
**금융분야 개인정보 유출
재발방지 종합대책**
- 경제혁신 3개년 계획 후속조치 -

2014. 3. 10

관계부처 합동

목 차

I. 그 간의 경과	1
II. 현황 및 문제점	2
III. 재발방지를 위한 세부과제	5
1. [정보 수집·보유·활용·파기] 단계별 정보보호 강화	6
2. [신용정보 주체의 권리 강화] 자기정보결정권 보장	15
3. [금융회사 책임 강화] 임원 책임 확대 및 엄정한 제재 ..	17
4. [정보보호·보안] 금융권 사이버 안전 대책 강화	21
5. [예방조치 강화] 기존 정보 처리 및 대응체계 구축	28
IV. 향후 계획	32
[참고] 종합대책 추진일정	33

I. 그 간의 경과

- 카드사 정보유출 사고 발생(검찰발표, '14.1.8)에 따라 금융위·금감원은 피해 확산 차단을 위한 대응방안을 즉시 발표(1.8)
 - * 해당 카드사에 즉시 현장검사 개시, 모든 금융회사의 개인정보처리 상태 점검, 피해 확산 차단 조치, 근본적인 재발방지대책 마련 추진
- 3개 카드사 및 KCB에 현장검사에 착수(1.13)하고, 「금융회사 CEO 긴급 간담회」를 개최(1.14)하여 정보보호 강화 촉구
- 금융위·안행부·방통위 등 유관기관 합동으로 재발방지 근본대책 마련을 위한 「금융회사 고객정보보호 정상화 TF」가동(1.17)
- 사고의 신속한 수습 및 안정화를 위해 재발방지 대책의 큰 틀 및 주요골자인 「금융회사 고객정보 유출 재발방지대책」 발표(1.22, 관계부처 합동)
- 불법정보 유통에 대한 국민 불안을 해소하기 위해 「개인정보의 불법 유통·활용 차단조치*」를 즉각 실시(1.24, 관계부처 합동)
 - * TM 등 비대면 영업제한, 대출모집인 모집경로 확인, 신속이용정지제도 등 → 엄격한 적법성 확인을 전제로 TM 영업부터 재개를 허용하는 「TM 등 비대면 영업제한 관련 후속조치」(2.4) 발표
- 3개 카드사에 대해서는 개인정보 유출에 대한 책임을 물어 법상 최고한도인 3개월 영업정지 처분(2.16)
- 국회 국정조사 과정에서 논의사항 및 그 간의 대책 등을 반영하여 종합적인 개인정보 보호강화 및 재발방지 방안을 마련

Ⅱ. 현황 및 문제점

◆ 금번 카드사 정보유출 사건을 계기로 금융회사의 개인 신용 정보에 대한 과도한 수집·활용 및 허술한 전산보안에 대한 우려가 제기

- 신용정보를 다루는 금융회사의 특성을 고려하여 엄격한 내부 통제방안을 마련하고 정보 수집·제공 체계를 정비할 필요

① (과도한 수집 관행) 금융회사 등이 영업에 필수적이지 않은 정보까지 수집*하여 장기간 보유

* 일반적으로 약 20여개(예: 전화번호, 주소) 많은 경우 약 50여개 항목 수집

- 불필요하게 과다하게 수집된 개인정보에 대한 관리소홀로 개인정보 노출시 불법 이용 등 피해 확산 우려

② (포괄적 동의 관행) 제3자 제공시 목적도 불분명한 “포괄적 동의” 등으로 인해 사실상 동의가 강요되는 등 불합리한 관행 지속

- 본인이 잘 모르는 수백개의 제휴사 등(제3자)에 신상정보가 제공되어 스팸광고 노출 위험 및 유출시 피해규모 예상도 어려움

③ (권리보장 미흡) 정보의 과도한 수집 및 포괄적 동의의 강요 등으로 정보주체의 개인정보 제공에 대한 ‘자기정보 결정권’이 실질적으로 보장되지 못하고 있음

- 또한, 본인의 정보 이용·제공 상황을 잘 알지 못하거나 알기 어렵고, 정보보호를 요청할 규정 및 절차가 미비한 상황

④ (불법정보 수요) 대출모집인 등*이 “무차별적” 모집·권유
영업하는 과정에서, 불법정보의 수요처로 작용

* 대출모집인, 대부중개업자, 보험설계사, 카드모집인 등

- “무차별적” 영업으로 인한 과도한 문자 발송 등으로 금융
이용자의 불편 초래 등 부작용
- 이러한 대출모집인 등을 활용해 금융회사는 “고객 모집”
이라는 편익을 받음에도, 이들에 대한 관리책임은 부족

⑤ (내부통제 부실) 이사회, CEO 등 주요 의사결정자에 대해 정보
보호 현황에 대해 충분한 보고가 이루어지지 않고, 관심이 부족

- 금융회사의 영업중시 관행으로 고객정보관리에 소홀하고,
보안규정도 준수하지 않는 등 내부통제가 미흡
- 그 동안 정보유출 사고 발생시에도 형식적 규정 준수로
면책이 되면서 정보보호와 관련한 주의가 부족

⑥ (불충분한 제재) 정보유출시 금융회사 등에 대한 제재 수준이
미미하여 재발방지 효과가 미흡

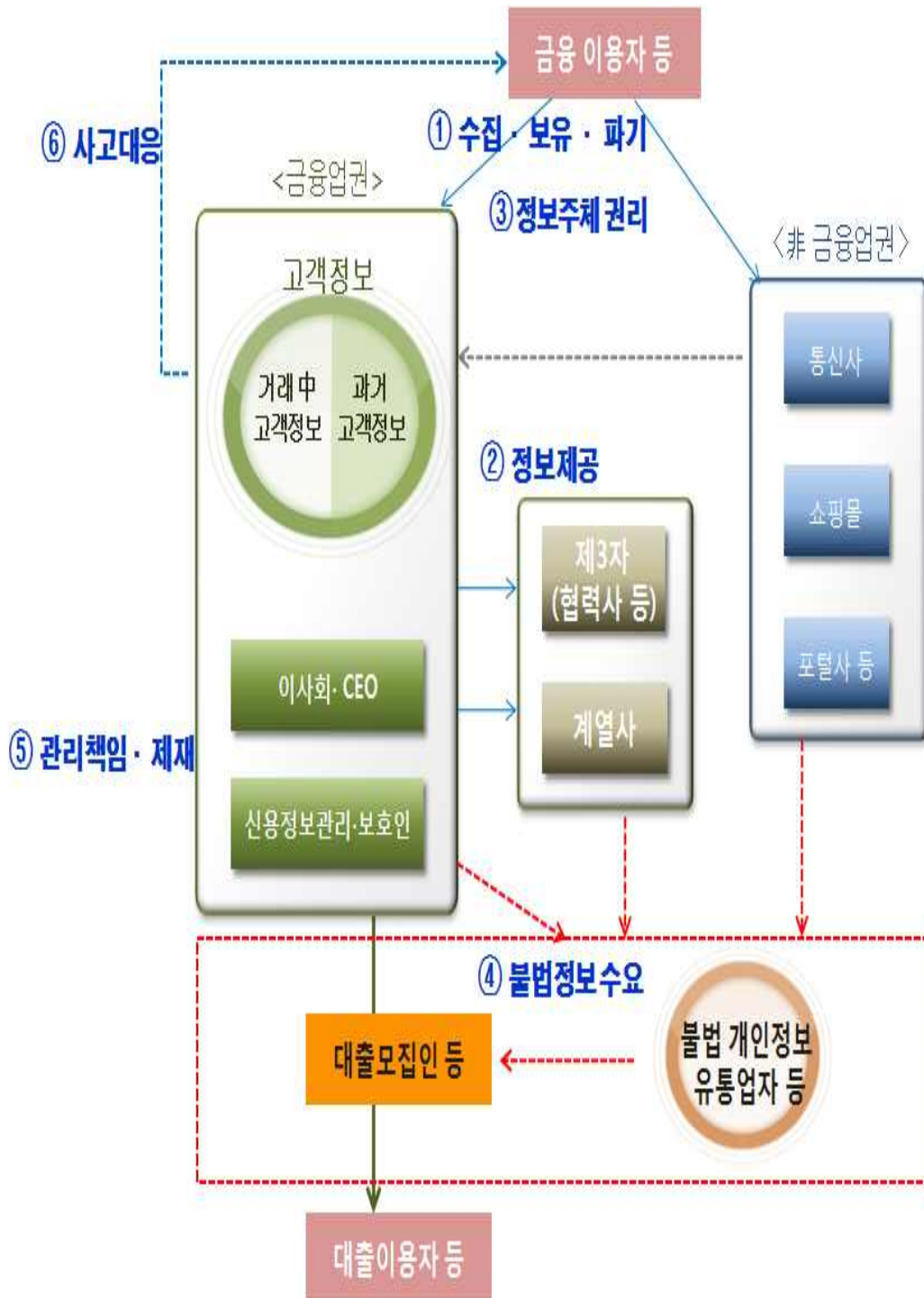
정보유출시	과태료	형벌	과징금
신용정보법	1천만원 이하	5년 이하 징역	없음
개인정보법	3천만원 이하	5천만원 이하 벌금	5억원 이하

- 금융회사가 정보를 유출하거나 불법정보를 활용하는 경우에도
충분한 금전적·형사적 제재 미부과*로 정보관리가 허술

* 그간 개인정보 유출시 해당 금융기관에 대해 낮은 수준의 과태료(최고
600만원) 부과 및 임·직원에게 대해서도 “주의” 수준의 가벼운 제재 부과

⇒ 개인정보의 수집·관리·제3자 제공·불법정보 수요·내부
통제·위반행위 제재 등 전 단계를 면밀히 살피고,

- 고객정보의 유출·불법유통 등이 재발하지 않도록 제도와
관행의 세밀한 부분까지 철저히 개선



Ⅲ. 재발방지를 위한 세부과제

〈 기 본 방 향 〉

◆ 개인정보 보호 강화 및 정보유출 재발방지를 위한 근본적인 제도개선 방안을 마련

- ① 편의성, 효율성 중시 → 금융소비자 권리 및 정보보호 강화
 - 금융거래의 편의성과 금융회사의 효율성 관점이 아닌 금융소비자의 관점에서 고객 보호 및 권리 보장을 강화
- ② 부분적·단편적인 개선 → 전면적·종합적인 개선
 - 정보의 수집, 제공, 유통, 관리 전반에서 제기되는 문제를 점검하여 개인정보 유출을 억제
- ③ 허술한 정보보안 → 강력한 전산시스템 보안체계 구축
 - 해킹 등 외부적 침입행위에 안전한 보안체계를 구축하여 신뢰있는 금융 서비스 제공
- ④ 낮은 수준의 제재 → 엄정한 제재를 통한 재발방지
 - 징벌적 과징금 도입 및 형벌, 과태료 등의 제재를 대폭 강화하여 정보의 불법유출·활용 등 유사범죄 예방
- ⑤ 형식적 가이드라인 → 중요사항 및 기본 원칙 법령 반영
 - 정보보호 및 금융소비자 권리강화 사항은 법령에 반영하여 실질적으로 구현

* 구체적인 기술적 보안방안에 있어서는 자율권을 부여하되, 유출사고 발생시에는 금융회사에 엄격한 책임을 부과

1. 정보 수집 · 보유 · 활용 · 파기 : 단계별 정보보호 강화

A. 수집 단계

가 수집정보의 필요최소화 (☞ 신용정보업감독규정 개정)

◇ 계약체결에 필수적인 정보와 선택가능한 정보를 구분하여 '필요최소한'의 정보만 수집하도록 개선

□ 현재 금융업권별 · 상품별로 30~50여개인 수집정보 항목을 필수항목(6~10개)과 선택항목으로 구분 · 최소화

○ (필수항목) 공통 필수정보*(6가지)와 금융업권 · 상품별 필수 정보(업권 · 상품별로 상이)를 구분

* 이름, 고유식별번호(주민번호 등), 주소, 연락처, 직업군, 국적

- 업권 · 상품별 특수성에 따른 필수정보*는 해당 상품을 이용하는 고객에 대해서만 별도로 수집

* (예) 재형저축 · 펀드 가입시 연소득, 질병보험 가입시 병력사항 등

○ (선택항목) 수집하는 목적과 제공처, 선택정보 제공시 혜택 등을 설명하고 고객 동의하에 수집

- 선택항목 동의는 “계약 체결에 필수적이지 않음”을 충분히 고지하고, 선택항목의 동의거부에 따른 불이익은 없도록 함

○ (금지항목) 사생활 침해 소지가 있는 결혼기념일, 종교, 배우자 및 가족 정보 등의 항목은 원칙적 수집 금지

나 주민번호 과다노출 관행 개선

◇ 주민번호 수집은 불가피하나, 수집방식·보관을 엄격히 제한하고, 유출시 엄정한 제재 부과

□ (수집) 최근의 정보유출로 주민번호 사용에 대한 우려가 있으나, 현재로서는 금융회사의 주민번호 수집·이용이 불가피*

* 주민번호는 금융부문에서 신용도 조회 등을 위해 정보를 집중하거나, 과세 기반 확보(금융소득종합과세 등)를 위해 공공부문과 연계시 유일한 식별값

○ 수집은 최소화하고, 보관은 엄격히 하되, 안행부를 중심으로 한 주민번호 대안마련 검토에도 적극 참여

□ (수집방식) 최초에만 주민번호를 수집하고, 이후에는 주민번호 기입없이 신원확인 절차만 거치도록 하여 노출을 최소화

○ 최초 거래시에는 전자 단말기 직접 입력*, 콜센터 활용 등을 통해 가급적 노출을 최소화하는 방식으로 주민번호를 수집

* 고객이 직접 인증센터와 연결된 전자단말기에 입력(Key-in)

- 다만, 법령상 규정 준수, 단체계약 체결, 보험금 지급 등의 경우 예외적으로 서식상 기입을 통해 주민번호를 수집 가능

○ 이후 거래에는 주민번호의 기입없이 신분증, 인증시스템 등을 통해 신원을 확인

- 법령상 특별한 규정이 있는 경우에만 신분증 사본 전체를 보관 가능하고, 그 외에는 사본에서 주민번호 뒷자리 삭제

□ (보관방식) 금융회사는 수집한 주민번호는 외부망은 물론 내부망에도 암호화*하여 보관·이용하여야 함

* 개인정보보호법 개정안 국회 통과('14.2월), 회사규모, 이용고객 수 등을 고려하여 단계적으로 시행될 계획

□ (책임강화) 주민번호를 불법활용 또는 유출한 경우에는 일반 개인정보 유출시보다 과태료 및 과징금 부과시 가중

B. 보유·활용 단계

가 금융지주그룹內 계열사 및 분사시 고객정보 이용 제한 등

◇ 계열사 고객정보의 외부영업 이용제한 및 내부통제절차 강화
(☞ 금융지주회사법 및 업무지침서 개정)

① 금융지주 內에서 고객의 사전동의 없이 계열사 보유정보를 제공받아 금융상품 판매 등 외부영업에 이용하는 것을 제한

* 그룹단위의 신용위험관리, 고객분석 등 내부 경영관리를 위해 필요한 경우에는 계열사간 고객정보 제공을 계속 허용

○ 제공받은 정보는 이용기간을 필요 최소한으로 제한*하고, 이용기간 도과시 영구 파기여부를 고객정보관리인이 확인

* 현재 3개월 이내로 제한 → 예: 1개월 이내로 제한

○ 지주사는 자회사의 고객정보관리에 대해 주기적인 종합점검 실시 → 시정조치사항 등을 감독당국에 보고

② 분사(分社)하는 회사의 경우, 원칙적으로 자사 고객이 아닌 개인정보는 이관받지 않도록 함 (☞ 신용정보법 개정)

* 분사에 따른 정보 이관 승인시, 개인신용정보의 범위를 더욱 엄격하게 검토하여 필수 정보만 이관되도록 할 것

○ 분사 이전 정보와 긴밀히 연계되어 있는 경우 등 불가피하게 이관받는 경우에는 자사 고객 정보와 분리하여 엄격히 관리*

* (예) 거래종료 정보에 준하여 영업목적 활용을 금지(1단계 보안조치) 하고, 5년 이내에 원칙적으로 모두 파기

나 제3자 정보제공의 구체화

◇ 제3자에 제공시, 필수/선택 사항을 구분하고 각각 동의
(☞ 가이드라인 제정 및 신용정보업감독규정 개정)

① 포괄적 정보제공 동의*를 제한하여, “계약 체결에 필수적인 제3자”와 “선택적 제3자”를 구분하여 동의를 받도록 함

* 선택적인 제공사항을 한꺼번에 제시하여, 부가서비스를 하나라도 이용하려는 경우 모든 개인정보를 모든 제3자에 제공 동의하여야 함

○ 제3자의 사업내용, 연관된 부가서비스 등을 기준으로 개별 또는 다수 그룹으로 구분하여 별도로 동의받도록 함

※ 동의하고 싶지 않은 제3자 그룹에 대해서는 이용자의 “비동의” 선택권을 실질적으로 보장하는 효과

② 제공되는 정보의 내용, 이용목적, 정보가 제공되는 업체명 및 업체 수, 제공기간 및 파기계획 등 구체적으로 적시

○ (제공목적) 제3자에 제공되는 목적 또는 혜택을 분명히 적시 하고, 이용목적에 부합하는 정보만을 한정하여 제공

○ (업체명·수) 제공되는 업체 그룹별로 업체명과 수를 명시하고, 제공되는 범위도 필요 최소한*으로 한정

* (예) 카드 모집인(0만명)(×) → 당사 소속의 카드 모집인(20명) (○)

○ (제공기간 및 파기 계획) 제3자에 제공하는 목적 등에 부합하게 “최소한의 기간”을 “구체적”으로 적시

- 파기 및 예외적 보관 등 계획도 구체적으로 안내*

* (예) 마케팅 등의 목적은 원칙적으로 1년간만 제공하고 즉시 파기
“사용 목적이 다한 경우” 등 불명확한 표현은 금지

참 고

수집·이용·조회·제공 동의서 양식 개선방안

◆ 금융회사가 최소한의 정보만을 수집하고 고객도 정보제공 내용을 명확히 인지할 수 있도록 동의서 양식을 개편

□ “필수사항”과 “선택사항”을 별도 페이지로 구분하고, 필수 사항에 동의하면 계약 체결*(서비스 제공)

* 선택사항에 동의하지 않는다고 서비스 제공이 거부되지 않도록 함

□ 제3자 정보제공의 경우 포괄적 동의를 금지, 정보제공의 대상·목적별로 그룹화하여 각각 동의받도록 함(필수/선택 제공 구분)

○ 현재 “제공목적 달성시까지” 등으로 규정된 정보보유기간을 구체적으로 명시(예: 마케팅 목적 제공시 “제공후 3개월내” 등)

수집·이용/조회/제공 동의서(현행)		필수 동의서	+	선택 동의서
수집·이용 필수+ 선택		수집·이용 필수		수집·이용 선택
조회 필수+ 선택		조회 필수		조회 선택
제공 필수+ 선택		제공 필수 (그룹1, 그룹2, 그룹3)		제공 선택 (그룹1, 그룹2, 그룹3)
현행	한 페이지에 수집·이용, 조회, 제공 동의서 한꺼번에 제시 (선택·필수정보 구분 x)			
개선	“필수사항”과 “선택사항”을 별도 페이지로 구분, 필수사항에 동의 → 계약 체결			

□ 글자 크기, 줄 간격 등을 확대*하여 읽기 쉽게 개선

* (예) 항목구분 글자 최소 12p, 본문글자 최소 10p 및 줄간격 130% 이상

개선 前	개선 後
<p>개인(신용)정보의 필수적인 수집·이용에 관한 사항(8p)</p> <p>1. 개인(신용)정보의 수집·이용 목적(7p)</p> <p>- 신용카드 이용 계약의 체결을 위한 본인 확인, 본인 신용조회, 신용카드 이용에 따른 카드대금 결제 등 계약의 체결·유지·이행·관리, 금융사고조사, 법령상 의무이행, 분쟁해결, 민원처리 등(6p)</p> <p>2. 수집·이용할 개인(신용)정보의 내용</p> <p>- 개인식별정보(성명, 주소, 주민등록번호, 성별, 국적,직업(직장명,부서,직위,주소 등), E-mail, (휴대)전화번호 등)</p> <p>- 농업 및 타금융회사와의 신용거래정보(본 동의 이전·이후의 신용, 체크, 직불, 선불카드의 카드번호, 발급 및 해지·한도, 사용금액·가맹점 구매 물품내역·카드승인번호 등의 실적을 포함한 카드 거래관련 정보 및 현금서비스, 카드론, 대출, 할부, 리스, 렌트, 채무보증현황 등)</p> <p>- 신용능력정보(재산, 채무, 소득, 납세실적 등)</p>	<p>개인(신용)정보의 필수적인 수집·이용에 관한 사항(13p)</p> <p>1. 개인(신용)정보의 수집·이용 목적(12p)</p> <p>- 신용카드 이용 계약의 체결을 위한 본인 확인, ----(중략)-----민원처리 등(10p)</p> <p>2. 수집·이용할 개인(신용)정보의 내용</p>

다 모집인 등의 불법정보 활용시 퇴출

◇ 불법정보 활용 모집인 전속계약 해지 및 5년간 재등록 제한

- ① 불법유통 정보를 활용한 대출모집인, 보험설계사 등에 대해서는 즉시 전속계약을 해지하고 재등록을 5년간 제한

- 이러한 사유로 계약이 해지된 대출모집인 등이 동일한 영업행위를 하는 것도 금지하여 사실상 영구 퇴출되는 효과

< 현행 법령상 금융상품 모집인별 재등록 금지기간 >

구 분	보험설계사	카드모집인	투자권유대행인	대부중개업자	대출모집인
재등록 금지기간	2년	2년	3년	5년	2년*

* “대출모집인 제도 모범규준”에서 규율

- ② 대출 모집인의 금지행위 위반 등에 관한 이력을 관리하는 통합관리시스템을 구축하여 모집인의 관리를 보다 체계화

라 무차별 비대면 방식의 개인정보 활용 엄격화

◇ 무차별적이고 정보의 적법성 확인이 어려운 SMS, 이메일, 전화 등을 통한 비대면 영업을 엄격하게 통제 (☞ 신용정보법 개정, 비대면 영업 통제방안 가이드라인 마련)

- ① 무차별적 문자전송(SMS)을 통한 권유·모집 등 영업행위 금지

- 마케팅 목적의 문자 수신과 관련한 별도 동의를 받거나 기존계약을 유지·관리*하는 경우는 제외

* (예) 보험계약의 보험료 미납, 연체, 실효, 해지, 만기안내 등

- ② 이메일·전화 등 비대면 영업에 대한 엄격한 통제방안 마련

- 이메일의 제목, 전화상담시 우선적으로 “소속회사, 송부인, 연락목적 및 정보획득경로” 등을 명확히 안내

마 불법정보에 기반한 범죄피해 예방 (☎ 전기통신사업법 등 개정)

◇ 대출사기, 보이스피싱, 스미싱 등 정보통신망(전화, 인터넷 등)을 통한 범죄수단을 차단하여 피해확산을 방지 도모

① (신속이용정지 제도) 불법대부광고, 금융사기 등에 이용된 전화번호를 신속히 차단하여 서민들의 금융피해 확대를 방지

※ 현재까지 「개인정보 불법유통 신고센터」(금감원)('14.2.6~)에 신고된 대포폰 등 1,137건에 대하여 경찰청에 이용정지 요청

○ 향후 범죄에 이용되거나 거짓으로 표시된 전화번호의 차단을 위한 관련법령 개정 등 추진(미래부 협조)

* 근거법인 전기통신사업법 개정안 국회통과 노력

② (전화번호 조작방지) 금융사기, 스팸 등으로 인한 피해예방을 위해 통신사업자에게 기술적·관리적 조치를 의무화

○ 통신사업자는 발신번호가 조작된 전화번호를 차단 또는 정상 번호로 전환하고 해외발신전화의 고객안내 등을 조치(미래부 협조)

* 근거법인 전기통신사업법 개정안 국회통과 노력

③ (스미싱 대응 시스템) 스미싱 의심문자를 자동 탐지하여 문자 발송을 차단하는 스미싱 피해 대응 시스템* 구축('14년 상반기 중)

* 미래부, 방통위, KISA 등 협조

④ (신입금계좌지정 서비스) 금융사기 피해를 최소화하고자 미지정 계좌로는 소액이체(1일 최대 100만원)만 허용

* 시스템 구축 및 사전홍보 등을 거쳐 '14.9월말 시행 예정

C. 파기 단계

가 필요한 기간만 엄격히 보관 후 파기 (👉 신용정보법 개정)

◇ 수집된 정보는 거래종료 후 원칙적으로 파기하도록 하고, 보관이 필요한 경우 '엄격한 보안조치'에 따라 보관

□ 정보유형별로 “체계적”인 보관 의무화

- (1단계) 거래종료 후에는 원칙적으로 필요한 정보(식별정보, 거래정보 등)만 보관하고 즉시(3개월 이내에) 파기*

* (예) 학력, 직업·직위 등의 정보

- 현재 거래중인 고객의 정보와 분리하여 보관(1단계 보안조치)

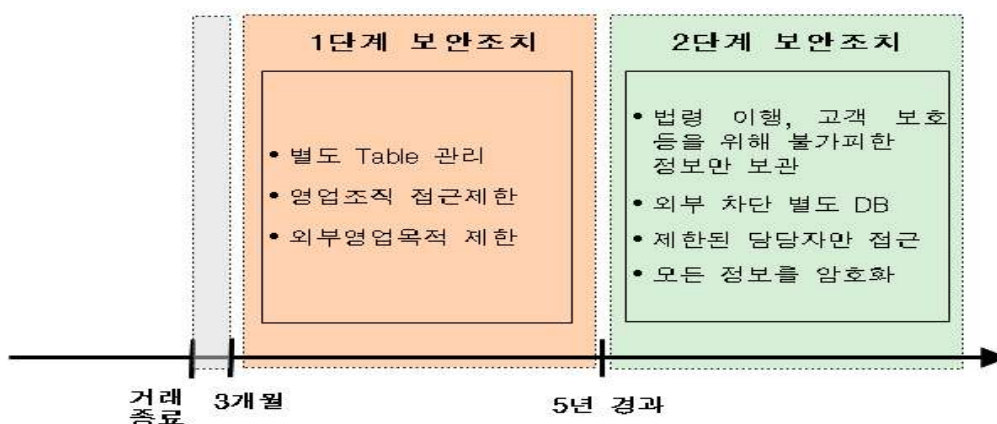
- (2단계) 거래종료 후 5년이 경과한 정보는 원칙적 모두 파기

- 다만, 법률상 의무이행 등*을 위해 보관이 불가피한 경우에는 “엄격히” 별도 관리(2단계 보안조치**)

* (예) 법령상 의무(‘자본시장법’상 투자자 계약관련 자료 10년간 보관), 상해보험 후유장애 보장을 위한 정보 등

** (예) 별도 DB 보관, 업무상 필수인원(예: 법무담당 등)만 접근가능 등

- 정보를 다시 이용하는 경우 사전통지 의무화(영업목적 사용 예방)



나 제3자에 제공된 정보통제 : 정보 파기 및 확인 의무화

◇ 제3자에 제공된 정보는 이용기간 도과시 파기하고, 금융회사는 이를 확인해야 함 (☞ 신용정보법 개정)

① 제3자가 제공받은 정보를 이용하는 “필요최소한” 기간을 설정하고, 기간 도과시 제3자는 파기 의무화

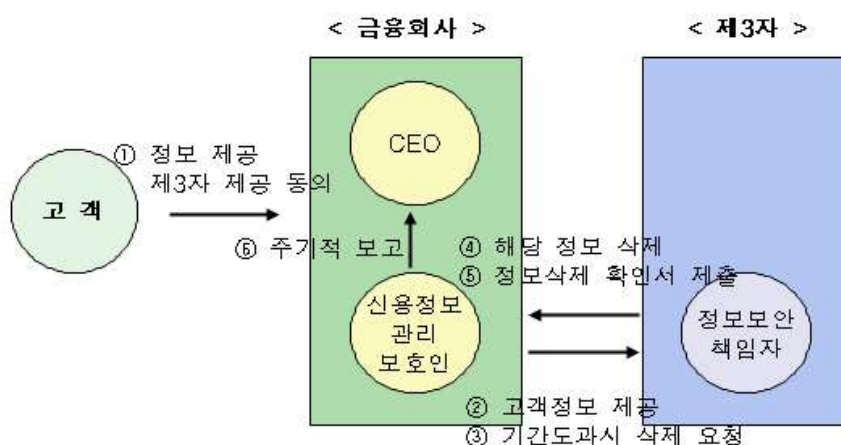
○ 금융회사는 제3자와 개인정보를 제공하는 계약 체결시, 구체적인 기간과 파기 계획을 명시하고, 불이행시 페널티(손해배상 등) 마련

② 금융회사는 제3자의 이용기간이 도과한 경우 정보를 파기하고 이를 확인해 줄 것을 요청 → 파기 확인서를 받도록 함

③ 금융회사는 제3자 제공정보 관리실태를 CEO 등에 주기적으로 보고하여 철저히 관리*

* 금감원을 통해 제3자 정보 파기 요청, 확인서 징구 등 금융회사의 제3자 제공정보 관리실태 등을 정기적으로 검사

[참고] 「제3자 제공정보에 대한 관리강화」



2. 신용정보 주체의 권리 강화 : 자기정보결정권 보장

가 본인정보 이용·제공 현황 조회 요청권 (☞ 신용정보법 개정)

◇ 정보 이용·제3자 제공 현황을 언제든지 확인할 수 있도록 함

□ 고객이 본인의 신용정보가 이용·제공되고 있는 현황*을 언제든지 확인할 수 있는 체계(조회시스템)를 금융회사별로 구축

* 이용·제공주체, 목적, 날짜 등 포함

* 전화 등을 통해서도 본인인증을 거친 경우 이용제공 현황을 안내

○ 정보제공 동의 철회권도 행사할 수 있도록 보장

나 연락중지 청구권

◇ 금융회사의 영업목적 연락(전화 등)을 중지할 것을 요청

□ 금융회사의 영업목적 연락(전화 등)에 대해 고객이 수신거부 의사(Do not call)를 밝힐 수 있는 체계를 구축

○ 금융권 협회 등에 수신거부 의사를 밝히면(통합 인터넷 사이트 등) 해당 금융회사로부터 영업목적 연락을 전면 차단

다 정보 보호 요청권 (☞ 신용정보법 개정)

◇ 금융회사가 보유한 본인 정보의 파기 및 보안조치 요구

□ 고객이 거래종료 이후 본인정보를 보호할 것을 요청할 경우, 금융회사는 파기 및 보안조치*를 취하고 그 결과를 즉시 통보

* 원칙적으로 모든 정보를 파기, 법령상 보존의무 등이 있는 경우는 2단계 보안조치(예 : 별도 DB 보관, 업무상 필수인원만 접근기능)를 통해 엄격히 관리

라 본인정보 조회중지 요청권 (☞ 신용정보법 개정)

◇ 명의도용이 의심되는 경우 일정시간 신용조회를 차단하여, 신용상의 불이익과 피해 및 사고를 예방

□ 개인 신용정보의 무단도용 등에 따른 피해(대출사기, 카드 무단 발급 등)를 예방할 수 있는 시스템을 구축

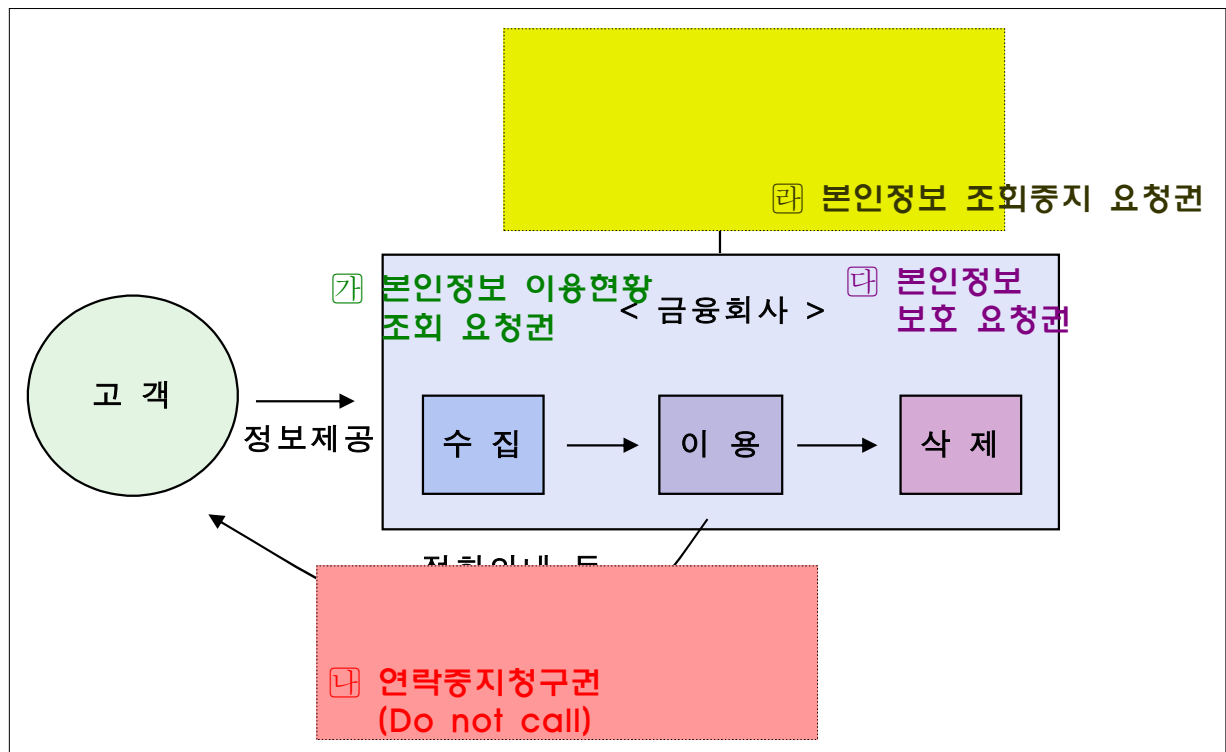
○ 고객 요청이 있는 경우*, 명의도용 의심되는 신용조회** 발생시 일정시간 조회를 중지(예 : 1일간)하고 고객에 “지체없이 통지”

* 금융회사 또는 신용정보회사(KCB, NICE 등)에 신청 가능

** 금융회사는 대출 또는 카드 발급시 개인 신용정보를 조회

○ 고객은 해당 사실을 확인하여 불법 유출정보를 악용한 제3자 대출 및 카드발급 시도 등을 차단

※ 정보유출에 따른 명의도용 의심시에는 유출한 금융회사에서 비용 부담



3. 금융회사 책임 강화 : 임원책임 확대 및 엄정한 제재

가 지속적 점검 및 평가 (☞ 신용정보법 개정)

◇ 금융회사 정보관리 현황의 동태적 점검을 통한 체계적 관리

- 1 금융회사는 신용정보 관리·보호, 내부통제 현황 및 정보보호 관련 정책 등을 담은 “연차보고서”^{*}를 작성하여 자체 점검

* 신용정보 수집·이용·제공·관리 등 제반 사항 포괄

- 2 “연차보고서”는 CEO·이사회 등의 보고를 거쳐 공개하고, 금융당국에도 제출하여, CEO 등의 책임을 강화

나 임원 책임 확대

◇ 정보보호·전산보안 관련 책임자의 권한과 책임을 대폭 강화

- 1 신용정보 관리·보호인의 책임과 권한 강화 (☞ 신용정보법 개정)

- 금융회사 등^{*}의 신용정보 관리·보호인을 “임원”으로 선임

* 신용조회회사·신용정보집중기관, 일정규모(자산 2조원 등) 이상 금융회사

- 신용정보 관리·보호인의 업무 범위를 명확화

- 정보이용·제공·보호관련 책임, 임직원·전속 모집인 등 정보보호 교육 및 보안규정 준수 점검 등

- 또한, 정보보호 현황 및 정책을 매년 작성(연차보고서)하여 CEO 및 이사회에 보고하고 감독당국(금융위)에 제출

- 2 정보보호최고책임자(CISO^{*})의 책임성 강화 (☞ 전자금융거래법 개정)

* Chief Information Security Officer : 금융 IT부문의 보안에 대한 책임자

- 정보보호 최고책임자(CISO)는 정보효율성을 강조하는 업무와의 상충 방지 등을 위해 타 IT관련 직위와의 겸직을 제한^{*}

* (예) 총자산 10조원 이상이고 종업원수 1,500명이상 금융회사

다 모집업무 위탁(대출모집인 등) 관련 관리강화(☞ 신용정보법 개정)

◇ 금융회사 모집인 등의 정보 수집·활용에 대한 철저한 관리

1 금융회사가 모집인을 통해 영업하는 경우, 정보의 제공·활용·파기 단계별로 내부통제 방안을 마련

- 금융회사가 모집인에 정보를 제공하는 경우, 최소한의 정보(이름, 전화번호 등)만을 암호화하여 제공

- 제공된 정보는 업무목적 외 사용을 금지하고, 모집인은 “정보 활용·파기 관리대장”을 작성 → 금융회사 주기적 점검

- 금융회사는 모집인*의 계약 승인시 “모집경로를 확인”하여 적법정보를 활용했는지 확인

* 대출모집인 외에 보험·카드모집인, 대부중개업자 등에도 확대 적용

- 모집인은 계약체결 등 모집행위 완료시 관련정보를 즉시 파기

2 정보유출·불법정보 활용시 모집인뿐만 아니라 금융회사에도 엄정한 책임*(과징금 부과)을 추궁

* 과징금, 형벌(3년 이하 징역, 3천만원 이하 벌금), 과태료(1천만원 이하)

- 다만, 정보제공 절차 준수, 교육 실시, 모집경로 철저 확인 등 주의의무를 다한 경우에는 금융회사는 면책

라 징벌적 과징금 제도 도입 (☞ 신용정보법 개정)

◇ 개인정보 유출·활용한 금융회사에 “징벌적 과징금” 부과

- 개인정보를 유출·불법활용한 금융회사에 대해서는 사회적 파장 등을 감안하여 대폭 상향된 “징벌적 과징금” 신설

- (부과대상) 불법 개인정보 활용(마케팅 등 영업), 관리소홀 등으로 인한 정보 유출(분실·도난 등) 등의 경우

○ (부과기준) 위반행위·불법정보 등에 영향을 받은 “관련 매출액(영업수익)”에 고의·과실 정도에 따라 기준금액을 산정

- 해당 기준금액에 ①위반행위의 기간 ②위반횟수 ③유출정보 건수 ④시장에 미치는 영향 등을 감안하여 가중·감경(예 : ±50%)

○ (부과한도) 매출액 일정비율 및 금액의 상한 설정 검토

① “불법정보 활용시” 에는 “관련 매출액의 일정비율(예 : 3%)”을 상한으로 설정(※금액은 사실상 무제한),

② 관리소홀 등으로 “정보를 유출”한 경우는 “일정 금액(예 : 50억원*)”을 상한*으로 설정

* 정보유출시 과징금 상한 : (정보통신망법) 1억원 (개인정보보호법) 5억원

* 금융회사 정보유출이 타 업권 등에 비해 사회적 파급효과가 큰 점을 감안하여 “금액상한”은 타법 사례보다 높은 수준으로 설정

마 형벌 강화 (☞ 신용정보법, 전자금융거래법 개정)

◇ 개인정보 유출 관련 형벌수준 대폭 상향

□ 신용정보법, 전자금융거래법 등 관련법에서 개인정보 유출·불법활용시 형벌수준을 금융관련법 최고 수준*으로 크게 상향

* (예) 은행법(§66) : “비공개정보 누설”시 10년 이하 징역 또는 5억원 이하 벌금

○ 확대·재생산 위험이 높은 개인정보의 특성을 감안하여 정보유출·불법 활용시 위반행위 당사자에 대한 처벌을 강화

< 개인정보 유출 관련 법령상 형량 수준 >

구분	신용정보법(안)	전자금융거래법(안)	개인정보보호법
적용대상	신용정보제공·이용자 (은행, 카드 등)	전자금융거래정보 처리자	모든 개인정보처리자
정보유출자 형량	10년 이하 징역 또는 1억원 이하 벌금	10년 이하 징역 또는 1억원 이하 벌금	5년 이하 징역 또는 5천만원 이하 벌금

바 과태료 강화 (☞ 신용정보법, 전자금융거래법 개정)

◇ 정보유출방지 주의의무 위반시 과태료 수준 대폭 강화

□ 정보유출이 일어나지 않더라도 금융회사가 보안대책 미비 등 주의의무를 다하지 않을 경우 과태료수준 대폭 강화

- * (신용정보법) i) 정보유출방지를 위한 보안장치 미비 : 600만원 → 5천만원,
ii) 신용정보관리인이 CEO에 정보보호관련 보고의무 해태 : 5천만원(신설),
iii) 식별정보 암호화 조치 미비·정보폐기 의무 위반 : 3천만원(신설)
- ** (전자금융거래법) 안전성 확보의무 위반 : 5천만원(신설)

○ 사전에 정보유출방지를 위한 주의의무를 다하지 않은 과실 등에 대한 책임을 물어 사고 예방효과를 높일 필요

사 행정제재 (☞ 신용정보법, 여전법 등 개정)

◇ 개별금융사에 대한 영업정지 수준 상향 등 기관제재 강화

□ 금융회사 임·직원에 대한 제재, 영업정지 등 기관제재도 보다 엄격히 이루어지도록 개선

○ (CEO 등 임원) 신용정보 관리·보호인 및 CEO에게 신용정보 보호와 관련한 의무를 부여하고, 이에 상응하는 제재*를 부과

* 신용정보 관리·보호인이 CEO에 주기적인 실태 보고 → 이에 따라 적정한 조치를 취하지 않은 경우 CEO에게 행위자 책임 부과

○ (신용정보회사) 임·직원의 위탁 업무 수행에 대한 엄격한 관리기준을 도입하고 위반시 기관 제재

- 불법정보 유출 관련시 영업정지(6개월 이내) 또는 이에 갈음한 과징금을 부과하고 3년내 재위반시 허가취소

○ (개별 금융사) 금융업권별 법령 개정을 통해 금융회사에 대한 기관제재도 강화(예 : 카드사 영업정지 3 → 6개월)

- 상시점검 미흡으로 사고인지를 못했거나, 사고 발생을 고의적으로 숨긴 경우 가중하여 엄정 제재

4. 정보보호·보안 : 금융권 사이버 안전 대책 강화

가 내부통제 강화

◇ 정보보안 관련 내부규정을 구체화하고, 주기적 점검 강화

- 금융회사 내부 보안규정의 수준 제고를 위해 감독당국이 금융협회와 공동으로 “금융전산 보안 표준지침(Best Practice)*”을 마련

* 보안관련 법규정, 업무별·직급별 정보접근 범위 등을 구체적으로 반영

- 금융회사별 “보안점검의 날”을 지정하여 CISO 책임하에 매월 보안점검*을 실시하고, CEO에게 점검결과 및 보완계획을 보고

* 필수 보안규정이 누락되지 않도록 ‘금융보안 표준 체크리스트’를 마련

- 금감원은 금융회사의 점검결과를 제출받아 검사에 활용하고, 보안점검 미이행시 엄중 제재 (☞ 전자금융감독규정 및 시행세칙 개정)

나 외주업체 통제 강화

◇ 외주용역 통제 규정의 준수를 담보하기 위한 시스템 구축
(☞ 전자금융감독규정 및 시행세칙 개정)

- 금융회사 외주용역의 입찰→계약→수행→완료 등 쏘 단계*에 걸쳐 세부적인 절차와 기준을 마련하여 보안관리체계를 개선

* ‘국가정보보안 기본지침’의 단계별 보안관리 체계를 참조하여 규정에 반영

- 외주용역 관련 핵심 보안점검사항은 일일점검 실시*

* ‘외주용역 일일 체크리스트’를 감독규정시행세칙에 반영

- 외주 개발업무는 장소적으로 분리하고, 개발시스템은 운영시스템과 분리하는 등 물리적 통제를 명확화

다 전산시스템 해킹방지 대책 강화

◇ ICT 발전에 따라 고도화되는 해킹 등 전자적 침해에 대응할 수 있는 강력한 전산시스템 보안체계 구축

① 해킹 등으로 인한 정보 유출·파괴에 대한 방어체계 대폭 강화

- 고객정보의 해킹 등에 대비하여 금융회사 내부망의 고객정보 DB에 저장된 고유식별정보의 암호화 추진(☞ 개인정보보호법령 개정)

* 암호화 추진절차(안) (안전행정부 협조)

- ① 회사규모, 이용고객 수 등 감안하여 적용대상, 추진일정 등 주요 요건은 개인정보보호법 시행령에 반영
- ② 금융회사는 금융위 주관하에 암호화 추진계획 마련(재투자시기 감안)
→ 매년 이행실적 점검(기한내 철저 이행 확보)

- 해킹에 대한 근본대책인 망분리 추진계획*을 금감원이 정기 점검하여, 미이행시 해당기관 및 책임자에 대해 제재

* 전산센터는 '14년말, 은행의 본점·영업점은 '15년말, 비은행은 '16년말 완료(망분리란 내부망(업무망)과 외부망(인터넷망)을 분리·운영하는 것임)

- 금융전산 보안관제* 범위를 은행·증권에서 보험·카드까지, 금융거래시스템 외에도 교육·홍보용 홈페이지 등까지 확대(☞ 전자금융거래법 개정)

* 보안관제는 금융회사 전산망에 대해 해킹 등 전자적 침해 여부를 모니터링 하는 서비스로서 현재 금융결제원과 코스콤이 수행중임

- 정부·유관기관의 전자적 침해사고 접수창구를 일원화*하고, 해킹 등 전자적 침해위협 정보의 기관 상호간 공유체계 강화(☞ 전자금융감독규정 개정)

* 금융위·금감원, 금융ISAC → 금감원 또는 “금융보안 전담기구”로 일원화

② 금융회사의 전산보안 관리수준을 대폭 제고(☞ 전자금융법규 개정)

- 객관적인 평가기관*이 금융전산의 보안관리 수준을 평가하는 “금융전산 보안인증제”를 도입·확대하고, 인증통과 여부를 공개

* (예시) 한국인터넷진흥원, 금융보안 전담기구 등

- 금감원은 인증결과를 IT부문 실태평가에 반영

※ 금융전산 보안인증제와 보안등급제 추진 관련 고려사항

- “금융전산 보안인증제” 추진시 기존 인증제와의 연계방안, 평가기관의 수급 상황 등을 감안하여 일정규모 이상 금융회사부터 순차적으로 추진할 필요(관계기관 협의)
- “금융전산 보안등급제”는 보안인증제의 경험을 축적하여 도입 검토

- 금융결제원의 금융공동망 등 금융공공기관의 주요시스템을 ‘주요정보통신기반시설’로 추가 지정하여 체계적 보안관리 실시

* 정보통신기반보호법에 의거 지정되며, 취약점 분석 등의 보안관리 대상

③ 금융회사 정보화사업에 대한 보안대책 강화

- 금융회사 IT사업에 대한 금감원의 보안성심의* 대상을 확대하고, 심의대상이 아닌 경우 자체 보안성심의 결과를 제출
(☞ 전자금융감독규정 개정)

* 금감원이 금융회사 정보화사업에 대하여 계획수립단계에서 전산시스템의 보안대책을 사전에 점검함으로써 보안사고를 예방하기 위한 제도

- 금융회사 모바일 어플리케이션을 보안 취약점 점검 대상에 포함시켜 모바일뱅킹의 안전성을 강화

(☞ 전자금융감독규정시행세칙, 모바일 앱 보안 가이드라인 배포)

라 금융회사 보안 이행실태 점검 강화

◇ 금감원 등 외부기관을 통한 금융회사의 보안 이행실태 점검 강화

□ 불시점검, 기획검사 등으로 검사효과의 극대화 및 실효성 제고
(☞ 금감원 검사계획에 반영)

- 금융회사의 보안규정 실천이 상시 준수되도록 금감원 주도*로 전산보안 “불시점검”을 수시로 실시

* 금감원 중심으로 인터넷진흥원, 금융보안 전담기구 등으로 “기동점검반” 구성

- 금감원의 검사 및 금융회사의 “월별 보안점검”의 분석결과를 토대로 전반적 미흡사항에 대해서는 기획·테마검사 실시

□ 금감원 감독·검사의 사각지대를 해소함으로써 금융회사의 보안불감증을 근절

- 원칙적으로 모든 금융회사에 대하여 일정 검사주기 내에 IT부분 점검을 할 수 있도록 검사계획을 수립

(☞ 금감원 검사계획에 반영)

* 금융회사의 규모, 업종, 보안취약점, 보유 고객정보수 등을 고려하여 차등 적용

- IT부분 검사시 법규정의 모든 안전성 기준이 빠짐없이 검사항목에 반영되도록 하여 검사의 실효성 확보

(☞ 금감원의 IT검사 매뉴얼 개정)

마 금융전산 보안전담기구 설치

◇ 금융전산 보안 관련 종합서비스를 제공하는 전담기구 설치

- 금융결제원 및 코스콤의 보안관제조직(ISAC)을 분리하고, 이를 금융보안연구원과 통합하는 방식으로 “금융전산 보안전담기구” 설치(‘15년 출범목표)



- 보안전담기구는 금융전산 보안관제 실시, 보안인증제 운영, 보안정책 연구·교육, 보안전문인력 양성* 등 종합서비스 제공

* 전문인력을 확보하여 모의해킹을 실시하는 방안도 검토

- 인터넷진흥원, 경찰청 사이버테러대응센터 등 보안유관기관과 공조체계를 강화하여 국가 전반의 사이버 보안수준을 제고

바 금융권 IT인력의 전문성 제고 및 보안인력 양성

- 현재 일부 대학원에서 개설하고 있는 정보보호관련 교육 과정 개설을 확대* (관계부처 협조)

* (2011년) 22개 대학원 → (2012년) 25개 대학원(260명 배출, 8% 증가)

- 금융연수원 및 금융보안연구원에 정보보호 과목을 개설하고 국내 대학(원) 보안관련학과 등에 대한 위탁교육 확대 유도

사 신용카드 결제시 안정성 강화

◇ 카드가맹점 단말기를 MS단말기에서 IC단말기*로 조속히 전환** 하고 사용을 활성화함으로써 카드결제과정에서 개인정보보호 강화

* IC(integrated circuit): MS(magnetic strip)에 비해 처리용량이 커 정보의 암호화 등이 가능

** 전체 전환대상(약 220만대)의 절반 수준인 약 110만대(POS단말기 34만대 포함)

<IC단말기로 전환 유도>

□ 정보유출 위험성이 상대적으로 높은 POS*단말기를 많이 사용하고 있는 일반·대형가맹점에 대해 '14.12월까지 IC단말기 先전환 유도

* POS(Point of Sale): 매출내역 및 고객관리 등을 위해 가맹점 단말기에 카드결제승인 관련 정보도 저장

□ 매출규모가 작고 단말기 교체비용 부담이 큰 '영세가맹점'의 경우, 사회공헌기금, 소멸포인트 등으로 (가칭) 「IC단말기 전환기금」을 조성하여 단말기 교체 지원

□ 카드사는 가맹점 신규계약 체결시 IC단말기 설치여부 확인

< IC단말기 사용 활성화 >

□ 가맹점이 신용카드 주요정보(카드번호, 유효기간 등) 암호화 등 보안 수준을 충족한 단말기를 사용토록 적극 유도함으로써 실효성 확보

○ '14.하반기중 IC결제 우선 승인제* 실시(☞ 가맹점표준약관 개정)

* IC결제 승인시간을 MS결제 승인시간보다 덜 걸리게 하거나, 가맹점이 IC 결제가능 단말기에서 MS 결제승인 요청시 '최초' 1회는 승인 거절

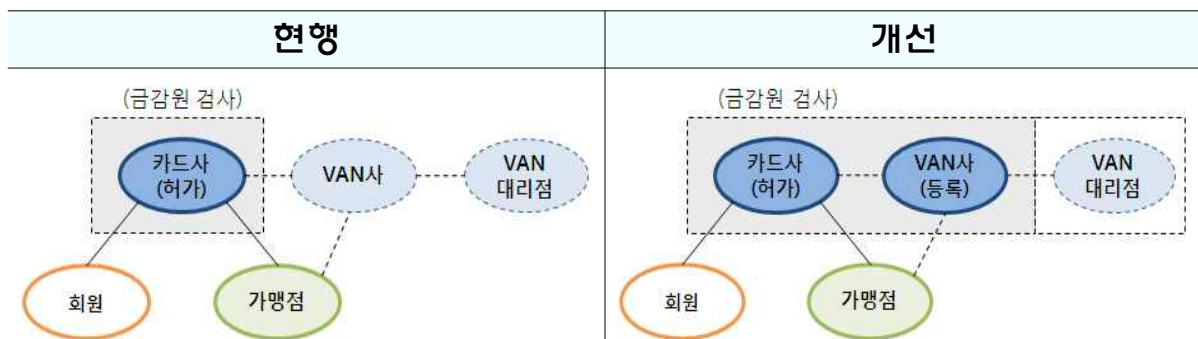
○ 또한, 가맹점의 IC결제시 가맹점수수료인하 등 인센티브 제공을 통해 IC결제 적극 유도

□ '15년부터는 IC단말기 설치 가맹점에서의 IC결제를, '16년부터는 **소 가맹점에서 IC결제를 의무화**(MS카드를 통한 결제는 중단)(☞ 여전법 개정)

아 VAN사에 대한 관리·감독 강화

◇ 신용카드 결제 승인·중계업자(VAN: Value Added Network)에 대한 체계적인 관리를 통해 감독의 사각지대 해소

- 카드사가 수탁자인 VAN사의 회원거래정보·관리실태에 대해 자체점검을 실시하는 등 자정기능 강화
- VAN사를 「여신전문금융업법」상 등록제로 운용(여전법 개정)
 - VAN사는 일정한 자격요건(자본금, 전산설비 등)을 갖추어 등록
- VAN사에 대해서 결제의 IT안전성 확보, 신용정보 보호, VAN 대리점 관리 의무 등을 부여
 - 금융회사에 적용되는 IT안전성 기준을 VAN사에도 적용
 - 결제업무에 필요하지 않은 개인정보 수집·보유는 엄격히 제한하고, 카드번호, CVC값 등 주요 정보는 암호화처리
- VAN사의 법령준수 여부에 대한 관리·감독 강화
 - 금감원은 VAN사의 법령 준수 여부를 수시로 점검하고, VAN사 검사 과정에서 VAN대리점 관리실태 등도 확인
 - VAN사의 법 위반 사실에 대해서는 과징금, 등록취소 등 중징계가 가능하도록 제재장치 마련



5. 예방조치 강화 : 기존정보 처리 및 대응체계 구축

가 기존 정보로 인한 피해 가능성 차단

① 금융회사 개인정보 보유현황 점검 및 파기

- 금융회사별 정보보유 현황에 대한 자체점검 및 타당성 평가 (‘14.2월~)를 토대로 “꼭 필요한 정보”외에는 모두 파기토록 추진

* 계약유지에 필수적인 정보, 다른 법률상 의무이행에 필요한 정보 등

- 또한, 보유기간이 5년 경과한 정보 등도 원칙적 파기

- 금융당국은 금융회사별 자체점검 작업의 이행실태 등을 점검
- 이번 점검 이후에 불필요한 정보를 보유하다 불법활용 또는 유출된 경우에는 엄중 제재할 방침

② 제3자 및 계열사 제공 개인정보 점검 및 파기

- 금융회사는 제3자 및 계열사에 대해 제공 정보에 대한 관리·보관 실태를 자체적으로 점검하도록 요청

- 제공 정보의 적정성 및 활용기간 도과 여부 등을 검토하여 불필요한 정보는 파기하도록 하고, 금융회사는 이를 확인

- 금융회사는 제3자 등의 정보관리가 미흡할 경우, 재계약 금지 등의 조치를 취해야 함

③ 고객이 개인정보 유출로 인한 피해를 우려하여 요청하는 경우, 카드 교체 등을 신속히 할 수 있도록 지원하는 방안 등을 마련

④ 기존의 불법 유통 정보에 대해서도 검·경 등 합동 단속을 무기한 실시하여 개인정보 유통업자 등을 근절

나 신속한 대응체계 구축

① 정보유출 사고 '대응매뉴얼' 마련 의무화 (☞ 신용정보업 감독규정 개정)

- 사고발생시 신속하고 세밀한 대응을 위해 금융회사별로 CEO 책임하에 대응매뉴얼*(Contingency Plan) 마련

* 통지·조회절차, 영업점·인터넷회선 확충 등 고객민원 대응 조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등 포함

- 금융회사의 대응매뉴얼 구비 여부, 실행가능성 등 점검(금감원)

② 대응시스템 구축 및 즉시 가동

- 해당 금융회사는 사고 발생(인지) 시점 즉시 자체 비상 대응 체계 및 보고체계 가동
- 금융당국은 사고 규모, 파급효과 등을 신속히 파악하여, 필요시 금감원 현장검사반을 즉각 투입하고 관계기관 합동 대응체계 가동

③ 소비자 피해확산 방지대책을 전방위적으로 시행

- 정보유출 사고 발생시 해당 금융회사는 고객들에게 유출사실, 고객 대응요령(Q&A) 등을 신속 통지
- 소비자 불편을 최소화하고, 불안감을 해소할 수 있는 조치 시행
 - 정보유출 발생시 국민 불안감을 악용한 금융사기 시도 증가에 대비하여 관계부처 합동으로 집중단속 시행

④ 정보유출 피해 구제절차 마련

- 금융회사의 정보유출로 인한 피해자의 금전적 손해에 대해서는 금감원 분쟁조정 절차 등을 통해 적극 구제 추진

※ 국회에서 제기된 징벌적 손해배상, 배상명령제도 등에 대해서는 소비자 피해자 구제 필요성과 기존법 체계 등을 고려하여 관계부처 논의 추진 → 4월 국회에서 입법 논의

* 현재 범정부 TF를 운영, 소비자 피해 구제방안을 다각적 검토중

1. [사고 인지] 사고대응 시스템 구축 및 즉시 가동

- ☐ (금융회사) 사고대응 전담부서 운영 등 대응매뉴얼 시행
 - 인지 즉시 자체 비상대응 체계 및 금융당국 보고체계 가동
 - 고객 통지대상, 범위, 절차 및 통지문구·고객 대응요령 등 마련
 - 향후 고객들의 현장방문, 전화문의, 인터넷 접속 등이 일시에 집중될 것에 대비하여 고객 불편 최소화 조치 사전 준비*

* 콜센터·통신회선·인터넷 서버 확충, 현장인력 증원, 공카드 물량확보 등

- ☐ (금융당국) 현장감독관 파견(금감원) 등 정확한 사실관계 파악 및 사고규모, 파급효과 등을 감안, 관계기관 합동 대응체계 가동

2. [고객 통보] 신속하고 안전하게 고객에게 통보

- ☐ (금융회사) 정보유출 사고 내역을 고객에게 신속·안전하게 통보
 - * 홈페이지에 정보유출 조회시스템 가동 및 이메일·우편발송 등을 통해 고객에게 개별 통지
 - 24시간 비상 대응센터 가동 및 고객대응요령(Q&A) 전파

- ☐ (금융당국) 고객통지 및 대응요령 전파 적정성 등 중점 점검·지도

※ (고객) 본인 정보유출 내역 확인, 대응요령 숙지 및 정보 유출 의심사례는 금융회사·금융당국에 즉각 문의·신고

3. [고객민원 대응] 고객 불편 최소화 대책 시행

- ☐ (금융회사) 민원처리 과정에서 점포혼잡 등 국민불편 최소화
 - 영업시간 연장(야간·휴일 연장근무), 후선인력의 영업점 투입 확대 등 점포혼잡 최소화
 - 콜센터 직원 확대투입, 통신·인터넷회선 확충 등 대기시간 단축
 - 카드 재발급 기일 단축 등 추가발급 시스템 가동

- (금융당국) 창구 동향, 고객불만·피해사항, 특이사항 등을 실시간 점검, 상황별로 적절한 대응조치 마련·지도

* 미래부, 안행부 등 관계부처와 유기적 협조체계 구축

※ (고객) 지속적으로 카드결제 내역 등 확인, 금융회사·당국의 통지내용 숙지 등 주의노력 지속

4. [고객불안 대응] 고객 안심조치 즉시 시행

- (금융회사) 고객 신청이 있는 경우 카드 등 즉시 교체(무료)

* 다만, 중요 카드정보가 유통된 경우 거래신뢰성 확보를 위해 전면 재발급도 검토

- 부정사용에 대비 결제내역 확인 문자(SMS) 서비스 제공(무료)
- 간편결제 등이 가능한 취약한 결제방식*에 대해서는 ARS 등 본인확인 절차를 추가하여 부정사용 가능성 차단

* 해외홈쇼핑, 학습지 등 일부 가맹점의 경우 카드번호, 유효기간으로 결제 가능

- 명의도용 방지를 위한 개인정보 보호시스템 제공(무료)

- (금융당국) 고객 불안감을 악용한 금융사기 시도 증가에 대비 관계부처 합동 집중단속 시행 및 대응시스템 가동

- 보이스피싱, 스미싱 등 사기 및 범죄에 이용된 전화번호 신속 차단
- 전자금융사기 예방서비스 확대(예: 본인인증추가 한도 300→100만원)

※ (고객) 금융회사에 결제내역 확인 문자서비스 신청, 부정사용 의심이 드는 카드의 신고 및 교체

5. [피해 구제] 피해발생시 구제절차 신속 진행

- (금융회사) 부정사용 등의 피해에 대해 신속하게 전액 보상

- (금융당국) 정보유출로 인한 피해자의 금전적 손해에 대해 적극 구제 추진(예: 금감원 분쟁조정 절차 등)

※ (고객) 피해 발생시 금융회사, 금융당국에 즉시 신고·보상 요청

IV. 향후 계획

① 법 개정이 필요하지 않은 대책은 최대한 조속히 시행될 수 있도록 조치

○ 금융회사의 기존 보유 정보중 불필요한 정보는 즉시 파기*

* 상반기 중 금융회사별로 자체 파기하고 신용정보관리보호인을 통해 파기 현황을 자체점검 → 4분기중 금감원 이행점검

○ 비대면 영업 통제방안 가이드라인은 3월중 확정, 4월 시행

○ 이번 대책을 위해 추진할 계획인 각종 시스템 구축은 상반기 중 세부 구축방안을 확정하고 7월부터 단계적 시행

* 정보 이용·제공 현황 조회 시스템, Do-not-Call시스템 등

○ 업권별 상품 가입신청서 및 개인정보 제공 동의서 양식 개편 방안을 확정(상반기중)하고 4분기중 시행

② 신용정보법·전자금융거래법 등의 법률개정안(국회 계류중)은 적극적 국회 설득 등을 통해 상반기중 국회 통과 추진

* 피해자 권리구제 강화를 위한 방안 등도 국회에서 논의예정

○ 또한, 현행 신용정보 집중 및 공유체계의 공공성을 강화 하는 방안* 등을 4월 국회에서 논의할 수 있도록 준비

* 신용정보집중기관의 형태·역할 재정립, 신용정보회사 정보보호 강화를 위한 통제장치 마련 등

③ 향후 「금융회사 고객정보보호 정상화 T/F」를 통해 금번 대책의 이행상황을 점검하는 등 차질없이 추진

○ 검·경 등 개인정보의 불법 수집·유통 집중단속에 적극 협조

○ 지속적인 의견 수렴 및 현장점검을 통해 추가 개선방안 검토

참고

「개인정보유출 재발방지 종합대책」 추진 일정(案)

과제 내용	담당	'14.4	'14.6	'14.9	14말
-------	----	-------	-------	-------	-----

1. 수집·보유·활용·파기 단계

A. 수집 단계

가. 수집정보 필요 최소화 · 필수·선택 항목으로 구분	금감원 금융 협회				
나. 주민번호 과다노출관행 개선 · 모범기준 마련	금감원				
· 전산설비 개선 등	금융 회사				

B. 보유·활용 단계

가. ① 계열사 고객정보 이용제한 금융지주회사법 개정	금융위				
② 분사시 고객정보 이관 금지 신용정보법 개정	금융위				
나. 제3자 정보제공 구체화 · 가이드라인, 동의서 양식 개편	금융위 금감원				
다. ① 모집인 등의 불법정보 활용시 퇴출 보험업법, 여전법 등 개정	금융위 금감원				
② 대출모집인 통합관리시스템 구축	은행 연합회				
라. ① 문자를 통한 권유·모집행위 금지 신용정보법 개정	금융위				
② 비대면 영업 가이드라인 마련 대출 모집경로 확인 등	금감원 금융 회사				
마. ② 스미싱 피해 대응시스템 구축 등	미래부 등				

과제 내용	담당	'14.4	'14.6	'14.9	14말
-------	----	-------	-------	-------	-----

C. 파기 단계					
가. 필요한 기간만 엄격히 보관 신용정보법 개정	금융위				
나. 제3자에 제공된 정보 파기 확인 의무 신용정보법 개정	금융위				
2. 신용정보 주체의 권리강화					
가. 본인정보 이용·제공현황 조회 금융회사 고객정보 조회 시스템 구축	금융회사				
나. 연락중지 청구권 Do not call 시스템 구축	금융회사				
다. 본인정보 보호 요청권 신용정보법 개정	금융위				
라. 본인정보 조회 중지 요청권 CB사 정보조회 중지 시스템구축	금융회사 CB사				
3. 금융회사 책임강화					
가. ① 연차보고서 양식 마련	금감원				
② 연차보고서 제출	금융회사				
나. ① 신용정보관리보호인 책임 강화 신용정보법 개정	금융위				
② 정보보호최고책임자 책임 강화 전자금융거래법 개정	금융위				
다. ① 모집인 영업 내부 통제방안 마련	금감원				
② 금융회사 책임 부과 신용정보법 개정	금융위				

과제 내용	담당	'14.4	'14.6	'14.9	14말
라. 징벌적 과징금 제도 도입 · 신용정보법 개정	금융위				
마. 형벌 강화 · 신용정보법 · 전자금융거래법 개정	금융위				
바. 과태료 강화 · 신용정보법 · 전자금융거래법 개정	금융위				
사. 행정제재 강화 · 신용정보법 · 여전법령 등 개정	금융위				
4. 금융권 사이버 안전대책 강화					
가. 내부통제 강화 전자금융감독규정 개정	금융위				
나. 외주업체 통제 강화 전자금융감독규정 개정	금융위				
다. 전산시스템 해킹 방지 대책 암호화, 망분리 등	금융 회사				
라. 금감원 보안점검 강화 금감원 점검	금감원				
마. 금융전산보안안전담기구 설치 추진	금융위				
사. 신용카드 안정성 강화 여전법 개정	금융위				
아. VAN사에 대한 관리·감독 강화 여전법 개정	금융위				
5. 기존 정보 처리 및 사고시 대응체계 구축					
기. ① 기존 정보 적정성 점검 및 파기	금융 회사				
② 금감원 이행실태 점검	금감원				
나. 신속한 대응체계 구축, 매뉴얼 마련 신용정보업 감독규정 개정	금융위 금감원 금융 회사				

세부 Q&A

1. 필수 정보 및 선택적 제공 정보의 구체적 예시는? (p.6)

- ☐ 현재 금융업권별·상품별로 30~50여개인 수집정보 항목을 필수항목(6~10개)과 선택항목으로 구분·최소화

① 전체 금융회사 등에 공통으로 적용되는 필수 정보

	정보명	필수 정보에 해당하는 사유
1	이 름	• 사용자 구분을 위한 필수 정보
2	고유식별정보 (주민번호, 여권번호 등)	• 금융실명법, 신용정보법상 본인 확인을 위한 필수 정보
3	집(직장) 주소	• 고객 통지 등을 위한 필수 정보 • 특정금융거래보고법(제4조, 제5조의2) (사업자의 경우는 직장주소 기입 의무)
4	연락처 (집, 직장, 휴대전화 중 선택 가능)	• 고객 통지 등을 위한 필수 정보 • 특정금융거래보고법(제4조, 제5조의2)
5	직 업	• 특정금융거래보고법(제4조, 제5조의2) • 자금세탁방지법(제38조)
6	국 적	• 특정금융거래보고법(제4조, 제5조의2) • 자금세탁방지법(제38조)

② 업권 또는 상품 특성에 따른 필수 정보(예시)

업권·상품특성 등	정보명	필수 정보에 해당하는 사유
은행/주택담보대출	담보물건(주택)	• 주택담보 설정을 위한 필수정보
은행/세금우대저축	연소득	• 조특법상 세금우대를 위한 필수정보
금투/재형펀드	연소득	• 조특법상 세금우대를 위한 필수정보
보험/질병보험	병력사항	• 보험료율 산정 등을 위해 필수정보

③ 금융이용자가 선택적으로 제공할 수 있는 정보(예시)

정보명	정보를 제공하는 사유 및 혜택
재 산	• 신용도 판단시 반영 (신용평점 가점요인으로 작용 가능)
가족관계, 맞벌이 유무, 투자 동기 등	• 가족카드 등 맞춤상품 권유 • 보험료율 산정 등에 활용

2. 금융회사와 최초 거래를 개시할 경우 주민번호 제공 방법이 어떻게 달라지는지? (p.7)

□ 고객 Key-in을 통한 주민번호 제공을 원칙으로 함에 따라 대부분 금융거래 서식상 주민번호란은 불필요하게 되므로 삭제

- 다만, 법령상 규정 준수, 단체계약 체결, 보험금 지급 등의 경우 예외적으로 서식상 기입을 통해 주민번호를 수집 가능

<거래 형태별 수집방식 >

① (점포) 고객은 원칙적으로 키패드 입력(Key-in), 금융기관에 신분증 사본 제공을 통해 주민번호를 제공

- * 금융기관은 신분증 사본을 가급적 내부망에 전자형태로 보관하고, 실물형태(예: 복사용지)의 보관은 최대한 자제

② (통화) 고객은 전화 다이얼을 이용한 주민번호 Key-in을 원칙으로 하되, 음성녹취 방식 선택 가능

- * 음성으로 신원확인이 가능하므로 금융기관의 신분증 사본 보관은 원칙적 금지(단, 불가피할 경우 추후 전자형태의 신분증 사본을 내부망에 저장)

③ (모집인) 고객은 모집인의 단말기에 주민번호를 Key-in 하거나 금융회사와 통화하여 주민번호 제공

- * 신분증 사본 보관시 모집인의 단말기로 전자화(예: 촬영)하여 금융기관 내부망에 바로 전송 또는 전송 후 즉시 파기

④ (인터넷) 화면상 보안 키패드에서 Key-in하여 제공

최초 거래	대면		非대면	
	① 점포	② 모집인	③ 인터넷	④ 통화
주민번호 수집	고객 Key-in, 신분증 사본제공	모집인의 단말기에 또는 금융회사와 통화하여 고객 Key-in	공인인증서, I-PIN 등 인증시스템 등록 (주민번호+비밀번호)	고객 Key-in, 음성녹취
신분증 사본	전자형태로 내부망에 보관 → 암호화	전자형태로 내부망에 보관 → 암호화	보관 금지 (인증시스템 발급 단계에서 신원확인)	보관 금지 (음성으로 신원확인 가능)

3. 이미 거래중인 금융기관과 금융거래시 주민번호 제공이 달라지는 부분은? (p.7)

- 이미 거래중인 금융기관과 거래시 고객은 이전 거래에서 주민번호를 제공하였기 때문에 또다시 제공할 필요가 없음
 - 거래방식별로 신분증(점포·모집인), 인증시스템(인터넷), 주민번호 이외의 식별정보(통화)를 통한 신원확인 절차는 거칠 필요
- 금융기관은 신분증 사본을 전자형태로 내부망에 보관시 개인정보법에 따른 주민번호 암호화에 맞추어 사본도 암호화
 - 복사 등 실물형태로 신분증 사본 보관시 주민번호 뒷자리를 삭제하여 주민번호가 노출되지 않도록 조치
- 고객이 주민번호를 제공하지 않음을 원칙으로 하므로 금융거래 서식상 주민번호란은 삭제
 - 다만, 법령상 규정 준수, 신분증·인증시스템의 재발급·갱신, 단체계약 체결 등의 경우 예외적으로 주민번호 재수집 가능

이후 거래	대면		非대면	
	점포	모집인	인터넷	통화
신원 확인	신분증 확인	신분증 확인	인증시스템 인증 (비밀번호)	주민번호 이외 식별정보로 확인 (주소, 전화번호 등)
신분증 사본	<ul style="list-style-type: none"> 전자형태로 내부망 보관 → 암호화 실물형태로 보관시 주민번호 뒷자리 삭제 	<ul style="list-style-type: none"> 전자형태로 내부망 보관 → 암호화 실물형태로 보관시 주민번호 뒷자리 삭제 	보관 금지 (인증시스템 발급 단계에서 신원확인)	보관 금지 (음성으로 신원확인 가능)

4. 동의서 양식이 구체적으로 어떻게 변경되는 것인가? (p.9)

- 금융회사가 최소한의 정보만을 수집하고 고객도 정보제공 내용을 명확히 인지할 수 있도록 동의서 양식을 개편
 - “필수 사항”과 “선택사항”을 별도 페이지로 구분하고, 필수 사항부터 일괄적으로 동의함으로써 계약 체결(서비스 제공)
 - * 선택사항에 동의하지 않는다고 서비스 제공이 거부되지 않도록 함
 - 제3자 정보제공의 경우 포괄적 동의를 금지, 정보제공의 대상·목적별로 그룹화하여 각각 동의받도록 함(필수*/선택 제공 구분)
 - * (예) 정보처리위탁, 우편발송위탁, 채권추심위탁 등
 - 현재 “제공목적 달성시까지” 등으로 규정된 정보보유기간을 구체적으로 명시(예: “거래 종료이후 2년 내” 등)

참 고

동의서 개편 양식(예시)

* 금감원, 금융권 협회 등을 통해 지속 구체화해 나갈 계획

I. 필수 동의사항

※ 동 필수 동의사항에 대한 동의만으로 상품 및 서비스 계약체결은 완료됩니다.

개인(신용)정보 수집·이용 동의서	1. 수집 및 이용 목적 <input type="checkbox"/> 계약 체결을 위한 본인확인, 신용조회, 대금결제 등 계약의 체결·유지·이행·관리, 카드·금융 상품의 부가·제휴서비스 제공, 금융사고 조사, 법령상 의무이행, 사후관리 등 2. 수집·이용할 개인(신용)정보 내용 <input type="checkbox"/> 개인식별정보, 전자금융거래정보, 신용거래정보(연소득, 대출현황), 채무불이행정보 3. 개인(신용)정보 보유·이용기간 <input type="checkbox"/> 거래종료일로부터 5년 이내		
개인(신용)정보 조회동의서	1. 조회 목적 <input type="checkbox"/> 계약 등 금융거래의 설정·유지 또는 사후관리, 신용관련 통계모형 개발 및 분석, 기타 금 융거래 관련업무 등 2. 조회할 신용정보 <input type="checkbox"/> 개인식별정보, 신용거래정보, 연체 등 채무불이행 정보, 직업·재산 등 신용능력정보, 공공 기관보유정보, 신용등급 및 평점, 타 기관의 신용정보 조회기록, 본인인증정보 등 3. 조회처 <input type="checkbox"/> 신용정보집중기관, 신용조회회사, 공공기관 및 통신회사 4. 조회동의 효력기간 <input type="checkbox"/> 상기 동의는 계약 소멸시까지 효력이 유지되나, 귀하가 신청한 금융거래가 당사에 의해 거절된 경우에는 그시점까지 유효합니다.		
개인(신 용)정보 제공동 의서	공통 필수	1. 제공목적 <input type="checkbox"/> 본인 신용도 판단, 공공기관에서 정책자료로 활용, 계약 등 금융거래의 유지 또는 사후관리, <input type="checkbox"/> 거래목적 달성(거래관계 설정 및 유지여부 판단, 금융사고 조사 등) 2. 제공정보내역 <input type="checkbox"/> 개인식별정보, 신용거래정보, 채무불이행정보, 신용능력정보 3. 정보 제공처 <input type="checkbox"/> 신용정보집중기관, 신용조회회사 <input type="checkbox"/> 채권추심회사 <input type="checkbox"/> 정보처리위탁회사, 우편물 발송 위탁회사 등 4. 정보 보유기간 <input type="checkbox"/> 등록사유 발생과 관련이 있는 거래가 존속하는 기간동안 보존<검토필요>	
	상품 필수 ※	<input type="checkbox"/> A그룹 (선택)	▫정보 제공처 : (총 ○개사) 유통업체, 통신사 ▫혜택 : 포인트 적립, 통신비 할인 ▫정보 보유기간 : 거래 종료 후 ○년 이내
		<input type="checkbox"/> B그룹 (선택)	▫정보 제공처 : (총 ○개사) 금융회사, 항공사 ▫혜택 : 금리우대, 마일리지 적립 ▫정보 보유기간 : 거래 종료 후 ○년 이내
[○○카드]가 위와 같이 본인의 개인(신용)정보를 수집·이용·조회·제공하는 것에 동의합니다.			
[○○카드]가 위와 같이 본인의 고유식별정보를 처리하는 것에 동의합니다.			
▫고유식별정보 : 주민등록번호, 운전면허번호, 여권번호, 외국인등록번호			
이 름			(서 명)

※ 고객이 선택하신 상품 유형에 따라 A그룹 또는 B그룹 중 선택되어 인쇄
 (다만, 기본상품을 선택하신 경우에는 백지로 인쇄될 수도 있음)

II. 선택 동의사항

※본 동의는 계약 체결에 필수적이지 않으며, 동의하셨더라도 당 사 홈페이지 및 고객센터를 통해 철회 가능합니다.

카드 이용권유동의 : ☐ 동의하지 않음 ☐ 동의(☐전체 ☐전화 ☐문자메시지(SMS) ☐서면(DM) ☐이메일)

※카드이용안내에 동의하셨더라도 이용권유목적의 연락에 대한 중단을 요청하실 수 있습니다.

※갱신 및 상품서비스 변경안내 등 계약 이행을 위한 필수 고지사항은 상기 동의 대상에서 제외됩니다.

개인(신용)정보 수집·이용 동의서

1. 수집 및 이용 목적

☐ 신용도 판단, 신용카드 해외부정사용 방지 등

2. 수집·이용할 개인(신용)정보 내용

☐ 직위 등 개인(신용)정보, 출입국 정보 등 신청서 선택항목 중 본인이 선택한 사항

3. 개인(신용)정보 보유·이용기간

☐ 거래종료일로부터 ○년 이내(단, 금융사고 조사, 분쟁해결, 민원처리, 법령상 의무이행을 위한 경우 별도 보관)

[○○카드]가 위와 같이 본인의 개인(신용)정보를 수집·이용하는 것에 동의합니다.

☐ 동의하지 않음 ☐ 동의

[○○카드]가 위와 같이 본인의 고유식별정보를 수집·이용하는 것에 동의합니다.

◦고유식별정보 : 주민등록번호, 운전면허번호, 여권번호, 외국인등록번호

☐ 동의하지 않음 ☐ 동의

개인(신용)정보 제공 동의서

☐ A그룹 (선택)

1. 제공 목적

☐ 제휴보험사의 보험서비스 제공, 보험모집(TM), 보험개발원 전산망의 보험정보 조회를 통한 보험료 정보제공 및 마케팅 활용

2. 제공 정보 내용

☐ 개인식별정보, 신용거래정보, 신용능력정보

3. 혜택

☐ 제휴 보험서비스 이용

4. 정보제공처

☐ 총 10개사(○○보험, □□보험....)

5. 개인(신용)정보 보유기간

☐ 거래종료일로부터 ○년 이내

☐ B그룹 (선택)

1. 제공 목적

☐ 제휴업체의 마케팅, 심사, 부가서비스 개발, 고객관리, 광고성 정보 전송

2. 제공 정보 내용

☐ 개인식별정보, 신용거래정보, 신용능력정보

3. 혜택

☐ 제휴업체 서비스 할인 등

4. 정보제공처

☐ 총 3개사(○○자동차, ○○통신..)

5. 개인(신용)정보 보유기간

☐ 거래종료일로부터 ○년 이내

[○○카드]가 위와 같이 본인의 개인(신용)정보를 제공하는 것에 동의합니다.

☐ 동의하지 않음 ☐ 동의

[○○카드]가 위와 같이 본인의 고유식별정보를 제공하는 것에 동의합니다.

◦고유식별정보 : 주민등록번호, 운전면허번호, 여권번호, 외국인등록번호

☐ 동의하지 않음 ☐ 동의

5. 비대면 영업 세부 통제 방안은? (p.11)

☐ 무차별적 문자전송(SMS)을 통한 권유·모집 등 영업행위 금지

- 마케팅 목적의 문자 수신과 관련한 별도 동의를 받거나 기존계약을 유지·관리*하는 경우는 제외

* (예) 보험계약의 보험료 미납, 연체, 실효, 해지, 만기안내 등

- 다만, 고객이 먼저 전화를 걸어오거나(In-bound), 블로그 등 광고 게시판 등에 연락처를 남긴 경우 등에는 영업가능

☐ 이메일의 제목, 전화상담시 우선적으로 “소속회사, 송부인(모집인 여부), 연락목적 및 정보획득경로” 등을 명확히 안내

- 고객이 관련내용을 확인할지를 쉽게 선택할 수 있도록 개선

* 전화상담의 경우 연락목적 안내 후 곧바로 “통화지속여부” 의사를 확인 하되, “정보획득경로”는 고객이 희망하는 경우 설명

☐ 동일인에 대한 전화상담은 통화 회수를 제한하는 방안도 검토

* (예) 1주일내 통화회수는 “1회”로 제한하되, 고객이 시간을 특정하여 re-call을 요청하거나 통화도중 전화가 중단되는 등 합리적인 이유가 있는 경우 예외

① 이메일 발송

제목 : [○○은행, 대출만기 안내]

본문 : ○○은행, ○○지점 ○○○차장입니다. 고객님의 ○○일 가입하신
대출의 만기가...

<본문 중략>-----

-----.

앞으로 이메일 수신을 원치 않으십니까?

수신 거부

② 전화상담

= 안녕하세요? ○○생명의 상담원 ○○○입니다.

= 고객님의 ○○생명의 신규 보장성 ○○상품을 설명드리려고 하는데, 지금
시간이 괜찮으신지요? (설명을 들으시겠습니까?)

[거부시]

= 오늘 다시 설명을 들으시겠습니까? (몇 시쯤 연락 드릴까요?)

[고객이 본인정보를 어떻게 취득했는지 묻는 경우]

= 고객님의 소중한 정보는 '13.2.1일 ○○○에서 제3자 제공동의로 취득하게
되었습니다.

[고객이 “연락금지”를 요청하는 경우]

= 고객님의 요청이 접수되었습니다. 향후 안내를 다시 희망하시는 경우
○○○-○○○로 연락하시면 됩니다.

6. 정보 이용·제공 현황 조회 시스템은 어떤 것이고, 언제쯤 구축되는 것인가요? (p.15)

- 금융회사가 수집한 고객 개인정보의 이용 및 제공 현황을 고객이 쉽게 확인할 수 있는 시스템을 구축
 - 각 금융회사별로 홈페이지에 시스템을 구축하고, 본인 인증을 거쳐 개인정보 이용 현황* 등을 조회할 수 있도록 함
 - * 이용·제공주체, 목적, 날짜 등 포함
 - * 전화 등을 통해서도 본인인증을 거친 경우 이용제공 현황을 안내
 - 또한, 원하지 않는 정보 제공 동의도 철회*할 수 있도록 하여 고객의 자기정보결정권을 실질적으로 보장
 - * 동의 철회로 서비스 제공이 중단되거나, 계약이 해지되는 경우에는 별도로 안내
- 동 시스템 구축은 정보 제공 동의서 양식 개편(필수/선택항목, 포괄적 동의 제한 등)과 연계하여
 - 상반기 중 세부 구축방안을 확정하고 4분기중 서비스를 제공할 계획임

7. Do-not-Call(연락중지 청구 시스템)은 어떤 것이고, 언제쯤 구축되는 것인가요? (p.15)

□ 연락중지 청구 시스템은 소비자가 원치않는 금융회사로부터의 마케팅 목적 전화를 거부(Do-not-Call)할 수 있도록 구현한 것

* 보험개발원 자동차보험('12.4월~) 및 공정위 전화권유판매(보험, 대부업 등 제외) 수신거부시스템 운영('14.1월~)

○ 금융업권별 협회 공동*으로 시스템을 구축하여, 소비자는 한 번의 등록으로 모든 업권의 금융회사의 영업목적 연락에 대한 중지를 요청**할 수 있음

* 다만, 대부업의 경우, 별도 홈페이지에서 동 시스템 구축 예정

** 정보제공 및 이용은 계속 동의하되, 마케팅 목적의 연락만을 차단

□ 구체적 구축방안 협의 후 6월중 서비스 개시 예정

※ 수신거부의사(Do-not-Call) 등록 절차(예시)

① 소비자가 금융협회 통합 Do-not-Call 홈페이지에서 휴대폰 인증을 통해 수신거부 의사를 등록

* 개별 금융회사 또는 전체 금융회사에 대한 수신거부 가능

② 수신거부의사를 등록한 전화번호는 해당 금융사로 주기적으로 통보(예 : 주 1회 등)

③ 금융회사는 수신거부의사가 등록된 전화번호로는 전화권유 판매를 하여서는 안됨

8. 정보 보호 요청권이란 것은 구체적으로 어떤 것인가요?

(p.15)

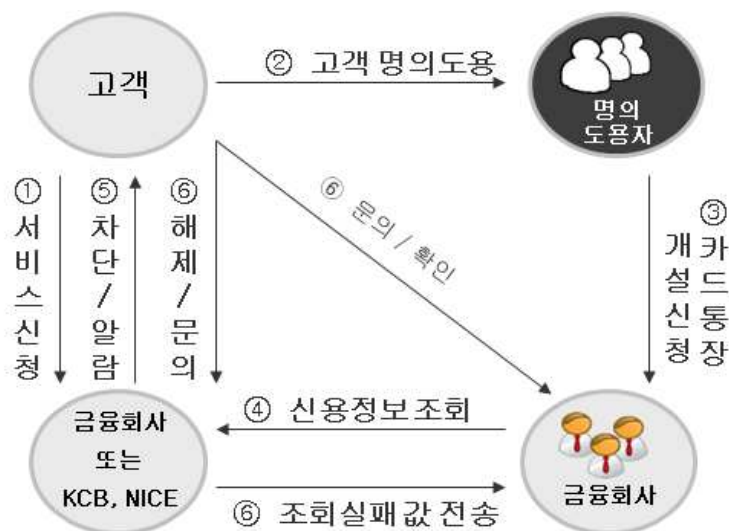
□ 거래가 종료된 경우, 금융회사가 보유한 본인 정보의 파기 및 엄격한 보안조치를 요구할 수 있는 권리를 보장

- ① 거래가 종료된 후 고객(신용정보주체)이 본인의 정보를 삭제해 줄 것을 금융회사 등에 요청하면,
 - ② 금융회사 등(신용정보 제공·이용자)은 해당 정보를 원칙적으로 삭제하되,
 - ③ 법령상 보관 필요성 등을 위해 보관이 불가피한 경우에는 “엄격히” 별도 조치하여 관리(2단계 보안조치*)하여야 함
- * 원칙적으로 모든 정보를 파기하고, 법령상 보존의무가 있는 경우는 2단계 보안조치(별도 DB 보관, 업무상 필수인원만 접근가능)를 통해 엄격히 관리
- ④ 삭제 또는 보안조치가 이루어진 경우에는 그 결과를 고객에 별도로 통지하여야 함

9. 본인정보 조회중지 요청권은 무엇이고, 어떻게 신청하여 이용할 수 있습니까? (p.16)

- 고객의 요청이 있는 경우 일정시간 신용조회를 차단하여, 개인 신용정보의 무단도용 등에 따른 피해(대출사기, 카드 무단발급 등)를 예방할 수 있도록 보장하는 권리로,
 - 정보유출시 또는 확인되지 않았으나 외부에 유출된 정보로 인한 국민 불안과 잠재적 피해 가능성을 차단하기 위한 것
- 고객 요청이 있는 경우*, 명의도용 의심되는 신용조회** 발생시 일정시간 조회를 중지(예 : 1일간)하고 고객에 “지체없이 통지”
 - * 금융회사 또는 신용정보회사(KCB, NICE 등)에 신청 가능
 - ** 금융회사는 대출 또는 카드 발급시 개인 신용정보를 조회
- 고객은 해당 사실을 확인하여 불법 유출정보를 악용한 제3자 대출 및 카드발급 시도 등을 차단

※ 정보유출에 따른 명의도용 의심시에는 유출한 금융회사에서 비용 부담



10. 금융보안 표준 체크리스트의 적용시기, 주요 점검 분야 및 미이행시 제재방안은? (p.21)

- (적용시기) 2014년 상반기중 금감원이 '금융보안 표준 체크리스트'를 마련 → 하반기부터 적용(전자금융감독규정 개정)
- (주요 점검 분야) 단말기 보호대책, 전산자료 보호대책 및 해킹 등 침해행위 방지대책 등 보안규정 전반을 포함할 것임
- (이행점검 및 제재) 각 금융회사가 자체적으로 '보안점검의 날'을 지정하여 매월 점검하도록 하고
 - 금감원은 금융회사의 점검결과를 즉시 제출 받아 검사에 활용하는 한편, 미이행시에는 당해 기관 및 책임자를 엄중 제재*할 예정임

* 전자금융거래법 §39⑥에 따라 시정명령, 기관주의 · 경고, 임직원 주의 · 경고 · 문책요구, 임원의 직무정지 · 해임권고 요구 가능

* 전자금융거래법 §43②에 해당될 경우 업무정지 명령 가능

11. 외주용역 체크리스트는 어떤 내용을 담고 있나? (p.21)

- 체크리스트는 외주용역 수행 중에 발생할 수 있는 정보유출사고 등을 예방하기 위한 **보안통제 점검항목**으로 구성되어 있음
 - (업무통제) 업무범위 외 작업수행 통제, 운영시스템 접근통제, 고객정보 **변환 사용**, 고객정보 사용내역 기록·관리 등
 - (PC관리) USB 차단 등의 **보안프로그램** 설치, 백신프로그램 설치, 고객정보 PC보관 금지, 인터넷 차단 등
 - (전산기기 반출입 및 외부인력 통제) 전산기기 반출입 통제, USB 봉인, 근무장소 통제, 외부인 출입내역 기록·관리 등

12. **현행 규정상 금융회사 IT사업에 대한 보안성 심의를 해야 하는 경우와 추가할 사항은?** (p.23)

□ 보안성심의를 금융감독원이 금융회사 정보화사업에 대하여 보안대책을 사전에 점검함으로써 보안사고를 예방하기 위한 제도임

○ 현재 보안성심의를 해야 하는 경우는

(i) 전산실 신규 설치·이전, 재해복구센터를 구축하는 경우

(ii) 외국금융회사의 전산시설에 대한 해외 설치·이전 및 공동 이용을 하는 경우

(iii) 그 밖에 전자금융거래 안전성 확보를 위하여 금융감독원장이 필요하다고 인정하는 경우

○ 향후, 보안성심의 대상에 추가될 정보화사업은 금융감독원, 금융회사 등과 협의하여 보안성심의 대상을 정할 계획임

< 보안성심의 대상에 추가될 정보화사업 (예시) >

- 대규모 정보시스템 구축(예, 10억이상) 정보화 사업,

- 다량의 개인정보(예, 100만명 이상)를 처리하는 정보시스템 구축 사업 등