금융분야 보이스피싱 대응방안

2022. 9.

관계기관 합동

목 차

Ⅰ. 추진배경 ····· 1

Ⅱ. 보이스피싱 대응방안 ····· 2

1. 대면편취형 보이스피싱 ····· 2

2. 비대면 계좌개설 ····· 4

3. 오픈뱅킹 ····· 6

4. 원격제어 ····· 7

5. 여신금융회사 ····· 8

6. 기존 대응수단 강화 ····· 8

Ⅲ. 향후 추진계획 ····· 10

[참고1] 현행 보이스피싱 관련 제도 ····· 12

[참고2] 금융결제원을 통한 신분증 진위확인 시스템 ····· 13

Ⅰ. 추진배경

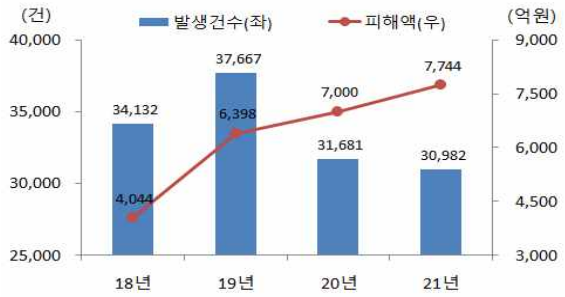
□ 정부와 금융권의 **보이스피싱 대응노력***으로 피해자가 범죄자에게 자금을 이체하는 **계좌이체 방식의 보이스피싱**은 **감소**

* 사기이용계좌 지급정지, 지연인출제, 사기이용계좌 명의인 등록 등

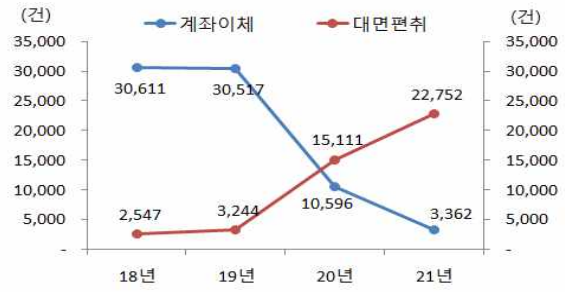
□ 그러나 최근에는 기존 대응체계를 회피하는 **새로운 유형의 보이스피싱**이 **증가**하고 **피해금액**도 **점차 확대**

❶ (**대면편취**) 계좌이체 없이 피해자를 **직접 만나 현금을 건네받는** 대면편취형 보이스피싱이 크게 증가

< 보이스피싱 건수·피해액(경찰청) >



< 보이스피싱 유형별 건수(경찰청) >



❷ (**비대면 계좌개설**) 피해자의 개인정보를 탈취하여 **피해자 명의의 계좌**를 **비대면으로 신규 개설**하고,

- (**오픈뱅킹**) 오픈뱅킹 가입 후, **피해자의 모든 계좌**에서 **직접 이체**

□ 어려운 경제상황에서 보이스피싱과 같은 민생침해 범죄가 증가할 수 있어 정부는 **보이스피싱 엄단**을 **국정과제**로 발표하고 **대응***

* 보이스피싱 범죄 정부합동수사단 출범, 보이스피싱 통합 신고·대응센터 설립 중

○ 이에 금융권도 보이스피싱 피해 예방 등을 위한 '**금융분야 보이스피싱 대응방안**'을 **마련**

- 특히, **디지털 환경의 취약점**을 악용하는 보이스피싱 수법에 **적극 대응**할 필요

Ⅱ. 보이스피싱 대응방안

1 대면편취형 보이스피싱

1. 대면편취형 보이스피싱에 피해구제절차 적용

□ (문제점) **대면편취형 보이스피싱**에 사용된 **사기이용계좌**에는 「통신사기피해환급법」에 따른 **지급정지 등 피해구제 불가**

○ 「통신사기피해환급법」 상 전기통신금융사기의 경우, 금융회사는 피해자 신고 등에 따라 **사기이용계좌***를 **지급정지**

* 피해자의 자금이 송금·이체된 계좌 및 해당 계좌로부터 자금이전에 이용된 계좌

○ **대면편취형 보이스피싱**은 전기통신금융사기*에 해당하지 않아 보이스피싱 조직원을 검거하여도 **신속한 지급정지**가 **불가능**

* 자금을 송금·이체하도록 하거나 자금을 송금·이체하는 행위

- 검거한 조직원을 수사하는 도중 **다른 공범**이 **피해금**을 **인출**

□ (**대응방안**) 대면편취형 보이스피싱도 지급정지 등 **피해구제**가 될 수 있도록 **「통신사기피해환급법」 개정**을 추진

* 현금을 제공받거나 제공하게 하는 행위도 전기통신금융사기에 포함

○ **수사기관***이 대면편취형 보이스피싱에 사용된 사기이용계좌를 확인하면, 금융회사에 **지급정지**를 **신청**

* 대면편취의 경우 자금의 송금·이체 기록이 없어 피해자가 사기이용계좌를 특정할 수 없으므로 경찰이 수사과정에서 계좌를 특정하여 신청

- **ATM 무통장입금**을 진행하고 있는 **범죄자를 검거**하여 신속히 **계좌**를 **지급정지**함으로써 범죄조직의 **범죄수익 획득**을 **방지**

○ **수사기관**이 피해자와 피해금액을 **특정**하면, **채권소멸**과 **피해환급금 지급** 등 구제절차를 **진행**

○ **선의의 계좌명의인**을 **보호**하기 위한 이의제기 등의 절차도 적용

2. ATM무통장입금 한도 축소

□ (문제점) **실명확인 절차가 없는 ATM 무통장입금**을 통해 대면 편취한 자금을 **범죄조직 계좌**로 **집금하는 등 범죄에 활용**

❶ ATM 무통장입금은 **동일인**이 하루에도 수차례 입금(1회 입금 한도 100만원)을 통해 **큰 금액**을 **송금 가능**

- 일부 ATM기기는 무통장입금 시 주민등록번호를 입력토록 하나, **타인 또는 가상의 번호**를 입력하더라도 **입금 가능**

❷ ATM 무통장입금을 통해 **수취할 수 있는 금액**에 **제한이 없어** 범죄조직이 **자금세탁 목적**으로 활용하기에도 **용이**

□ (**대응방안**) 실수요자의 불편을 최소화하는 범위에서 **ATM 무통장입금 관련 이용한도**를 **축소**

❶ 실명확인 없는 **ATM 무통장입금 한도**를 **축소**(1회 100만원 → 50만원)

- 전체 송금·이체 거래 중 **ATM 무통장입금**의 **비중***은 **매우 낮고, 실수요자**는 **50만원 단위로 나누어서 입금 가능**

* 국민·기업·신한·우리·하나은행 수단별 송금·이체 비중('22.1분기, %) : (모바일)71.01, (인터넷)14.59, (ATM매체)10.46, (텔레뱅킹)2.17, (창구)1.41, (ATM무매체)0.36

- 반면, 대면편취형 보이스피싱 범죄자(수거책)에 대한 **검거***는 **증가**할 것으로 예상

* 최근 반복적인 ATM 무통장입금 행위를 수상히 여겨 신고하는 사례가 많아 ATM 무통장입금 횟수가 많아질수록 수거책이 검거될 가능성은 증가

❷ 수취계좌의 실명확인 없는 **ATM 무통장입금 수취한도**(1일 300만원*)를 **신규 설정**

* ATM 무통장입금을 통해 송금받는 계좌의 약 99.6%는 일일 수취금액이 300만원 이하

- **ATM 매체**(통장·카드) **입금, 창구, 비대면 채널** 등을 통한 자금 수취는 기존과 동일하게 사용 가능

- 반면, 보이스피싱 조직의 **범죄수익 집금 과정**은 **크게 불편**

2 비대면 계좌개설

1. 비대면 계좌개설 시 본인확인 강화

□ (문제점) **신분증 사본 제출**을 통한 **실명확인** 과정이 신분증 **위조** 또는 **도용**에 **취약**

< 비대면 실명확인 방법 >

의무 (2개 이상)	권고 (1개 이상)
① **신분증 사본 제출** ② 영상통화 ③ 접근매체 전달과정에서 확인 ④ **기존계좌 활용**(1원 송금) ⑤ 기타 이에 준하는 방법(생체인증 등)	⑥ 타 기관 확인결과 활용 (인증서, I-Pin, 휴대폰 인증 등) ⑦ 다수의 고객정보 검증 (전화번호, 주소, 이메일 등)

❶ 금융결제원을 통한 **신분증 진위확인시스템**(참고2)을 **활용하지 않는 금융회사***는 **위조된 신분증 검증**에 **실패**

* 신분증의 문자정보(주민등록번호, 발급번호 등)만을 대조하므로 사진위조에 취약

- 특히, 중·소형 증권사의 **신분증 진위확인시스템 활용**이 **저조**

- 오픈뱅킹 참여 시, 해당 업권을 활용한 **사기이용계좌**가 **증가**

* ('20.12월) 증권사, 상호금융 ('21.4월) 저축은행

< 업권별 사기이용계좌 수 >

< 사기이용계좌 수 추이(오픈뱅킹 참여=100) >

❷ 신분증 **진위확인시스템**은 신분증 **도용여부**는 **검증 불가**

□ (**대응방안**) **제출된 신분증 사본**에 대한 **본인확인 절차**를 **강화**

❶ **'신분증 사본 제출'**을 통한 비대면 실명확인 과정은 반드시 **신분증 진위확인시스템**(금융결제원)으로 진위여부를 검증

- **신분증 진위확인시스템을 통과하지 못하는 경우** '신분증 사본 제출' 방식은 **사용 불가***

* 이 경우 신분증 사본 제출 外 2개 이상의 실명확인을 거칠 필요 :
(예시) 영상통화 + 기존계좌 활용

❷ **안면인식 시스템**을 **도입**하되, **자체도입이 어려운 금융회사**는 **금융결제원**을 통한 안면인식 시스템(개발 예정)을 활용 가능

- 시스템 도입 초기에는 **낮은 인식률**로 인한 **소비자 불편*** 등이 있을 수 있어, **일정기간은 권고사항으로 운영**

* 신분증 진위확인시스템 → 안면인식을 통한 본인인증(추가) → 1원 송금

2. 1원 송금을 통한 실명확인 절차 보완

□ (**문제점**) 1원 송금의 허점을 이용한 **대포통장 개설 사례**가 발생

❶ 일부 금융회사는 1원 송금을 통한 실명확인 과정에서 **인증번호 유효기간**을 지나치게 **길게 설정**(7일~14일)

- 대포통장 구매자가 **ID·비밀번호**를 **설정**할 수 있는 시간*을 확보

* (대포통장 유통업자) 비대면 계좌개설이 진행중인 대포폰과 1원송금 인증번호를 판매 → (대포통장 구매자) 직접 ID와 비밀번호를 설정 : 1~2일 소요

❷ 피해자는 **비대면 계좌개설 절차가 진행중**이라는 사실을 **인지하지 못하고** 본인계좌로 도착한 **인증번호**를 타인에게 **전달**

□ (**대응방안**) 1원 송금방식이 대포통장 개설에 이용되지 않도록 정비

❶ 모든 금융회사가 1원 송금을 통한 인증번호의 **입력 유효기간**을 최대 **15분 이내로 단축**

❷ 1원 송금 시, **'계좌개설용'**이라는 문구를 인증번호와 함께 표기

3 오픈뱅킹

1. 피해규모 축소

□ (**문제점**) 비대면으로 피해자 명의의 **알뜰폰**을 **개통**하고 계좌를 개설한 범죄자는 **오픈뱅킹**을 통해 직접 **자금**을 **편취**하므로,

○ 직접 자금을 이체하지 않은 **피해자**는 피해 발생 후에도 상당 시간 동안 **피해 사실을 인식하지 못할 가능성**

□ (**대응방안**) 범죄자의 오픈뱅킹을 통한 **자금편취**를 **최소화**

❶ (**일정기간 활용 제한**) 금융회사는 **비대면 계좌개설**을 통한 오픈뱅킹 가입 시 **3일**간 오픈뱅킹을 통한 **자금이체**를 **차단***

* 소비자는 본인의 다른 금융회사 앱 등에 직접 접속하여 이체 가능

- 금융결제원은 **오픈뱅킹 신규 가입 시 3일간** 해당고객의 **이용한도***를 **축소**(1일 이용한도 : 1천만원 → 300만원)

* 자금이체가 아닌 결제, 선불충전 등의 목적으로만 이용 가능

❷ (**이상거래 탐지강화**) 오픈뱅킹 가입 시 계좌제공기관과 이용기관 간 **고객 전화 식별정보 등**을 **공유**할 수 있는 **시스템**을 **구축**

- 금융회사는 同시스템과 FDS(이상금융거래탐지시스템)를 통해 **이상거래로 판단**될 경우 **거래 차단**

2. 피해자 방어수단 마련

□ (**문제점**) **범죄자**가 피해자의 계좌에서 **직접 자금을 송금·이체**하는 범죄에 피해자가 **대응할 수 있는 수단**이 **부재**

○ 직접 자금을 송금·이체한 피해자는 **사기이용계좌 지급정지**를 통해 범죄 피해금이 이전된 **모든 계좌**의 **자금이전**을 신속하게 차단

○ 그러나 범죄자에게 개인정보를 노출시킨 피해자가 **본인명의 계좌의 자금이전 등**을 **신속하게 차단**할 수 있는 수단이 **부재**

□ (**대응방안**) 범죄자의 오픈뱅킹을 통한 **자금편취**를 **최소화**

❶ (**오픈뱅킹 가입제한**) 피해자가 **개인정보노출자 사고예방 시스템***(금감원) 등록 시, 명의인의 **오픈뱅킹 가입신청 및 계좌 연결**을 **제한**

* 개인정보 노출 사실 등록 시, 계좌개설·대출·카드발급을 제한

❷ (**본인계좌 지급정지**) 피해 발생(우려)시, 피해자가 **본인명의 계좌의 거래**를 **일괄/선택 제한**할 수 있는 시스템을 구축

- (**1단계**) 피해자가 **계좌정보통합관리서비스**(어카운트인포)에서 명의도용 계좌 개설여부를 확인하고, **지급정지 신청**

- (**2단계**) 피해자가 **금융회사 창구 및 고객센터**를 통해서도 본인명의 계좌에 대한 **일괄 지급정지**를 **신청 가능**

4 원격제어

□ (**문제점**) 피해자가 폰에 **원격조종 앱을 설치토록 유도**한 후 원격조종 앱을 통해 **범인이 오픈뱅킹 가입·자금이체**

* 피해자에게 원격조정앱 설치 유도 → 범인이 원격조정 앱을 실행하고 미리 받은 신분증 사진, 휴대전화 인증번호 등 필수정보 입력 후 오픈뱅킹 가입

○ 금융회사 앱 구동 시 **원격조정 앱 연동**을 **차단**하면 범죄 피해를 줄일 수 있으나, 이를 **차단하지 않은 금융기관**이 존재

□ (**대응방안**) 금융회사는 금융회사 앱과 **원격조종 앱이 연동되지 않도록** 하고, 금융보안원이 이를 **점검**

○ **디지털 취약계층 지원**을 위한 경우, 금융회사 고객센터 등과의 연동은 허용되나,

- 이 경우에도 **계좌개설·자금이체·대출신청 등 거래 관련 기능**은 **반드시 차단**

5 여신금융회사

□ (**문제점**) 금융실명법에 따른 실명확인 적용대상이 아닌 **카드사** 등은 주로 **핸드폰 또는 인증서를 통해 본인인증**을 진행

○ 피해자 명의의 알뜰폰을 보유하고 있는 범죄자가 피해자 명의의 앱 카드 발급 후, **카드론**을 **실행**하는 사례가 발생

□ (**대응방안**) 여신금융회사도 **카드발급** 또는 **대출신청** 단계 중 선택하여 **신분증 사본을 제출**받고,

○ **신분증 진위확인시스템**(금융결제원)을 통해 **신분증 진위여부 검증절차**를 적용

6 기존 대응수단 강화

1. 보이스피싱에 대한 처벌강화

□ (**문제점**) 보이스피싱 범죄 자체에 대한 **처벌규정**이 **상이**하고 **수준**도 **낮으며**, 단순 **조력행위**에 대한 **처벌규정**은 **부재**

○ 현재 **보이스피싱**(전기통신금융사기)은 「형법」 상 **사기죄**(10년 이하의 징역 또는 2천만원 이하의 벌금)에 해당하며,

- **「통신사기피해환급법」 제15조의2**는 사기죄 적용이 불확실한 유형의 보이스피싱*을 **처벌**(10년 이하의 징역 또는 1억원 이하의 벌금)하기 위해 신설된 조항('14.1.28.)

* 컴퓨터 등 정보처리장치에 타인으로 하여금 정보 또는 명령을 입력하게 하는 행위 또는 타인의 정보를 이용하여 정보 또는 명령을 입력하는 행위

○ **단순 조력행위**(피해금 송금·인출·전달 등)는 별도 처벌규정이 없어 위법성에 대한 **경각심**이 **부족**

□ (**대응방안**) **「통신사기피해환급법」**에 **보이스피싱**과 **단순 조력 행위**에 대한 **처벌규정**을 마련

○ 전기통신금융사기범에 **'1년 이상의 유기징역** 또는 **범죄수익의 3배 이상 5배 이하**에 상당하는 **벌금***'을 부과하고,

* 「자본시장법」§443조의 미공개정보 이용, 시세조종 등과 동일

- 단순 조력행위자에도 **'5년 이하의 징역** 또는 **5천 만원 이하의 벌금'**을 부과

○ **미수범**도 **처벌**하고 **상습범**은 **가중**하여 처벌

2. 보이스피싱 예방제도 설명 강화

□ (**문제점**) 고객 선택으로 적용 가능한 **보이스피싱 예방서비스**를 운영 중이나, **활용**이 **저조**

□ (**대응방안**) **계좌 개설** 단계에서 **보이스피싱 예방 서비스**에 대한 **설명**을 제공하고 **가입 의사**를 **확인**

〈 보이스피싱 예방서비스 〉

❶ (**지연이체**) 일정 금액(예 : 100만원) 이상 이체시 이체요청 이후 **일정 시간**(최소 3시간)이 경과 후 입금되는 서비스(입금 30분 前 취소가능, 창구거래 未적용)

❷ (**입금계좌지정**) 미리 지정하지 않은 계좌로는 **소액송금**(1일 100만원 이내 이체한도 설정)만 **가능**(창구거래 未적용)

❸ (**단말기 지정서비스**) **미리 지정**한 PC, 스마트폰 등 단말기에서만 공동인증서발급, 이체 등이 가능하도록 **접근권한**을 **제한**(최대 5개)

3. 홍보활동 강화

□ (**문제점**) 여러 관계기관이 **다양한 홍보활동** 중이나 진화하는 신종수법에 의한 **피해**가 **지속 발생**

□ (**대응방안**) 옥외전광판 등 기존의 홍보채널 외에 **웹 드라마** 등 **경각심 제고 효과**를 **극대화**할 수 있는 수단* 활용

* 계층별·범죄수법별 맞춤형 홍보영상 제작·방영 등

Ⅲ. 향후 추진계획

1 **법 개정**이 필요한 과제는 방안발표 직후 **의원입법**을 **추진**하여 조속히 국회에 제출

2 **시스템 개발**과 **규정개정 등**도 신속히 추진하여 **속도감 있게 집행**

3 금번 방안 발표 후에도 진화하는 **보이스피싱에 대응하기 위한 여러 방안***을 **지속 보완**

* 예) 최근 보이스피싱 범죄피해금의 현금화 수단으로 활용되고 있는 전자금융업자(선불충전업자)에 대한 대책 등

< 세부 추진계획 >

과제내용	추진계획	관계기관
1. 대면편취형 보이스피싱		
1 피해구제절차 적용	▸ 「통신사기피해환급법」 개정안 발의 협의 ('22.10월)	총괄기획단
2 ATM무통장입금 한도 축소		
❶ 입금한도 축소 ❷ 수취한도 신설	▸ 금융회사 내규 개정·시스템 개발 ('22년, 일부 금융회사는 '23.上)	금융회사
2. 비대면 계좌개설		
1 비대면 계좌개설 시 본인확인 강화		
❶ 신분증 진위확인 시스템 이용 확대	▸ 금융회사 시스템 구비 ('23.9월) ▸ 비대면 실명확인 가이드라인 개편 ('23.上)	금융회사 은행과
❷ 안면인식 시스템 도입	▸ 시스템 개발 ('23.下) ▸ 비대면 실명확인 가이드라인 개편 ('23.上)	금융결제원 은행과
2 1원 송금을 통한 실명확인 절차 보완		
❶ 인증번호 유효기간 단축 ❷ 계좌개설 표기	▸ 시스템 개발 ('22년)	금융회사

과제내용	추진계획	관계기관
3. 오픈뱅킹		
1 피해규모 축소		
❶ 이체·출금 제한(3일)	▸ 시스템 개발 ('23.上) ▸ 시스템 개발·오픈뱅킹 규정 개정 ('23.上)	금융회사 금융결제원
❷ 이상거래 탐지 강화	▸ 시스템 개발 ('22년)	금융결제원
2 피해자 방어수단 마련		
❶ 오픈뱅킹 가입 제한	▸ 시스템 개발 ('22년)	금융회사
❷ 본인계좌 지급정지 (1단계)	▸ 시스템 개발 ('22년)	금융결제원 금융회사
❷ 본인계좌 지급정지 (2단계)	▸ 시스템 개발 ('23.上)	금융결제원 금융회사
4. 원격제어		
원격조종 앱 차단	▸ 시스템 구축·점검 ('23.上)	금융회사 금융보안원
5. 여신금융회사		
본인확인 강화	▸ 업계 가이드라인 마련 ('23.上) ▸ 금융회사 시스템 구비 ('23.9월)	여전협회 금융회사
6. 기존 대응수단 강화		
1 처벌강화	▸ 「통신사기피해환급법」 개정안 발의 협의 ('22.10월)	총괄기획단
2 보이스피싱 예방 제도 설명 강화	▸ 설명자료 준비('22년)	금융회사
3 홍보활동 강화	▸ 강화된 홍보활동 시행('22~23년)	금융감독원 금융회사

참고1 현행 보이스피싱 관련 제도

1. 피해예방

1 (**지연인출·이체**) 100만원(1회) 이상 입금(송금·이체 등)된 통장에서 **자동화기기**를 통한 출금·이체 발생 시, **30분간 거래**를 **지연**

2 (**지연이체서비스**) 수취인 계좌에 **일정시간**(최소 3시간) **경과** 후 입금되며, 입금 **30분**前 **취소 가능**(창구거래 未적용)

※ 건별한도(최대100만원)를 설정하여 즉시이체 이용가능

3 (**입금계좌지정서비스**) 미리 지정하지 않은 계좌로는 **소액송금**(1일 100만원 이내 이체한도 설정)만 **가능**(창구거래 未적용)

4 (**해외IP차단서비스**) 국내사용 IP대역이 아닌 경우 **이체거래 차단**

5 (**은행전화번호진위확인서비스**) **은행**에서 고객대상으로 **전화·문자** 발송시 사용하는 **전화번호**를 **조회**

2. 피해 확산방지 및 구제

1 (**임시조치**) 금융회사 자체점검결과 **피해의심거래계좌**에 대해 **이체·송금**을 **지연 또는 일시 정지**

2 (**지급정지**) **보이스피싱 피해금**이 송금·이체 된 **사기이용계좌**의 전부에 대해 **지급**을 **정지**

3 (**전자금융거래제한**) **지급정지**가 이루어진 **계좌명의인**의 모든 **전자금융거래**를 **제한**

4 (**채권소멸·피해금환급**) **예금채권**을 **소멸**시켜 **피해자**에게 **환급**

5 (**전화번호이용중지**) 보이스피싱 범죄에 사용된 **전화번호 이용중지**

6 (**금융회사에 대한 조치**) 금융위는 **금융회사 또는 임직원**에 대하여 **권고·요구·명령 또는 개선계획 제출 명령** 가능

※ ❶ 금융회사 및 임직원에 대한 주의·경고·견책 또는 감봉, ❷ 금융회사의 전자금융거래 업무 수행에 있어 안전성과 신뢰성 확보를 위한 전산인력·전산시설·전자적 장치 등의 개선 또는 보완

참고2 금융결제원을 통한 신분증 진위확인 시스템

□ 창구, 모바일 등을 통해 제출된 신분증의 **문자**와 **사진 정보**를 **신분증 발급기관***에 등록된 정보와 비교하여 **진위여부**를 **확인**

* ('14.8월)행안부 ('15.7월)경찰청 ('17.1월)비대면 ('20.12월)외교부 ('22.12월[e])법무부

< 업무처리 절차 >

❶ 고객은 실명확인이 필요한 경우, 금융회사에 신분증 제출

❷ 금융회사는 제출된 신분증 스캔 후, 진위확인에 필요한 정보 추출

신분증	발급기관	추출 정보
주민등록증	행정안전부	성명, 주민등록번호, 발급일자, **사진특징점**
운전면허증	경찰청	성명, 주민등록번호, 면허증번호, 발급일자, **사진특징점**
여권	외교부	성명, 여권번호, 발급일자, MRZ(Machine Readable Zone), **사진특징점**

❸ 금융회사는 추출한 진위확인 정보를 결제원에 전송

❹ 결제원은 금융회사로부터 수신한 진위확인 정보를 행정정보공동이용센터(이하 '행공') 전문으로 변환 후 행공에 전송

❺ 행공은 결제원으로부터 수신한 진위확인 정보를 신분증 발급기관별로 전송

❻ 신분증 발급기관은 수신한 정보의 진위여부를 비교 검증

❼ 신분증 발급기관은 진위확인 결과정보를 행공에 전송

❽ 행공은 신분증 발급기관별로 수신한 진위확인 결과정보를 결제원에 전송

❾ 결제원은 행공으로부터 수신한 진위확인 결과정보를 금융회사 전문으로 변환 후 금융회사별로 전송

➡ 문자정보와 사진정보를 모두 비교함으로써 **위·변조 검증**에 효과적