금융생활에 필요한 모든 정보, 인터넷에서 「파인」 두 글자를 쳐보세요

"금융은 튼튼하게, 소비자는 행복하게"

보 도 참 고 자 료

보도	배포 후 즉시	배포	2020. 9. 9.(수)

담당부서	불법금융대응단	이선진 팀장(3145-8521), 신상주 선임조사역(3145-8125)

제 목 : 신분증·카드번호를 요구하는 자녀 사칭형 보이스피싱 경보!

▣ 소비자경보 2020 - 14호			
등급	주의	경고	위험
대상	금융소비자 일반		

소비자 경보 내용

◈ 최근 사기범이 **가족**을 **사칭**하여 **문자**로 **접근**한 후 피해자의 **개인(신용)정보**를 **탈취**하여 **자금**을 **편취**하는 신종 **피해사례**가 발생

○ 특히, 탈취한 개인(신용)정보를 활용해 **피해자 명의**로 **핸드폰 개통**과 **계좌개설** 후 **대출**까지 받아 **피해***가 확대

* 최근 금융감독원에 이와 같은 사례로 피해구제신청서가 접수된 건은 총 229건

◈ 이에, **가족**(아들, 딸)을 **사칭**한 **문자메시지**로 다음 사항에 해당하는 내용을 요구할 경우 **보이스피싱이 의심**되므로 **각별한 주의**가 필요

* 실제 사기범의 문자메시지 사례는 <붙임>을 참조

○ 핸드폰 **고장·분실** 등을 **이유**로 평소와 **다른 전화번호**를 사용하여 **문자**로 가족에게 **접근**

○ 온라인 소액결제 등의 사유로 피해자(부모 등 가족)에게 **주민등록증 사본, 신용카드번호** 등 **개인(신용)정보**를 **요구**

○ **원격조종 앱** 등 출처 불분명한 **앱 설치**를 **요구**

⇒ 위와 같은 문자 수령시 **가족인지 확인** 전까지는 **응대 거절**하고, 특히 **신분증 사본, 카드번호** 등 **개인(신용)정보**는 절대 **제공 금지!**

1 소비자경보 발령 배경

□ 최근 가족을 사칭하여 부모에게 접근한 후 **개인(신용)정보*를 탈취**하고, **원격조종 앱 설치**를 유도하여 **자금을 편취하는 신종 보이스피싱이 급증****

* 주민등록증(운전면허증) 사본, 은행 계좌번호(비밀번호), 신용카드 번호(비밀번호) 등

** 최근 이와 같은 사례로 금융감독원에 피해구제신청서가 접수된 건은 총 229건

○ 그간 **지인을 사칭하여 카카오톡('메신저 피싱')** 등 SNS를 통해 **자금 이체**를 **유도**하는 피해사례는 지속 발생해 왔으나,

○ SNS가 아닌 **문자**를 **피해자**에게 **보내,** 직접적인 자금의 이체를 **유도하기 보다는 개인 및 신용정보를 탈취하여 피해자 명의로 계좌 개설 후 자금 이체** 및 **대출을 받는 사기수법**이 새롭게 나타남

□ 이에, 최근 **가족(특히 아들, 딸)을 사칭**한 **문자메시지**로 보이스피싱을 **유도**한 피해사례에 대해 **각별한 주의가 필요하여 소비자 경보를 발령함**

2 소비자 행동 요령

□ **(문자로 금전 및 개인정보 요구시)** 가족 및 지인 등이 문자 또는 메신저로 **금전** 및 **개인(신용)정보를 요구**하는 경우 **반드시 가족 여부를 확인**하고, **의심스러운 경우 무조건 거절**할 필요

○ 핸드폰 고장, 분실 등의 **사유로 연락이 어렵**다고 하면 **더욱더 주의**

□ **(출처가 불분명한 앱 설치 요구시)** 사기범이 원격조종 앱 등 악성앱 설치를 유도할 수 있으므로 출처가 불분명한 앱 설치 요구시 **무조건 거절**

□ **(보이스피싱 피해를 입은 경우)** 송금 또는 **입금 금융회사 콜센터** 및 **금융감독원 콜센터**(☎1332)에 전화하여 해당 계좌에 대한 **지급정지 요청** 및 **피해구제신청을 접수**

○ **"계좌정보통합관리서비스*"**(www.payinfo.or.kr)를 활용하여 본인도 모르게 **개설된 계좌** 또는 **대출을 한눈에 확인**

* '내계좌한눈에', '내카드한눈에', '금융정보조회' 코너를 활용

○ 개인정보 유출에 따른 추가 피해를 막기 위해 금융감독원 금융소비자 정보포털, **'파인'**의 **『개인정보노출자 사고예방시스템』***도 적극 활용

* 개인정보 노출사실을 시스템을 통해 금융회사가 공유해 본인 확인에 더욱 주의토록 함으로써 사고를 예방하기 위해 마련된 시스템('03.9월)

○ **본인이 알지 못한 핸드폰 개통 여부**는 한국정보통신진흥협회에서 운영하는 **명의도용방지서비스**(www.msafer.or.kr)에 접속하여 **가입사실현황***을 **조회**

* 피해자 명의로 가입된 휴대전화 등의 통신서비스 가입현황을 조회일자 기준으로 확인

□ 아울러, 보이스피싱 위험으로부터 스스로를 보호하기 위해 아래의 **보이스피싱 피해예방 핵심 행동요령**을 **숙지**하시길 당부드림

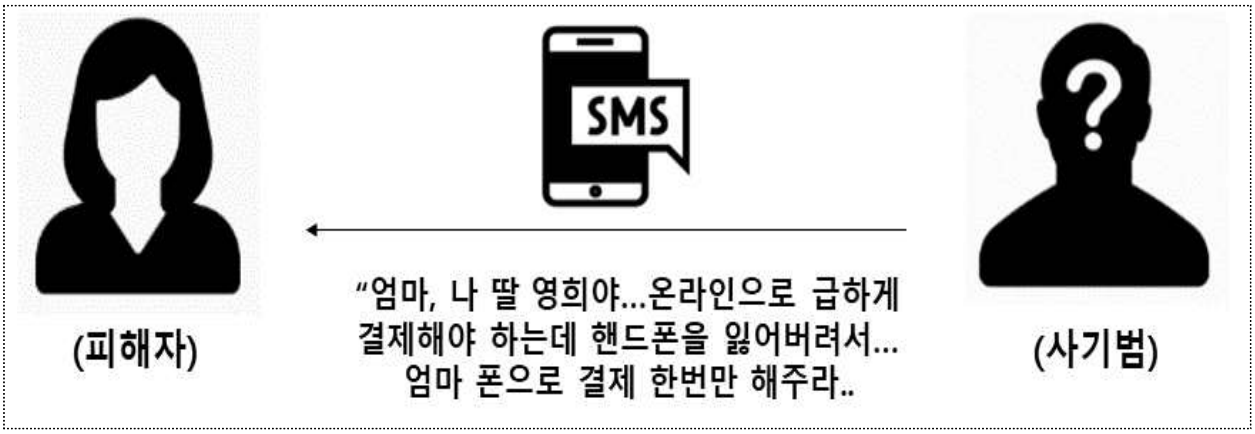
보이스피싱 피해예방 핵심 행동요령

1. 카카오톡·문자 등을 통해 금전을 요구하면 유선 확인 전까지 무조건 거절
2. 문자를 보내 신분증 사본, 계좌번호·신용카드 번호 요구시 절대 제공 금지
3. 출처 불분명 앱, URL 주소는 무조건 클릭 금지
4. 등급 상향, 저금리 전환, 대출 수수료 명목 금전 요구는 무조건 거절
5. 검찰·경찰 · 금감원이라며 금전을 요구하면 무조건 거절

3 구체적 신종 보이스피싱 수법

1 딸 · 아들을 사칭하여 급하게 도움이 필요하다며 부모에게 접근

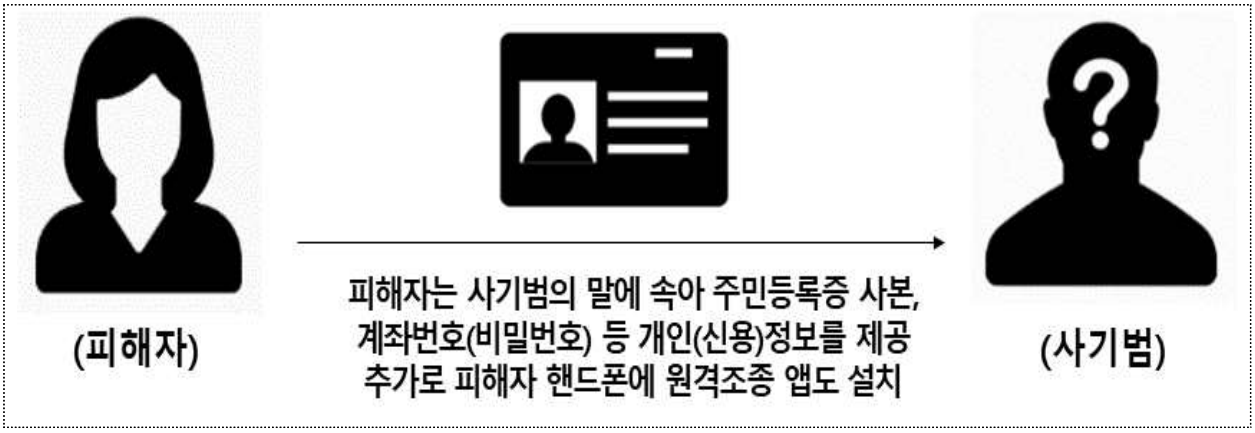
○ 대부분 **자녀를 사칭**하여 온라인 소액 결제, 회원 인증 등을 사유로 **부모에게 문자로 접근**



2 결제, 인증 등의 사유로 피해자에게 개인 및 신용정보 제공을 요구

○ **온라인 결제, 회원인증** 등을 위해서는 피해자의 주민등록증 사본, 신용카드 번호 및 비밀번호가 필요하다며 **개인 및 신용정보를 요구**

○ 그 이후 결제(인증)가 잘 안된다며, 피해자 폰으로 직접 처리를 하기 위해 **원격조종 앱을 설치하도록 유도**

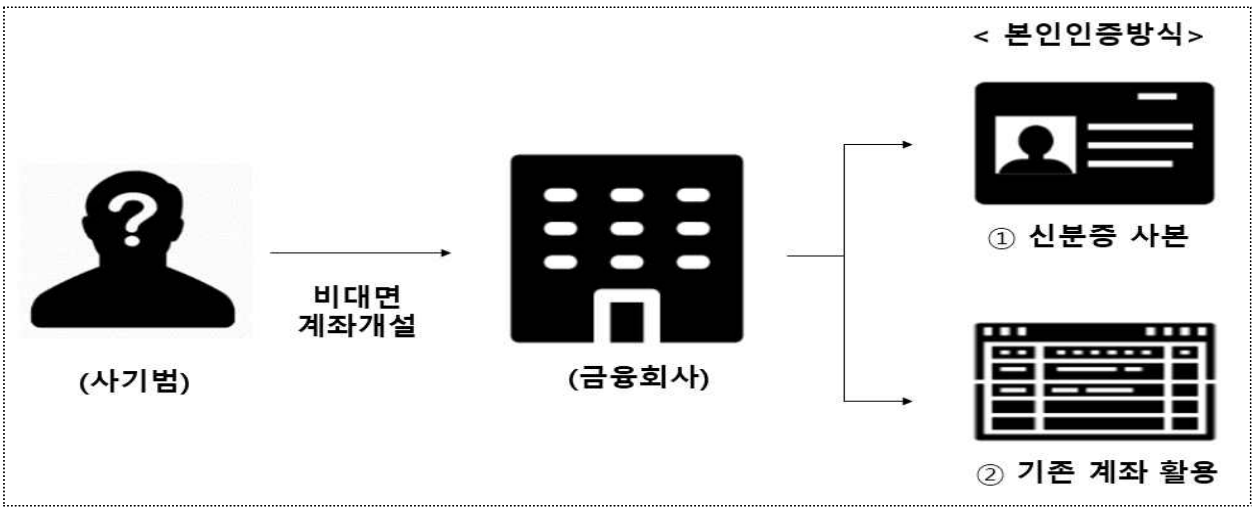


3 탈취한 개인 및 신용정보를 활용하여 피해자 명의 비대면 계좌 개설

○ 사기범은 **탈취한 신분증과 개인·신용정보**를 **활용**하여 피해자 명의로 **핸드폰**(주로 선불 알뜰폰)을 **개통**한 후

○ 피해자 명의의 핸드폰과 **신분증** 등을 **이용**하여 금융회사에 **비대면 방식**으로 **계좌를 개설**

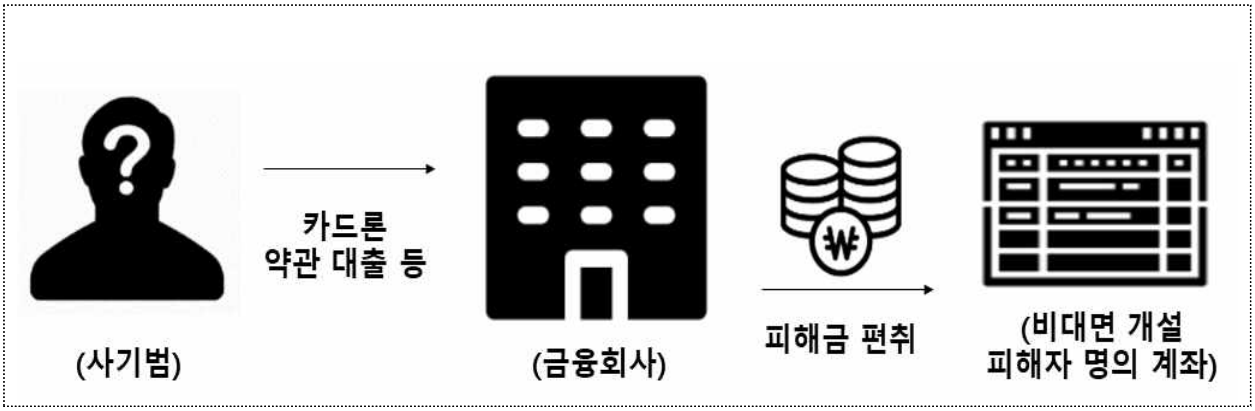
○ 사기범은 사기 과정에서 **원격조종앱**을 통해 **피해자의 모바일앱**에 **접근**도 하고, 계좌개설시 등 **금융회사가 제공하는 안내문자** 등도 가로채는 것으로 보임



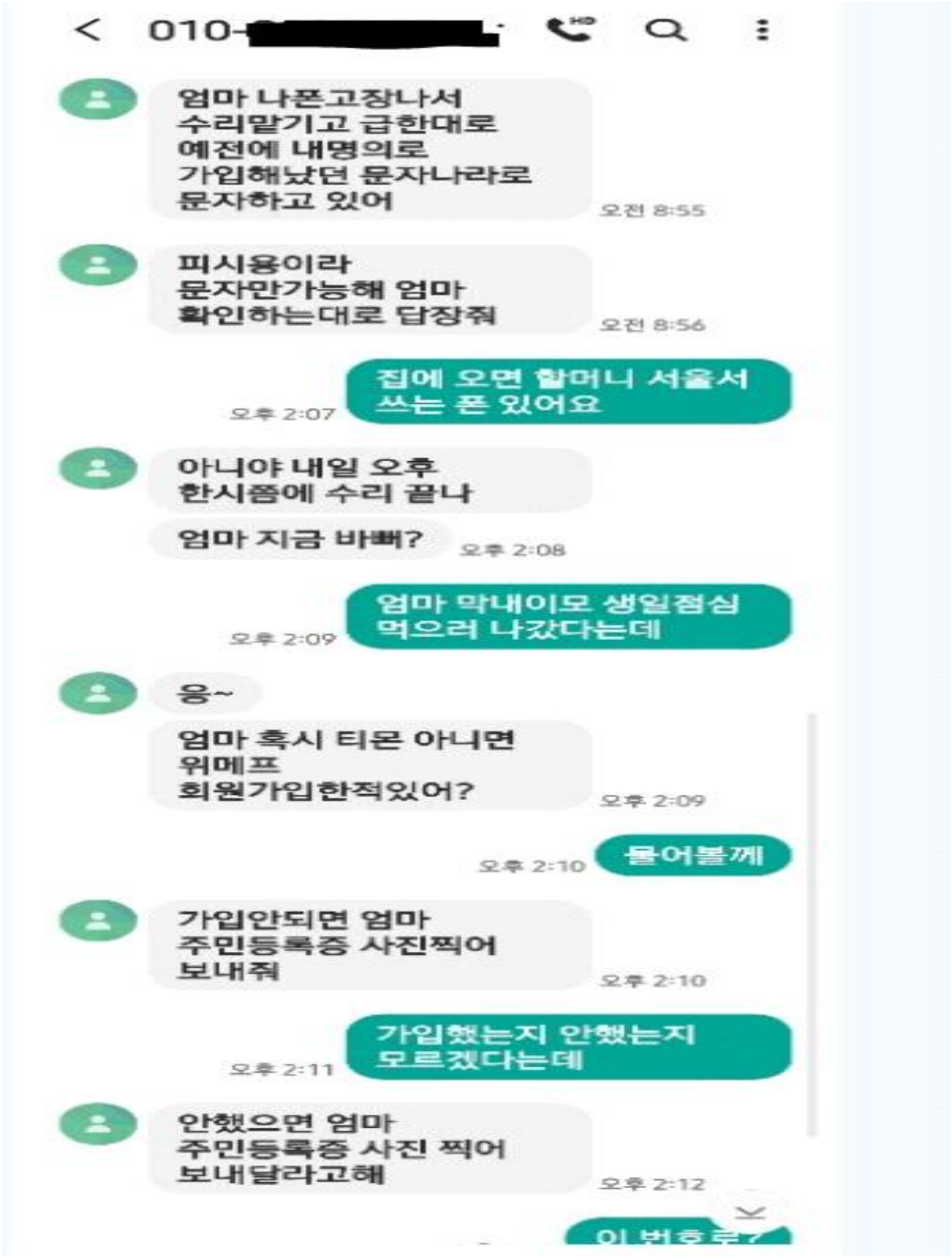
* 신분증 사본 + 기존계좌 활용 방식(계좌개설시 개설 금융회사가 피해자 명의의 다른 은행 계좌로 1원 송금시 적요란에 적혀있는 숫자를 확인)을 주로 사용

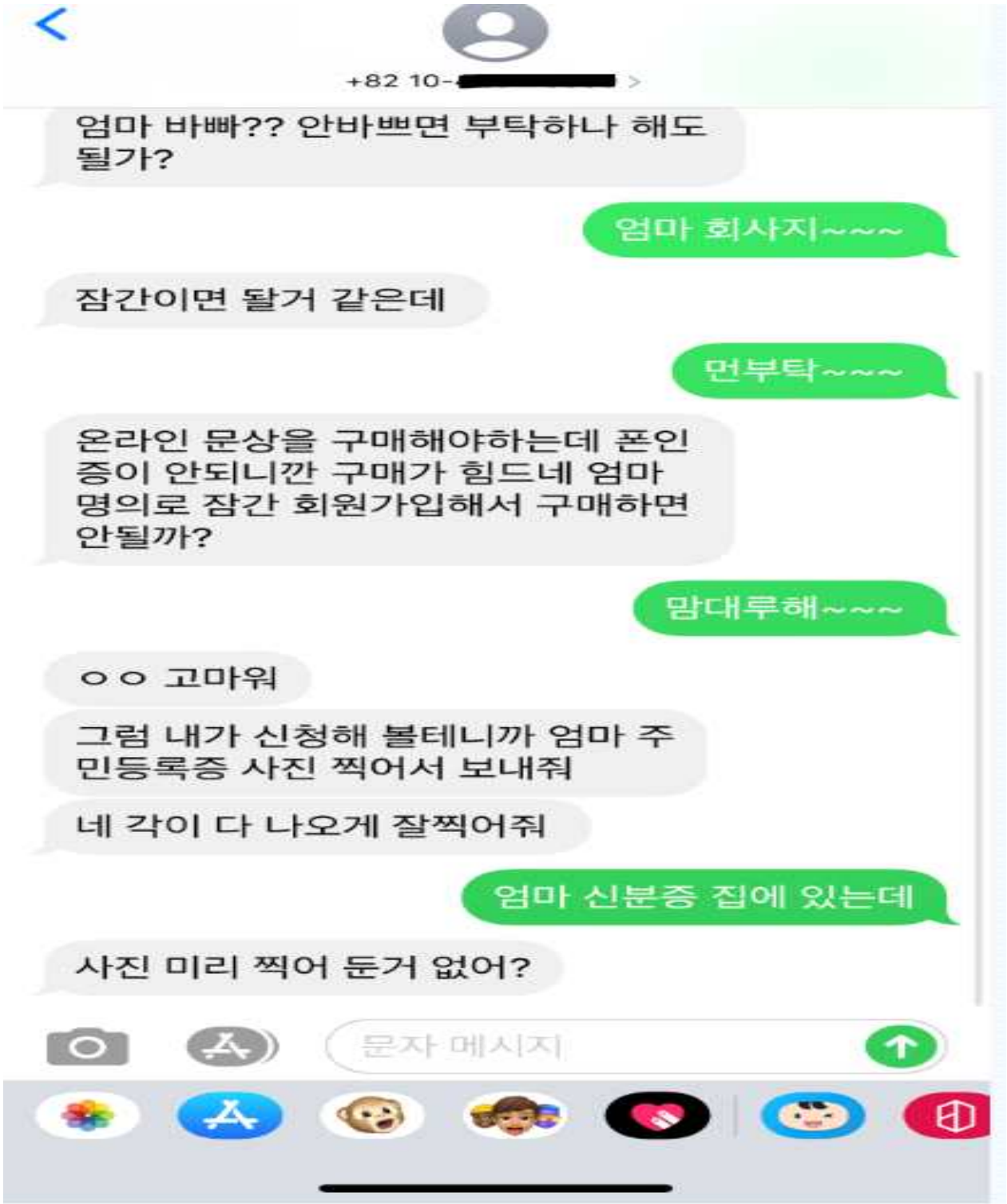
4 탈취한 개인 및 신용정보를 활용하여 피해자 명의로 대출 신청

○ 사기범은 탈취한 신분증과 신용정보를 활용하여 금융회사로부터 **피해자 명의 카드론, 약관대출 등 대출**을 **받고, 비대면으로 개설한 계좌에 이체**



붙 임 | **보이스피싱 실제 문자 사례**





☞ 본 자료를 인용하여 보도할 경우에는 출처를 표기하여 주시기 바랍니다.(http://www.fss.or.kr)