlisle, David, Occasional Paper “Virtual Currencies and Financial Crime: Challenges and Opportunities”, Royal United Services Institute for Defence and Security Studies, 2017(https://rusi.org/sites/default/files/rusi_op_virtual_currencies_and_financial_crime.pdf.

Hefendehl, R., § 263, Joecks, W./Miebach, K. (Hg.), MK-StGB, Bd. 5, 2. Aufl., 2014.

Hessel, S., Soziale Netzwerke im Fokus von Phishing-Angriffen — Eine Analyse aus technischer und rechtlicher Sicht, JurPC Web-Dok 137/2016, Abs. 1-102.

宋樹寰, “電信詐欺犯罪類型、特徵與防制策略之研究”, 國立台北大學犯罪學研究所, 2008. 7.

丁水復, “新興詐欺犯罪問題防治法制之研究”, 國立中山大學大陸研究所, 碩士論文, 2005.

神元隆賢, ‘振り込め詐欺を巡る刑法解釈上の諸問題’, 法政論叢 第46巻 第2号, 2010.

産経新聞, “振り込め詐欺〝キング〟に懲役20年 東京地裁”, 2010年 3月24日 記事.

田中優輝, 「犯罪行為により自己名義口座に振り込まれた預金の払戻しと詐欺罪・窃盗罪の成否——東京高判平成25年9月4日、判例時報2218号 134頁」, 広島法学 40巻3号(2017).

松宮孝明, 「譲渡・売却目的を秘した銀行口座開設に詐欺罪の成立が認められた事例(最三決平成19・7・17 刑集61巻５号521頁)」, 『立命館法学』, 323号, 2009.

尾田清貴,「振込め詐欺の防止に向けた官民共同対策について」,『日本法学』, 第八十一巻 第四号(2016.2).

3. 그 밖의 참고자료

IT dongA, "[IT강의실] 인터넷으로 싸게 전화하자 – VoIP", 2015.10.02. https://it.donga.com/22530/ (최종검색일 : 2023.09.03.)

KBS뉴스, ""널 사랑해, 병원비 좀"···달콤한 사기 '로맨스 스캠' 기승", 2022.12.18. https://news.kbs.co.kr/news/view.do?ncd=5628560 (최종검색일 : 2023.08. 12.)

MBN뉴스, "'달리는 오토바이'가 보이스피싱 중계기···수법 기상천외", 2022.10.18. https://www.mbn.co.kr/news/society/4865043 (최종검색일 : 2023. 08. 05.)

SBSNEWS, "[단독] "보이스피싱 중계기 직접 들고 지하철로 수도권 일주"...신종 수법 '덜미'", 2023.01.05. https://news.sbs.co.kr/news/endPage.do?news_id=N1007034063&plink=ORI&cooper=NAVER (최종검색일 : 2023.08.05.)

SBSNEWS, "[친절한 경제] 이젠 유튜브도 신경써서 봐야해?...'고정댓글 피싱' 주의", 2023.02.09. https://news.sbs.co.kr/news/endPage.do?news_id=N1007073359 (최종검색일 : 2023. 08. 29.)

YTN, "조직적 중고 거래 사기 '사이트 피싱'...피해규모와 대책은?", 2022.11.14. https://www.ytn.co.kr/_ln/0115_202211141310206433 (최종검색일 : 2023. 08. 26.)

경찰청 2022년 7월 17일 보도자료, "2022년 상반기 전화금융사기 발생·검거 현황 분석"(https://police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20220718094502653, 검색일: 2023년 6월 10일).

경찰청 사이버안전국 홈페이지, https://www.cyber.go.kr/prevention/prevention10.jsp?mid=020310 (최종검색일 : 2023. 08. 20.)

국가법령정보센터, 전자금융거래법 전체 제정·개정이유, https://www.law.go.kr/LSW/lsRvsRsnListP.do?lsId=010199&chrClsCd=010202&lsRvsGubun=all (최종검색일 : 2023. 8. 16.)

국무조정실 2022년 9월 29일 보도자료, "보이스피싱 범죄근절을 위한 통신·금융분야

대책 발표"(https://www.fsc.go.kr/no010101/78643, 검색일: 2023년 6월 10일).

국무조정실 국무총리비서실 보도자료, "보이스피싱 대응 범정부 TF 회의, 2023.02.01. https://www.opm.go.kr/opm/news/press-release.do?mode=view&articleNo=152623&srSearchVal=%EB%B3%B4%EC%9D%B4%EC%8A%A4%ED%94%BC%EC%8B%B1&article.offset=0&articleLimit=10 (최종검색일 : 2023. 08. 20.)

금융감독원 2021년 4월 16일 보도자료, "'20년 중 보이스피싱 현황 분석" (https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=16265&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EB%B3%B4%EC%9D%B4%EC%8A%A4%ED%94%BC%EC%8B%B1&pageIndex=3, 검색일: 2023년 6월 10일).

금융감독원 2021년 9월 6일 보도자료, "'21년 상반기 보이스피싱 피해 현황" (https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=16510&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EB%B3%B4%EC%9D%B4%EC%8A%A4%ED%94%BC%EC%8B%B1+%ED%94%BC%ED%95%B4+%ED%98%84%ED%99%A9&pageIndex=1, 검색일: 2023년 6월 10일).

금융감독원 2022. 11. 1.자 보도자료

금융감독원 2022년 4월 20일 보도자료, "21년 보이스피싱 피해현황 분석" (https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=55444&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EB%B3%B4%EC%9D%B4%EC%8A%A4%ED%94%BC%EC%8B%B1&pageIndex=2, 검색일: 2023년 7월 17일).

금융감독원 2023. 4. 20.자 보도자료

금융감독원 2023년 4월 21일 보도자료, "2022년 보이스피싱 피해현황 및 주요 특징" (https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=127319&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=&pageIndex=14, 검색일: 2023년 6월 10일).

금융감독원 보도자료 사이트https://www.fss.or.kr/fss/bbs/B0000188/list.do?menuNo=200218 (최종검색일 : 2023. 08. 30.)

금융감독원 보도자료, "9.1.[목]부터 대면편취형 보이스피싱 피해예방 활동이 강화됩니다.", 2022.08.25. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=56670&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=2 (최종검색일 : 2023. 07. 08.)

금융감독원 보도자료, "가족 또는 지인 사칭해 개인정보와 돈을 요구하는 메신저 피싱 근절 위해 관계기관 힘 모아", 2020.06.24. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=15800&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=5 (최종검색일 : 2023. 07. 08.)

금융감독원 보도자료, "금융감독원 피싱사이트 유도 문자메시지 주의!", 2012.03.23. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=9092&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=18 (최종검색일 : 2023. 6. 27.)

금융감독원 보도자료, "대출빙자형 보이스피싱 사기범 목소리 최신사례 공개", 2016.09.12. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=12775&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=13 (최종검색일 : 2023. 07. 01.)

금융감독원 보도자료, "대출빙자형 보이스피싱에 주의하세요", 2016.08.31. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=12745&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=14 (최종검색일 : 2023. 07. 01.)

금융감독원 보도자료, "대포통장이 아닌 정상계좌를 이용한 피싱사기 주의", 2013.07.16. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=10155&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=17 (최종검색일 : 2023. 6. 27.)

금융감독원 보도자료, "인터넷 피싱사이트를 이용한 신종 전화금융사기 주의!", 2011.01.19.

금융감독원 보도자료, "제2차 금융분야 보이스피싱 대책 발표", 2023.02.28. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=58200&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC

%EC%8B%B1&pageIndex=1 (최종검색일 : 2023. 07. 09.)

금융감독원 보도자료, "지인을 사칭한 메신저피싱 주의 당부", 2018.12.18. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=14721&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=7 (최종검색일 : 2023. 07. 06.)

금융감독원 보도자료, "코로나19 정부지원대출 빙자 보이스피싱, 스미싱 주의", 2020.04. 29. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=15709&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%94%BC%EC%8B%B1&pageIndex=5 (최종검색일 : 2023. 07. 08.)

금융감독원 보도자료, "'12.6.26일(화)부터 「지연인출제도」 시행", 2012.06.11. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=9245&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EC%A7%80%EC%97%B0%EC%9D%B8%EC%B6%9C%EC%A0%9C%EB%8F%84&pageIndex=1 (최종검색일 : 2023. 08. 05.)

금융감독원 보도자료, "외환 무역사기거래에 대한 유의사항 안내", 2021.12.02. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=16658&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%EB%AC%B4%EC%97%AD%EC%82%AC%EA%B8%B0&pageIndex=1 (최종검색일 : 2023. 08. 19.)

금융감독원 보도자료, "해외 주요국의 금융사기 피해실태-대응조치 및 시사점", 2015.06. 11. https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=11681&menuNo=200218&cl1Cd=&sdate=&edate=&searchCnd=1&searchWrd=%ED%95%B4%EC%99%B8+%EC%A3%BC%EC%9A%94%EA%B5%AD%EC%9D%98+%EA%B8%88%EC%9C%B5%EC%82%AC%EA%B8%B0&pageIndex=1 (최종검색일 : 2023. 05. 05.)

금융위원회 '제2차 금융분야 보이스피싱 대응방안(2023. 2. 28)'

금융위원회 2023. 2. 21.자 보도참고자료

뉴스웍스, "[성년의 날⑭] 피해자 10명 중 4명 '20대'...청년 노리는 '몸캠피싱' 피하려면", 2023.05.14. https://www.newsworks.co.kr/news/articleView.html?idxno=711610 (최종검색일 : 2023. 08. 20.)

뉴스타운, "무선인터넷 이용 은행 피싱사이트 조직 첫 검거", 2005.11.17.

https://www.newstown.co.kr/news/articleView.html?idxno=25093 (최종검색일 : 23. 8. 15.)

매일경제, ""편해서 좋았는데"···보이스피싱 타깃된 간편송금, 피해대책 나왔다", 2023.07.25. https://www.mk.co.kr/news/economy/10793349 (최종검색일 : 2023.07.29.)

머니투데이, "[단독] "목소리 소름주의"...400억 가로챈 '딥보이스 범죄' 檢도 나섰다.", 2023. 02. 11. https://news.mt.co.kr/mtview.php?no=2023020913433930492 (최종검색일 : 2023. 08. 20.)

머니투데이, "폭증하는 간편송금 시장...토스·카카오가 97%장악", 2018.08.14. https://news.mt.co.kr/mtview.php?no=2018081410305678343 (최종접속일 : 2023.08.15.)

방송통신위원회·금융위원회·경찰청·금융감독원 공동보도자료, "가족, 지인 사칭「메신저피싱」주의 당부 – 이동통신3사 전 가입자 대상 피해예방 문자메시지 발송 –", 2022.05.12. (최종검색일 : 2023. 08. 05.)

서울경제 2023년 5월 3일자, "해외직구 결제 639,000원'…보이스피싱 그놈 미끼였다" (https://www.sedaily.com/NewsView/29PFOGNET4, 검색일: 2023년 5월 10일).

서울경제, "하다하다 이젠 '가짜 우편물까지···치떨리는 보이스피싱", 2023.08.30. https://www.sedaily.com/NewsView/29TLWS81AJ (최종검색일 : 2023. 08. 30.)

서울남부지방법원 주희양 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰

서울동부지방법원 이은미 변호사, 2023.08.14., 보이스피싱 범죄 유형 관련 인터뷰

서울신문, "비대면의 역설... 명의 도용 대포폰·신용카드로 나도 모르게 '빚더미'", 2023.05.23. https://www.seoul.co.kr/news/newsView.php?id=20230523002004&wlog_tag3=naver (최종검색일 : 2023. 08. 26.)

서울중앙지방법원 김효선 변호사, 2023.08.14., 보이스피싱 범죄 유형 관련 인터뷰

아시아경제, "금감원 이메일 해킹 '무역사기' 주의보 발령", 2021.12.01. https://view.asiae.co.kr/article/2021120109555910380 (최종검색일 : 2023. 08. 19.)

아주경제, "지하철 물품보관함, 보이스 피싱 장소로 전락?...교통공사 주의 당부", 2022.02.15. https://www.ajunews.com/view/20220215164829682 (최종검

색일 : 2023.08.30.)

연합뉴스 2023년 5월 9일자, "'주식손해보상' 미끼로 접근…신종 보이스피싱 주의보" (https://www.yna.co.kr/view/AKR20230509081400004?input=1195z, 검색일: 2023년 7월20일).

연합뉴스, "[진화하는 보이스피싱] ③ "극단적 선택까지"···갈수록 심해지는 폐해(끝)", 2023.05.27. https://www.yna.co.kr/view/AKR20230526109400061?input=1195m (최종검색일 : 2023. 08. 20.)

연합뉴스, "'로맨스 스캠' 피해자 70%가 여성···30대 이하가 87%", 2023.05.28. https://www.yna.co.kr/view/AKR20230527033000004 (최종검색일 : 2023. 08 12.)

연합뉴스, "'앱 하나 깔았다가'···휴대폰 속 모든 정보가 피싱범에게로", 2023.05.25. https://www.yna.co.kr/view/AKR20230525053000061 (최종검색일 : 2023. 08. 05.)

인천지방법원 김도윤 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰

인천지방법원 김지수 변호사, 2023.07.20., 보이스피싱 범죄 유형 관련 인터뷰

일요서울, "[심층취재]'신종 보이스피싱' 오픈뱅킹·간편송금 등 "돈 되찾기 더 어려워" 사기수법 지능화", 2023.08.07. http://www.ilyoseoul.co.kr/news/articleView.html?idxno=477290 (최종검색일 : 2023. 08. 28.)

조선일보 2023년 5월 8일자, 직접 결제해 상품권 번호까지 넘겼다…진화한 상품권 피싱에 눈물 흘리는 청년들(https://www.chosun.com/national/national_general/2023/05/08/3GM6DRTQFRHL3IPEQRL4YTQTBY/?utm_source=naver&utm_medium=referral&utm_campaign=naver-news, 검색일: 2023년 5월 10일).

중앙일보, ""보증금 도와줘"영통까지 한 친구···'딥보이스'피싱에 당했다", 2023.06.18. https://www.joongang.co.kr/article/25170581#home (최종검색일 : 2023. 08. 20.)

카카오, "메신저 피싱, 사기범들은 이렇게 접근합니다(사례를 통해 알아보는 피해 예방 요령), 2019.10.17. https://brunch.co.kr/@andkakao/125 (최종검색일 : 2023. 08. 05.)

카카오뱅크, "내 퓨대폰에 숨어 있는 악성앱, 카카오뱅크가 찾아드려요",

https://www.kakaobank.com/bank-story/234 (최종검색일 : 2023. 08. 05.)
한겨레, "'몸캠 피싱' 협박해 현금숙책 활용...보이스피싱의 '신종 인력 충원'", 2023.01. 30. https://www.hani.co.kr/arti/society/society_general/1077426.html (최종검색일 : 2023. 08. 20.)

Abstract

A Study on the Response Plan for each Stage of Voice Phishing Crime

Yoon Hae-Sung, Jeon Young-sil, Lee Jung-Min, Kim Gye-Hwan

Voice phishing crime has been recognized as a representative crime that infringes on the economy of the common people. However, recently, thanks to the development of communication and financial technology, we can see that the methods are becoming more and more sophisticated. Voice phishing, which first occurred in 2006, is now causing crimes targeting the entire population and the amount of damage is on the rise.

Moreover, with new technologies and non-face-to-face authentication services, it is clear that voice phishing crimes are evolving further. Therefore, this study aims to establish step-by-step supplementary measures for voice phishing crimes due to advanced, intelligent, and advanced technology, as well as preventive and damage relief checks.

In response, we diagnosed the problems of the current voice phishing crime and sought countermeasures through interviews with working-level officials from various fields, including the government departments, the Financial Supervisory Service and the Financial Services Commission, the National Police Agency and the Prosecution Service, the Korea Communications Commission, and the Ministry of Science and ICT.

In particular, with the help of the Financial Supervisory Service and the National Police Agency, he helped conduct empirical research with the support of the latest statistics and cases related to voice phishing crimes. In addition,

I received a lot of help in conducting this study with the advice of prosecutors and lawyers related to voice phishing crimes. With the help of many experts and practitioners, we tried to understand the step-by-step method of voice phishing crimes as much as possible and analyze the means by crime type, such as crime methods and victim characteristics.

Furthermore, we focused on diagnosing the government's measures and presenting implications for damage relief. Based on the results of this study, we hope that voice phishing crimes will no longer take root and contribute to the development and dissemination of technologies for the Fourth Industrial Revolution that can be used with confidence, hoping to establish preemptive preventive measures and use them in the research results of securing evidence and tracking criminals.

연구총서 23-AB-05

보이스피싱 범행단계별 대응방안 연구

발　　행 | 2023년 9월
발 행 처 | 한국형사·법무정책연구원
발 행 인 | 하 태 훈
등　　록 | 1990. 3. 20. 제21-143호
주　　소 | 서울특별시 서초구 태봉로 114
전　　화 | (02)575-5282
홈페이지 | www.kicj.re.kr
정　　가 | 7,000원
인　　쇄 | 고려씨엔피 02-2277-1508/9
I S B N | 979-11-91565-94-2 93360