금융위원회	**보 도 자 료** **브리핑시부터 보도 가능**	• 미래창조 금융 • 따뜻한 금융 • 튼튼한 금융

작성부서	**(금융위원회)** 서민금융과, 중소금융과, 전자금융과, 금융제도팀 **(기획재정부)** 자금시장과 **(미래창조과학부)** 통신자원정책과 **(안전행정부)** 개인정보보호과 **(방송통신위원회)** 개인정보보호윤리과 **(금융감독원)** 감독총괄국, 상호여전감독국, 여신전문검사실, IT감독국, 개인정보보호단, 서민금융지원국			
책 임 자	최용호 과장(2156-9470)	담 당 자	전은주 사무관(2156-9670) 김영대 사무관(2156-9472)	
	이윤수 과장(2156-9850)		이종림 사무관(2156-9856)	
	전요섭 과장(2156-9490)		임왕섭 사무관(2156-9494)	
	손영채 팀장(2156-9680)		윤동욱 사무관(2156-9681)	
	김병환 과장(044-215-2750)		박재형 팀장(044-215-2751)	
	김성규 과장(2110-1940)		박시혜웅 사무관(2110-1947)	
	문금주 과장(2100-1738)		이갑준 사무관(2100-2816)	
	반상권 과장(2110-1520)		정복덕 사무관(2110-1521)	
	권순찬 국장(3145-8300)		김동성 팀장(3145-8001)	
	김영기 국장(3145-7550)		김동현 팀장(3145-7435)	
	조성목 실장(3145-8810)		박상춘 부국장(3145-8805)	
	송 현 국장(3145-7180)		김윤진 부국장(3145-7182)	
	정인화 단장(3145-7850)		차재성 수석(3145-7852)	
	양현근 선임국장(3145-8150)		남택준 부국장(3145-8140)	
배 포 일	2014.3.10(월)	배포부서	대변인실(2156-9543~48)	총 10매

제 목 : 「금융분야 개인정보 유출 재발방지 종합대책」

Ⅰ 기본방향

□ 정부는 『**경제혁신 3개년 계획**』의 "**원칙이 바로 선 시장경제**" 분야 핵심과제 중 하나로 「**금융분야 개인정보 유출 재발방지 종합대책**」을 **관계부처 합동**으로 마련하였음

○ 금번 대책은 최근 발생한 **카드사 정보유출**과 **과거 해킹사고** 등에서 드러난 문제점에 대한 **근본적·종합적 재발방지 방안**을 마련하여 부분적·단편적 대응에 따른 **반복적인 정보유출·해킹사고를 차단**하고,

- 이번 사고를 계기로 **ICT에 기초한 신용사회의 기반을 재구축**한다는 차원에서 **금융분야 개인정보 보호 및 사이버안전을 획기적으로 제고**할 수 있는 방안을 강구하는데 중점을 두었음

○ 이를 위해, 「**고객정보 보호 정상화 TF**」를 중심으로 「**금융회사 고객정보 유출 재발방지대책**(1.22)」과 「**개인정보 불법유통·활용 차단조치**(1.24)」 등 기발표된 대책의 내용을 전문가와 관계부처·기관 검토를 거쳐 보다 발전·구체화 시켰으며,

- 정무위 **국정조사** 등 국회 논의과정에서 **제기된 내용 등도 반영**하였음

□ 이번 **"종합대책"**은 **다음 4가지 기본방향**에 따라 마련하였음

① **개인정보의 「수집-보유·활용-파기」 등 단계별로 금융소비자의 권리 보호 및 금융회사 책임을 대폭 강화**

- 구체적인 기술적 보안방안에 있어서는 **자율권을 부여**하되, 유출사고 발생시에는 **금융회사에 엄정히 책임을 물어** 형식적 기준과 절차만 준수하면 사고가 발생해도 제재를 받지 않는 문제를 방지

② **금융회사가 확실하게 책임지는 구조를 확립**

- **CEO 등의 책임을 강화**하고 **모집인과 제3자**에게 제공한 정보에 대해서도 금융회사에 **관리책임**을 부과하고

- 징벌적 과징금 도입, 형벌과 행정제재 상향을 통해 **개인정보보호법 등 정보보호의 일반법보다 책임을 한층 강화**

③ 해킹 등 외부로부터의 **전자적 침해행위에 대해서도 기존 대책**('13.7월 발표)**을 대폭 보강**

- **주기적인 보안 이행실태 점검·보안전담기구 설치** 등으로 **상시적인 보안체계** 구축

④ 이미 계열사와 제3자에 제공되었거나 외부유출된 정보로 인해 **잠재적으로 피해가 발생할 가능성**에 대해서도 **대응방안을 강구**

Ⅱ 주요 내용

< 요 약 >

1 금융회사의 정보수집을 **최소화**하고 **보관기간을 5년**으로 단축하는 등 정보를 **체계적으로 엄격히 관리**

⇒ **정보유출 및 불필요한 사용을 예방**하고, **유출시 피해를 최소화**

2 주민등록번호는 **최초 거래시에만 수집**하되, **번호 노출이 최소화**되는 방식으로 수집(예: key-pad 입력)하고, **암호화하여 제대로 보관**

⇒ **불필요한 주민번호 수집을 억제**하여 **유출시 위험 감소**

3 정보 제공 등의 **동의서 양식을 중요 사항**은 잘 보이도록 **글씨를 크게** 하고 **필수사항에 대한 동의만으로 계약이 체결**되도록 전면 개편

⇒ 고객이 **내용을 명확히 인지**하고 **정보제공 여부를 결정**할 수 있도록 보장

4 금융회사의 **개인정보 이용·제공 현황을 조회**하고, **영업목적 전화에 대한 수신 거부**(Do-not-Call) **등록** 등을 위한 **시스템 구축**

⇒ 개인의 **"자기정보결정권"이 실질적으로 구현**

5 **임원 등의 정보보호·보안관련 책임을 강화**하고, 불법정보 활용·유출과 관련한 **금전적·물리적 제재를 대폭 강화**

⇒ 정보보호와 관련해서는 **금융회사가 확실하게 책임지는 구조**를 **확립**하여 **불법정보 활용·정보유출을 근절**

6 금융전산 **보안전담기구 설치** 등을 통해 금융회사의 **보안통제를 강화**하는 한편, **카드결제 정보**가 안전하게 처리되도록 **단말기를 전면 교체**

⇒ 해킹에 **철저히 대응**하고, **카드결제과정**에서의 **정보보호도 한층 강화**

7 금융회사가 **보유** 또는 **제공한 정보도 불필요**한 것은 **즉시 삭제**하고, 정보유출시 **대응 매뉴얼**(Contingency Plan)**마련** 및 **비상 대응체계 구축**

⇒ 기존 정보로 인한 **잠재적 피해 가능성을 차단**하고, **신속하고 세밀한 대응**을 통해 **피해 최소화 및 확산 억제**

1. 정보 처리 단계별 금융소비자의 권리 및 금융회사 책임 강화

(1) 「수집-보유 · 활용-파기」 단계별 정보보호 강화

□ 그간 금융회사가 **영업에 필수적이지 않은 정보까지 수집**하여 **장기간 보유**하고 **소홀하게 관리**하였던 문제를 근본적으로 해결할 것임

○ **(수집)** 현재 30~50여개에 이르는 수집정보 항목을 **필수정보 6~10개*** **등 필요최소한만 수집**

* 공통 필수항목(이름, 주민번호, 주소, 연락처, 직업, 국적)과 상품성격상 필요 정보(예: 재형저축 가입시 연소득 등)

- 필수정보 외 부가서비스 제공 등과 관련된 **추가적 정보 수집**은 **"계약체결에 필수적이지 않음"을 고지**하고, 수집목적·제공처 등을 설명한 후 **고객 동의하에 수집**

○ **(보유·활용)** 금융지주 內 **계열사 정보**를 고객동의 없이 **외부영업에 이용하는 것을 제한**하고, 계열사간 정보 제공시 **이용기간을 필요최소한**으로 설정

- **제3자 정보제공시 포괄적 동의**를 **금지**하고 서비스 제공에 **필수적/선택적 제3자**를 구분하여 동의를 받도록 하며, 정보이용 목적, 제공업체, 제공기간, 파기계획 등을 구체적으로 적시

○ **(파기) 거래종료 후**에는 **식별·거래정보** 등 일정기간 보관이 필요한 정보를 제외한 여타 신상정보 등은 **즉시**(3개월 이내) **파기**

- 보관정보도 **법령상 추가 보관의무** 등 불가피한 경우*만 제외하고 **5년내 파기**

* 예: 자본시장법 상 투자자 계약관련 자료 10년간 보관, 상해보험 후유장애 보장을 위한 정보

(2) 금융거래시 주민번호 노출 최소화

□ 금융거래시 서식에 직접 주민번호를 기입하고 신원확인시 매번 제공함에 따라 **주민번호가 과다노출**되고 **불법활용·유출 위험도 증가**하는 문제를 개선하겠음

○ **최초 거래시에만 주민번호를 수집**하되 **번호 노출이 최소화**되는 방식으로 수집(예: key-pad 입력)하고,

- 이후에는 **주민번호 수집 없이** 여타 정보 활용 등을 통해 **신원확인**

○ 수집 주민번호는 **암호화**하여 안전하게 **보관**

○ 주민번호 불법활용·유출에 대해서는 **일반 개인정보보다 가중하여 제재**

(3) 정보제공 동의서 양식 전면 개편

□ **금융회사**가 **최소한**의 **정보만 수집**하고 **고객**도 정보제공 내용을 **명확히 인지**할 수 있도록 **동의서 양식을 개편**하겠음

○ **"필수사항"**과 **"선택사항"**을 **구분**하고 **필수사항 동의**로 **계약 체결**(서비스 제공)이 이루어지도록 하여, 선택사항에 동의하지 않는다는 사유로 서비스 제공을 거부하지 못하도록 함

○ 동의서의 **글자 크기, 줄 간격 등도 확대**하여 **읽기 쉽게 개선**

(4) 문자 등을 통한 비대면 영업행위 제한

□ **금융소비자 불편**을 초래하고 **정보의 적법성을 확인**하기 어려운 **비대면 영업행위**는 엄격하게 제한하겠음

○ 무차별적 **문자메시지 전송**을 통한 **영업행위는 전면금지**

○ 기타 **전화·이메일** 등 여타 非대면방식 모집·권유행위는 **엄격한 정보활용 기준***에 따라 **제한적인 범위내에서만 허용**

* 예 : 이메일·전화상담시 "소속회사, 목적, 정보획득경로" 등을 사전에 명확히 안내

(5) 금융소비자의 자기정보결정권을 확실히 보장

□ 금융소비자가 본인 정보가 어떻게 **활용**되는지 **알지 못하고**, 본인 정보의 **제공·조회·삭제 등을 스스로 결정할 수 없었던** 문제를 해결하겠음

○ **(정보 이용현황 조회권)** 고객이 **본인 정보의 이용·제공 현황**을 **언제든지 확인**할 수 있도록 금융회사별로 **조회시스템** 구축

○ **(정보제공 철회권)** 고객이 원하는 경우 **기존의 정보 제공 동의를 철회**할 수 있는 권리를 보장

○ **(연락중지 청구권) 고객이 수신거부 의사**를 밝히면 **해당 금융회사**로부터 **영업목적 연락**을 **차단**(Do not call)하는 시스템 구축

○ **(정보보호 요청권)** 거래종료 고객이 **본인 정보의 보호를 요청**할 경우, 금융회사가 **파기 또는 보안조치**를 취하도록 하는 제도를 도입

○ **(신용조회 중지 요청권) 명의도용 피해 방지** 등을 위해 고객이 요청하는 경우, 대출, 카드발급 등을 위한 **신용조회를 일정기간**(예 : 1일간) **중지**

2. 금융회사가 확실하게 책임지는 구조 확립

(1) CEO 등의 책임 강화

□ CEO 등 주요 의사결정자가 **정보보호와 보안에 대해 관심이 부족**하고 **정보보호책임자의 역할도 제한적**이었던 문제를 개선하겠음

○ **정보보호 현황 및 정책**을 **매년 작성**하여 **CEO 및 이사회**가 직접 보고를 받도록 하고, **감독당국**에도 **제출**

○ **신용정보 관리·보호인**을 **임원**으로 두도록 하고 권한도 강화

○ **정보보호최고책임자***(CISO)가 정보 효율성을 강조하는 업무 담당시 발생하는 이해상충 방지를 위해 일정규모 이상 금융회사의 CISO는 **타 IT 관련 직위와 겸직 제한**

* 전자금융거래법상 전자금융 보안 책임자(Chief Information Security Officer)

(2) 모집인·제3자 정보제공시 금융회사 책임 강화

□ 모집인, 계열사·협력사 등이 무분별하게 정보를 활용하고 정보유출 위험도 높았던 문제를 해결하기 위해 **금융회사의 관리책임**을 강화하겠음

○ 금융회사가 모집인에 정보 제공시에는 **최소한의 정보**만을 **암호화**하여 제공하고, **"정보활용·파기 관리대장"**을 작성하여 **주기적으로 점검**

- 금융회사는 모집인의 계약 승인시 **모집경로를 확인**하여 **적법 정보를 활용했는지 확인**

- 정보유출·불법정보 활용시 **모집인***뿐만 아니라 **금융회사에 대해서도 엄정한 책임**(과징금 등)을 추궁

  * 즉각 계약해지, 5년간 재등록 제한(다른 업권의 동일한 모집행위도 금지)

○ 금융회사는 **제3자 및 계열사**에 정보를 제공한 경우에도 **이용기간 도과시 파기여부를 확인**하고, **관리실태를 CEO** 등에 **주기적으로 보고**

(3) 사후적 제재 대폭 강화

□ 정보유출시 **국민불안·피해 등 사회적 파장에 상응하는 수준으로 제재**함으로써 금융회사 등이 경각심을 갖고 재발방지에 노력하게 하겠음

○ **대폭 상향된 "징벌적 과징금"** 부과

- **불법정보 활용**시 **"관련 매출액"의 일정비율**(예 : 3%)**을 부과** (금액은 사실상 무제한)

- **정보 유출**시에도 여타 법률보다 **높은 한도**(예 : 50억원)로 부과

○ **형벌수준**을 **금융관련법 최고 수준**(10년이하 징역 등)으로 상향

○ **영업정지** 등 기타 제재도 **크게 강화**

- **신용정보회사**는 불법정보 유출 관련시 **영업정지**(6개월 이내) 또는 **이에 갈음하는 과징금**을 부과하고, **3년내 재위반시 허가 취소**

- 금융회사가 보안대책 미비 등 주의의무를 다하지 않은 경우 **과태료 상향**(600만원 → 5,000만원)

- **금융회사**의 **영업정지** 등 기관제재 **강화**(예 : 카드사 영업정지 3→6개월)

  * **상시점검 미흡**으로 사고인지를 못했거나, **사고 발생을 고의적으로 숨긴 경우 가중**하여 엄정 제재

3. 해킹 등 전자적 침해행위에 대해서도 강력히 대응

(1) 기존 전산보안 대책 대폭 보강

□ 기발표한 「**금융전산 보안 강화 종합대책**('13.7월)」을 **철저히 이행**하는 한편, 전산보안 강화를 위한 **추가적인 노력**도 다각도로 추진하겠음

○ **내·외부망 분리***를 차질없이 추진하고(점검 후 미이행시 제재 부과), **주민번호 암호화도 조기에 추진****

* 전산센터는 '14년말, 은행의 본점·영업점은 '15년말, 비은행은 '16년말 완료
** 암호화 적용대상, 추진일정을 마련하여 단계적으로 시행

○ **금융전산 보안관제*** **범위**를 은행·증권에서 **보험·카드**까지 확대하고, "**금융보안 전담기구**" 설치도 추진('15년 출범목표)

* 금융회사 전산망에 대해 해킹 등 전자적 침해 여부를 모니터링하는 서비스

○ 객관적인 평가기관*이 금융회사의 **전산보안 수준을 평가·공개**하는 "**금융전산 보안인증제**"를 **도입·확대**하고, 금융회사 IT사업에 대한 금감원의 **보안성 심의도 확대 실시**

* 예: 한국인터넷진흥원, 금융보안 전담기구 등

(2) 정보보안 관련 점검·관리 강화

□ 현장에서 **정보보안 규정이 제대로 지켜지지 않아** 미연에 방지할 수 있었던 사고가 발생하는 것을 차단하기 위해 **점검과 관리**를 강화하겠음

○ **CISO** 책임하에 **매월 보안점검***을 실시, **CEO에게** 점검결과를 **보고**하고 금감원에도 제출

* 금감원은 필수 보안규정이 누락되지 않도록 **'금융보안 표준 체크리스트'**를 마련

○ 금융회사 외주용역의 **입찰→계약→수행→완료 등 全 단계**에 걸쳐 **관리 기준 및 절차를 마련***하는 등 **통제를 강화**

* '국가 정보보안 기본지침'의 관리절차를 전자금융감독규정에 반영

○ **불시점검***, **기획검사** 등을 통해 금융회사의 보안규정 실천을 체질화

* 금감원 중심으로 인터넷진흥원, 금융보안전담기구 등으로 '기동점검반' 운영

(3) 신용카드 결제시 개인정보 보호 강화

□ **신용카드 결제정보**가 **가맹점 단말기, VAN사** 등을 거쳐 처리되는 과정에서 **정보유출 위험이 없이 안전하게 처리**될 수 있도록 다각적인 개선방안을 추진하겠음

○ 보안성이 낮은 마그네틱 신용카드를 **IC카드로 조속히 교체**하고, **가맹점 단말기**도 정보의 암호화가 가능한 **IC단말기로 조속히 전환**

- 카드사 가맹점계약 체결시 **IC단말기 설치여부 확인, 영세가맹점**에 대한 **단말기 교체 자금 지원**(소멸포인트 등으로 기금 조성)

○ 가맹점이 **보안이 강화된 단말기**를 사용하도록 적극 유도

- '14년 하반기중 **'IC결제 우선 승인제***'를 실시하고, '15년부터는 IC단말기 설치 가맹점의 IC사용, '16년부터는 **全 가맹점 IC사용 의무화**

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

○ **VAN사 등록제**를 도입하고, **IT안전성 확보, 신용정보 보호, VAN사 대리점 관리 의무를 부과**하고, 의무 위반시 **과징금·등록취소** 등 제재장치 마련

4. 기제공·유출된 정보로 인한 잠재적 피해 가능성 차단

□ 금융회사가 **현재 보유**하고 있거나 협력사·계열사 등에 **제공한 정보**, 또는 확인되지 않았으나 **외부에 유출된 정보**로 인한 **국민 불안과 잠재적 피해 가능성을 차단**하기 위한 조치도 시행하겠음

(1) 기존정보로 인한 피해 가능성 차단

○ 현재 진행중인 전면점검을 통해, **금융회사가 보유**하고 있거나 **제3자 등에 제공**된 개인정보의 적법성을 철저히 점검

- 계약유지, 법률상 의무이행 등에 꼭 필요한 정보외에는 **일괄 파기**('14년중)

- 이번 점검 이후에 **불필요한 정보를 보유하다 불법활용 또는 유출**된 경우에는 **엄중 제재**

○ 고객이 개인정보 유출로 인한 피해 등을 우려하여 요청하는 경우, **카드 교체** 등을 신속히 할 수 있도록 지원하는 방안 등을 마련

(2) 대응체계 구축

○ 정보유출 사고 발생시 **신속하고 빈틈없는 대응**을 위해 금융회사별로 **CEO 책임**하에 **대응매뉴얼(Contingency Plan)** 마련

○ 금융회사는 사고 발생(인지) **즉시 자체 비상 대응체계를 가동**하고, 필요시 **금융당국**은 물론 **관계부처·기관 공조를 통해 대응**

- **정보유출 피해 최소화**(고객 불편·불안 최소화, 금융사기 단속 등), **피해예방조치***의 신속한 이행, **피해자 구제** 등을 위한 **전방위적인 피해확산 방지대책**을 마련하여 시행

* 예 : 결제내역 확인 문자(SMS) 무료 서비스 제공,
전자금융사기 예방서비스 적용범위 확대 시행(300→100만원)

Ⅳ 향후 계획

□ 법 개정이 필요하지 않은 **불필요한 정보 삭제, 고객정보 보호를 위한 시스템 구축** 등은 **최대한 조속히 시행**

□ 신용정보법·전자금융거래법 등 **법률 개정안**(국회 계류중)은 **적극적 국회 설득** 등을 통해 **상반기 중 국회 통과 추진**

□ 「**고객정보 보호 정상화 TF**」를 통해 **금번 대책의 이행상황을 지속적으로 점검**하는 등 차질없이 추진

※ 별첨 : 「금융분야 개인정보 유출 재발방지 종합대책」