

유럽연합의 PSD 2 시행이 금융권에 미치는 영향 분석

최규선*, 이지영**

I. 연구배경 및 범위	1
II. PSD 2 개요 및 현황	2
가. 도입 목적	2
나. 도입 경과	3
다. 주요 내용	5
라. 연관 법령	14
마. 적용사례	16
III. PSD 2 시행이 금융권에 미치는 영향	18
가. 유럽연합 내 금융회사	18
나. 유럽연합 내 비금융회사	21
다. 국내 금융권에 미치는 영향	23
IV. 시사점	28

* 금융결제원 금융결제연구소 전문연구역(E-mail : ksunchoi@kftc.or.kr)

** 금융결제원 금융결제연구소 연구역(E-mail : joannajyoung@kftc.or.kr)



1. 연구배경 및 범위

- 유럽연합은 역내 지급결제시장을 통합하고 소비자들에게 보다 편리하고 안전한 지급결제서비스를 제공하기 위하여 지급결제서비스 지침을 개정(PSD 2)하여 2018년 1월부터 시행하고 있음
 - 이에 유럽연합의 PSD 2의 도입 목적과 주요 내용을 검토하고 동 지침의 시행이 EU 내 금융권에 미치는 영향을 알아보고자 함
- 국내에서도 보다 안전하고 효율적인 금융생태계를 구현하기 위해 이와 유사한 형태의 논의가 활발하게 진행되고 있어, 향후 국내 금융권에 미치는 영향을 파악하고 시사점을 도출하고자 함

2. PSD 2 개요 및 현황

- PSD 2는 유럽은행감독청(EBA)이 규정하고 있는 유럽연합 내 지급결제서비스에 관한 지침인 PSD를 개정한 것임
 - (PSD의 규제 체계 범위 확대) 거래의 지리적 및 통화 범위를 확대하고, 신규 지급결제서비스 등 포괄적인 형태의 전자금융거래를 동 지침의 규정범위에 포함
 - (지급결제서비스의 경쟁 및 혁신 촉진) 지급지시서비스 제공업자(PISP), 계좌정보서비스 제공업자(AISP) 등 제3자 지급결제서비스 제공업자를 규정하고 이들의 소비자 계좌에 대한 접근을 보장
 - (소비자 보호 강화 및 투명성 제고) 서비스 제공업자의 거래에 대한 정보공개 의무 및 거래에 따른 보안조치가 강화됨
- 또한 EBA는 PSD 2에 의거하여 동 지침의 후속조치로 지급결제서비스에 대한 보안요구사항을 규정하는 규제기술표준(RTS)을 마련하고, 2019년 9월부터 시행 예정임



- **(강력한 고객인증)** 모든 지급결제서비스 제공업자는 소비자 보호를 위하여 2요소 인증, 동적요소 인증 등을 활용하여 전자금융 개시 및 처리 시 거래자의 신원을 파악해야 함
- **(개방형 통신표준)** 금융회사는 거래에 대한 명확한 동의의사를 확인하고 인증을 거쳐야 하며, 제3자 지급결제서비스 제공업자에게 안전한 통신채널을 통해 계좌정보에 대한 접근권을 보장

3. PSD 2 시행이 금융권에 미치는 영향

- 신규 서비스제공업자의 금융시장 진입 및 계좌접근 허용에 따라 EU 내 오픈뱅킹 흐름이 가속화되어, 금융회사를 포함한 역내 지급결제서비스 제공업자는 다양한 방식으로 대응하고 있음
 - **(은행 등 신용기관)** 기존의 비즈니스를 바탕으로 비즈니스 모델을 발굴하여 수익창출의 기회로 삼고 금융소비자와의 접점을 모색
 - 한편 거래투명성 제고에 따라 가격경쟁이 심화되어 수익이 감소하고, 규제준수에 따른 관리비용이 증가할 것으로 예상
 - **(신용카드업자)** 계좌간지급거래로 인한 카드 발급-매입 비즈니스 축소가 예상되며, 카드매입사는 자체 솔루션 개발을 통해 카드네트워크 활성화를 도모할수있음
 - **(전자상거래업자)** 대금결제에 따른 거래비용을 절감하고, 고객의 구매 및 결제정보를 보유함에 따른 빅데이터 활용이 가능해짐
 - **(플랫폼기업 및 핀테크업체)** 비금융회사의 금융업 진출이 가능해짐에 따라 비즈니스 모델을 다양화하여 혁신적인 지급결제 및 금융서비스 제공이 가능해질 것으로 예상
- PSD 2의 시행이 국내 금융회사에 미치는 영향은 제한적이나, 금융서비스 및 산업의 지형변화에 따라 정책적·기술적·산업적 측면에서 다양한 이해관계자에게 영향이 있을 것으로 판단

약어

A2A	계좌간 Account-to-Account
AISP	계좌정보서비스 제공업자 Account Information Service Provider
API	응용프로그램 프로그래밍 인터페이스 Application Programming Interface
ASPSP	계좌기반 지급서비스 제공업자 Account Servicing Payment Service Provider
CI	신용기관 Credit Institution
CSC	개방형 통신표준 Common and Secure open standards of Communication
EBA	유럽은행감독청 European Banking Authority
EEA	유럽경제지역 European Economic Area
EMI	전자화폐기관 Electronic Money Institution
GDPR	EU 개인정보보호법 General Data Protection Regulation
IBAN	국제은행계좌번호 International Bank Account Number
PFM	개인종합자산관리 Personal Finance Management
PI	지급결제기관 Payment Institutions
PISP	지급지시서비스 제공업자 Payment Initiation Service Provider
PSD	지급결제서비스지침 Payment Services Directive
PSP	지급결제서비스 제공업자 Payment Service Provider
RTS	규제기술표준 Regulatory Technical Standards
SCA	강력한 고객인증 Strong Customer Authentication
SEPA	단일유로지급결제지역 Single Euro Payments Area
TPP	제3자 지급결제서비스 제공업자 Third Party Payment Service provider
XS2A	계좌접근 Access-to-Account

1. 연구 배경 및 범위

- 유럽연합은 역내 지급결제시장을 통합하고 소비자들에게 보다 편리하고 안전한 지급결제서비스를 제공하기 위한 목적으로 기존의 지급결제서비스지침(PSD)을 개정하여 2018년 1월부터 실시하고 있음
- 개정된 지급결제서비스 지침(PSD 2)의 시행에 따라 제3자 지급결제서비스 제공업자는 소비자의 계좌에 접근하여 금융서비스를 제공할 수 있게 되었으며, 이를 위해 금융회사는 표준화된 방식을 통해 고객의 금융정보에 접근할 수 있도록 조치해야 함
 - 또한 서비스제공업자가 지급결제서비스 제공 시 강력한 고객인증 수단을 마련하도록 권고하고 금융정보가 유통되는 경우에도 높은 보안수준을 유지할 수 있도록 추가 조치를 마련해야 함
 - 따라서 유럽연합의 PSD 2의 도입 목적과 주요 내용을 검토하고 동 지침의 시행이 역내 금융권에 미치는 영향을 알아보고자 함
- 또한 국내에서도 보다 안전하고 효율적인 금융생태계를 구현하기 위해 이와 유사한 형태의 논의*가 활발하게 진행되고 있어, 향후 국내 금융권에 미치는 영향을 파악하고 시사점을 도출하고자 함
 - * 핀테크 혁신 활성화 방안(2018.03), 금융분야 데이터 활용 및 정보보호 종합방안(2018.03), 금융분야 마이데이터 산업 도입방안(2018.07) 등

II. PSD 2 개요 및 현황

- Payment Services Directive 2 (이하 “PSD 2”)는 유럽은행감독청(EBA, European Banking Authority)이 규정하고 있는 유럽연합 내 지급결제서비스에 관한 지침인 PSD를 개정한 것임
 - PSD는 EU 내 지급결제서비스 및 지급결제서비스 제공업자(Payment Services Provider, 이하 “PSP”)에 대하여 규제를 통한 서비스 경쟁력 강화 및 소비자의 권익 보호 등을 주요 내용으로 하여 2009년부터 정식 시행 (2007년 제정)
- PSD 2는 보다 효율적이고 안전한 지급결제서비스 제공을 위해 새로운 유형의 PSP 허용, 소비자에 대한 정보투명성 제고 등을 주요 내용으로 하여 2018년 1월 정식 시행 (2016년 제정)

가. 도입 목적

(1) EU 지급결제시장 통합을 위한 지침 범위 확대

- PSD는 유럽연합 및 유럽경제지역(EEA, European Economic Area) 내 안전하고 효율적인 지급결제서비스를 제공하기 위해 2007년 제정됨
 - 초기 목적은 EU 회원국 간의 지급결제서비스를 회원국 내 지급결제서비스와 동일한 수준으로 제공하는데 있었으며 결과적으로 단일유로지급결제지역(SEPA, Single Euro Payments Area) 형성에 도움
- 다만 EU내 지급결제서비스가 취급하는 거래통화 범위가 확대되고 기존 지침의 규제 범위를 벗어난 형태의 지급결제서비스가 개별 국가별로 규정되면서 EU 차원의 법적 불확실성을 해소할 필요성 부각

(2) 지급결제서비스의 경쟁 및 혁신 촉진

- 금융회사(은행 등) 위주의 서비스 공급이 이루어졌던 지급결제시장에 핀테크회사, IT업체 등 제3자 지급결제 서비스 제공업자의 진입을 허용함으로써 시장 내 경쟁 촉진 및 서비스 혁신 유도

(3) 거래투명성 제고 등 소비자 보호 강화

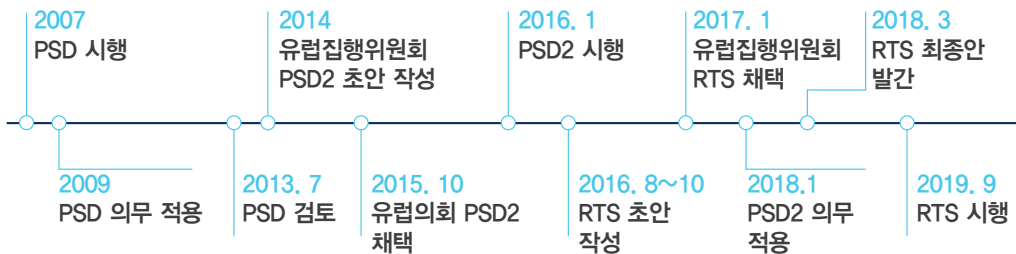
- PSD에서는 제한된 범위의 지급결제서비스 및 서비스 제공업자만이 규제 범위에 포함되어 금융소비자 보호가 미약
 - PSD 개정과 관련된 초기 논의는 카드결제에서 발생하는 수수료 할증(surcharging) 방지를 위한 내용을 포함하고 있었으며, 동 내용은 현행 카드 거래 수수료에 관한 규정*(2015.12)으로 별도 입법
 - * Regulation (EU) 2015/751 on interchange fees for card-based payment transactions (“MIF Regulation”)
 - 한편 PSD 2에서는 지급결제서비스 제공업자에 대하여 거래에 수반되는 정보 공개 의무를 보다 강화하고 부정거래 등에 대한 책임소재를 명확화하여 소비자 권리를 강화
- 또한 후속조치인 규제기술표준(RTS) 제정을 통하여 전자금융 거래에 있어 강력한 고객인증을 요구하는 등 엄격한 보안요구사항을 명시하여 개별 거래의 보안수준 강화

나. 도입 경과

- 2007년 유럽연합의 지급결제서비스지침(PSD) 도입 이후 EU 역내 소액결제시장은 핀테크업체의 성장, 지급결제 부문 비즈니스모델의 혁신 및 지급결제서비스의 지리적 범위 확장 등 급속한 변화를 경험
 - 2013년 중 기존 지침의 적용 범위를 벗어난 지급결제서비스의 법적 불확실성과 새로운 형태의 보안 위험이 발생하면서 이를 해결하고자 지침의 개정 필요성 논의
- 2015년 10월 유럽의회에서 PSD 2가 공식 채택되어 2016년 1월 기준으로 시행되었으며 2018년 1월까지 각국 법령에 입법하여 의무 적용할 것을 권고
 - 2018년 1월부터 시행된 의무적용 범위에 포함되는 지침은 제1단계(거래투명성 강화, 규제 범위 확대) 수준

- 2018년 1분기 중 PSD 2의 후속조치로서 고객인증, 데이터 전송방식 등 기술적 측면을 규제하는 규제기술 표준(RTS)이 발간되어 18개월의 유예기간을 거친 후 2019년 9월 발효되어 시행될 예정
- 동시에 규제기술표준이 발효되는 2019년 9월부터 PSD 2의 제2단계(보안) 및 제3단계(계좌접근권)도 의무 적용 범위에 포함되어 본격 시행

〈그림 1〉 PSD 2 도입 추진 경과



기간	주요 동향
2007~2009	- 2007년 PSD 시행 및 2009년 전면 의무 적용 ◦ 30여개 유럽국가에서 자금이체·지급결제 관련 공동 규정 제정 ◦ 유럽단일지급결제시장(SEPA) 활성화를 위한 법적 토대 마련 ◦ 유럽연합 내 수수료 효율화 및 지급결제 보안 향상
2013~2014	- 2013년 유럽집행위원회, PSD 개정 (PSD 2) 추진 ◦ 지급결제서비스 혁신, 소비자 보호 강화, 인터넷 결제 보안 강화, 계좌접근 허용 등
2015~2016	- 2015년 10월 유럽 의회에서 채택 - 2016년 1월 EU 저널지에 공식 발표 (시행)
2017~2019	- 유럽은행감독청(EBA), PSD 2 활성화를 위한 규제기술표준(RTS) 제정 및 시행

※ 자료 : Evry, 2017

다. 주요 내용

- PSD 2는 117개 조항으로 구성되어 있으며, 연관된 주제에 따라 6개의 타이틀로 구성되어 있던 기존의 PSD에서 일부 조항을 추가 및 수정하는 형태로 개정

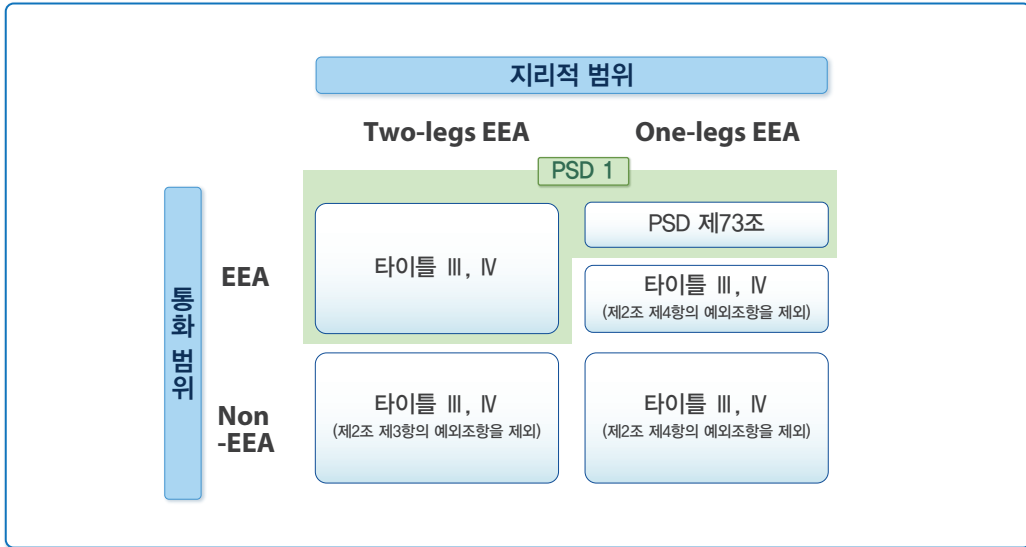
〈표 1〉 PSD 2 조문 구성

<p>타이틀 I 주제, 범위 및 용어정의 : 대상기관, 적용범위, 예외, 정의</p> <p>타이틀 II 지급서비스 제공업자(PSP)</p> <ul style="list-style-type: none"> - 지급결제기관(Payment Institutions)의 일반 원칙, 감독, 면제규정 - 공통조항 : 지급결제시스템 접근, 계좌접근, 금지사항 <p>타이틀 III 지급결제서비스 관련 거래 투명성, 정보공개 요건</p> <p>타이틀 IV 지급결제서비스 제공 및 사용에 관한 권리 및 의무</p> <ul style="list-style-type: none"> - 공통조항 : 범위, 수수료, 적용면제 거래 - 지급거래 인가 : 지급결제서비스 제공업자 및 사용자의 의무 등 - 지급거래 실행 : 지급명령, 결제시간, 책임소재, 데이터보호, 리스크 등 <p>타이틀 V 위임규정 및 규제기술표준(RTS)</p> <p>타이틀 VI 최종 조항</p>
--

1) PSD의 규제 체계 범위 확대

- **(지리적 및 통화 범위의 확대)** 기존의 PSD는 거래당사자(지급인 또는 수취인) 쌍방의 지급서비스 제공업자(PSP)가 EU내 위치하고 유로를 사용하는 거래만을 적용 범위에 포함
 - PSD 2에서는 규제 범위에 포함되는 거래의 지리적 및 통화 범위를 확대하여 적용 (제2조: 범위)
 - **(지리적 범위)** 거래당사자 중 적어도 일방의 PSP가 역내에 위치(one-leg in/out)하면 통화 종류에 관계없이 지침 적용범위에 포함
 - **(거래 통화 범위)** 거래당사자 쌍방의 PSP가 역내에 위치(two-legs in)하면서 유로화가 아닌 통화로 거래되는 경우 지침이 적용됨
 - 다만 동 지침은 EU 역내에서 발생하는 거래 부분만을 적용대상으로 함

〈그림 2〉 PSD 2의 규제 체계 범위



○ 동 지침의 규제범위에 포함되는 거래는 지급결제서비스 관련 거래투명성 및 정보공개 요건(타이틀 III)과 서비스 제공 및 사용에 대한 권리의무(타이틀 IV)를 준수해야 함

□ (거래 범위의 확대) 신규 지급결제서비스 등 포괄적인 형태의 전자금융거래를 동 지침의 규정 범위에 포함

〈표 2〉 지급결제서비스의 범위 (부록 1)

- 현금 입금 등에 필요한 서비스
- 현금 인출(입금이체, 납부자자동이체, 출금이체) 등에 필요한 서비스
- 카드 등을 통한 결제 (여신을 수반하는 지급거래)
- 지급수단(카드, 지갑 등) 발행
- 송금
- 지급지시서비스
- 계좌정보서비스

주) 밑줄은 PSD 2에서 지급결제서비스 범위에 신규 포함된 서비스임

- 특히 PSD에서는 통신사업자가 소비자와 PSP 사이의 중개자 역할을 하는 형식의 지급결제는 지침 범위에 포함되지 않았으나, PSD 2에서는 통신사업자를 통한 상품·서비스 구매에 따른 지급결제를 포함
 - 다만 별도 규정을 통해 통신사업자를 통한 거래 가운데 건당 50유로, 1개월간 300유로 이하의 지급거래는 제외
- 한편 지침의 적용대상에서 제외된 지급유형을 별도로 규정함으로써 소비자 편의를 증대 (제3조: 예외사항)

〈표 3〉 지침 적용대상에서 제외된 지급유형

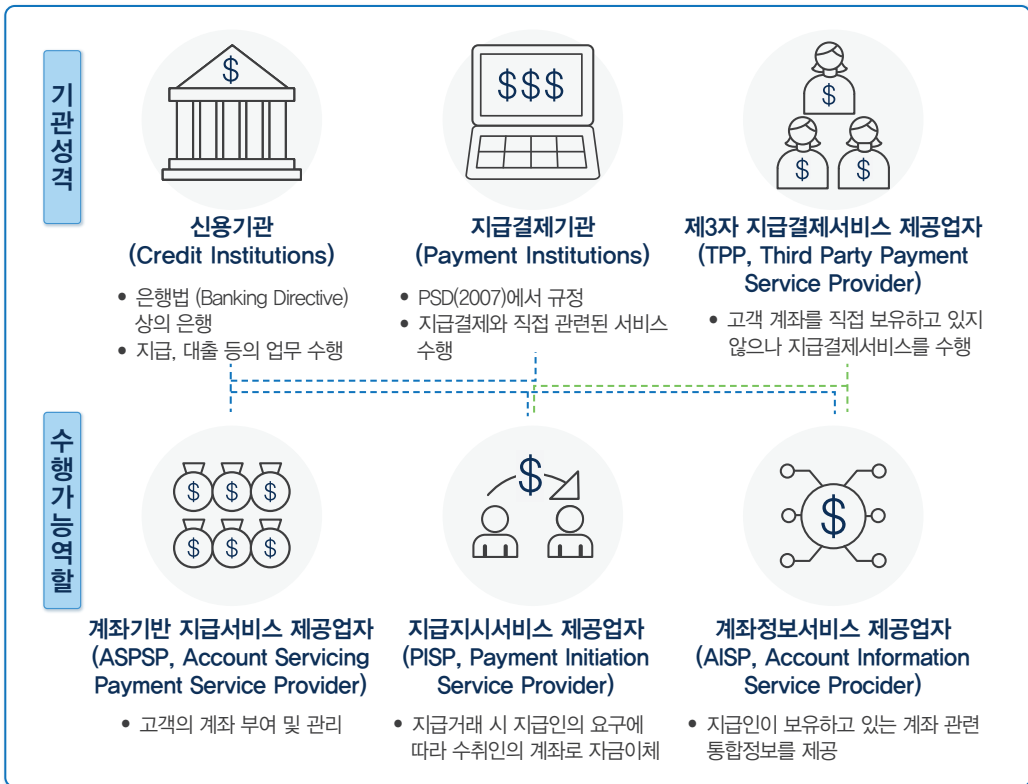
<ul style="list-style-type: none"> • 지급인·수취인간 현금거래 (중개기관 또는 중개인을 경유하지 않는 경우) • 장표기반 지급거래 (종이수표·어음, 거래증빙서류, 여행자수표 등) • 지급결제시스템 지급결제서비스 제공업자, 결제·청산기관, 중앙은행, 참가기관간 지급거래 • 증권 관련 지급 거래 (배당금 및 소득 분배, 증권 상환 및 판매) • 제한된 상품·서비스 구매에 사용하는 특정 지급수단 (주유카드, 식권 등) • 전자통신 네트워크서비스업체(통신사업자)가 제공하는 일부 지급거래 (디지털 콘텐츠, 음성기반 서비스 구매, 자선 활동, 티켓 구매 등) • 중계기관 또는 중개인을 거치지 않은 장의 사업 관련 지급 거래 • 카드발행기관을 대신하는 서비스 제공업체의 ATM 현금인출거래
--

(2) 지급결제서비스의 경쟁 및 혁신 촉진

- 새로운 유형의 지급결제서비스 제공업자(PSP) 규정
 - PSD에서는 지급결제서비스를 제공할 수 있는 기관을 신용기관(Credit Institution)*, 전자화폐기관(EMI, Electronic Money Institutions)**, 지급결제기관(PI, Payment Institutions)으로 규정하였음 (제1조: 대상기관)
 - * 신용기관의 활동 및 신용기관, 금융투자회사의 건전성 감독에 관한 지침(2013)에 의해 허가받은 기관으로, 일반적인 의미의 은행
 - ** 전자화폐기관(EMI)은 유럽의회가 제정한 전자화폐지침(E-money Directive, EMD, 2014)에서 규정하고 있으며, 동 지침에 의해 허가받은 기관임
 - PSD 2에서는 지급결제기관(PI)을 부록 1에서 명시하는 지급결제서비스를 수행하는 기관으로 포괄적으로 정의

- 고객의 계좌를 직접 보유하고 있지 않더라도 계좌정보에 접근하여 서비스를 제공할 수 있도록 하는 제3자 지급결제서비스 제공업자(Third Party Payment service provider, TPP)를 허용
- 이들 TPP는 은행을 통해 고객의 계좌에 접근하여 지급지시하거나 계좌정보서비스 제공업자로서의 역할을 수행할 수 있음

〈그림 3〉 PSD 2의 지급결제서비스 제공업자 및 수행역할

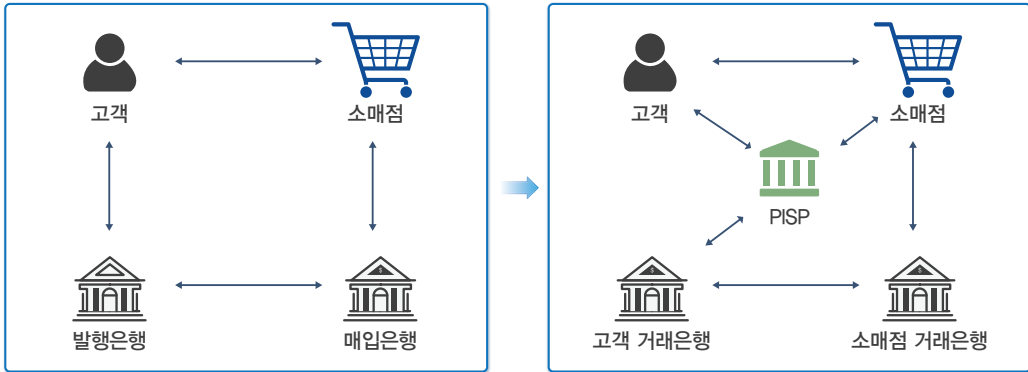


※ 자료 : European Payments Council, 재구성

○ 지급지시서비스 제공업자 (PISP, Payment Initiation Service Provider)

- (서비스 개요) 지급인의 지급개시 요청(payment order)에 따라 지급인의 은행으로부터 거래에 필요한 지급결제정보를 송수신하여 온라인 판매자 등 수취인 앞으로 지급지시
- 동 지침에 따르면 구체적인 사례로 수취인(온라인 판매자)의 웹사이트에서 지급인(구매자)의 은행 계좌기반 지급결제가 가능하도록 서비스를 연결하는 전자상거래 결제수단을 제시 (recital 27)

〈그림 4〉 지급지시서비스 제공업자(PISP)의 업무처리 흐름도



- (특징) 지급인의 은행으로부터 대금을 지급받아 보유하거나 잔액 정보 등 계좌정보를 열람할 수 있는 권한은 없으며, 이체에 필요한 자금여부 등을 확인하여 거래 완결의 가부를 판단하고 지급지시
- 지급인-수취인 계좌간(Account-to-account, A2A) 지급지시를 통한 온라인 대금결제가 가능하므로, 계좌를 보유하고 있지 않은 기관도 지급결제서비스를 제공 가능
- (서비스 예시) 전자상거래업자 아마존은 결제기능을 연결하여 선불충전수단, 신용카드 외 은행계좌를 통한 대금지급이 가능

〈그림 5〉 “아마존페이” 서비스 흐름도



※ 자료 : Driving change with PSD2 and the MIF regulation, Payon (2016. 05)

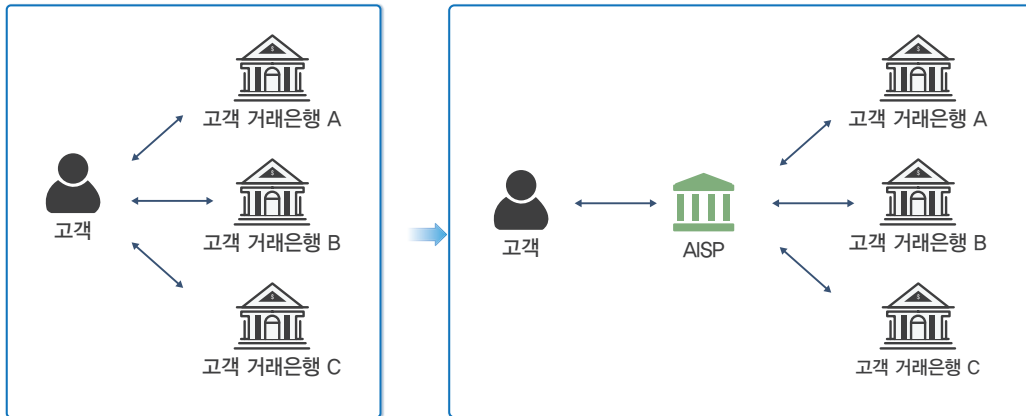
- **(제공업자 요건)** 지급결제기관(P)의 일반요건을 준용하되 자금을 보유하지 않는 특성을 고려하여 초기자본 요건을 낮추고* 동 서비스만을 제공하는 경우 자기자본 계산 대상에서 제외

* P의 경우 일반적으로 초기 자본을 최소 12만 5천 유로로 규정하고 있으나, PISP의 초기자본은 최소 5만 유로로 하고 있음

o 계좌정보서비스 제공업자 (AISP, Account Information Service Provider)

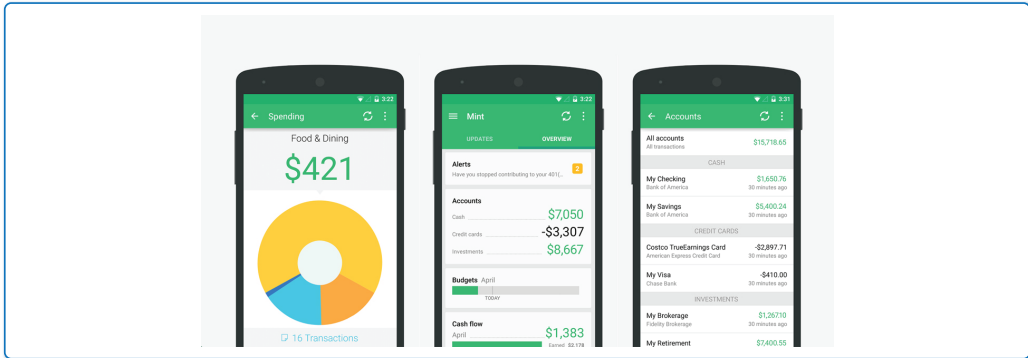
- **(서비스 개요)** 금융소비자가 거래하는 은행의 계좌정보(예금주, 계좌번호), 최근 거래내역, 잔액 정보 등의 금융정보를 통합하여 제공

〈그림 6〉 계좌정보서비스 제공업자(AISP)의 업무처리 흐름도



- **(특징)** 기업 및 개인은 자신의 재무 상태에 대한 통합된 정보를 제공받을 수 있으며, 제공업자는 해당 데이터를 활용하여 리스크관리, 교차 판매기회, 상품 추천 등 다양한 형태의 비즈니스로 확장 가능
- **(서비스 예시)** 개인명의로 금융계좌(은행·금융투자·대출 등)를 통합하고, 계좌이체 및 카드결제 내역을 통해 개인의 수입·지출을 관리하는 개인종합자산관리(PFM) 형태로 구현
- 계좌정보서비스에 지급지시서비스를 결합하여 자금의 계좌 간 연동이 가능해짐에 따라, 개인의 재무 상황 및 재무 목표에 따라 계좌정보서비스 제공업자를 통해 자산·부채 포트폴리오 규모를 조정하는 등 보다 개인화된 자산관리가 가능할 것으로 예상

〈그림 7〉 미국 개인종합자산관리서비스 “민트(Mint) “ 서비스 화면 예시



- (제공업자 요건) AISP 서비스만을 수행하는 제공업자의 경우 지급결제기관(P)이 준수해야 하는 아래 요건의 적용범위에서 제외
- 거래투명성 및 정보공개 요건(타이틀 III)과 서비스 제공 및 사용에 대한 권리·의무(타이틀 IV)의 적용범위에서도 제외되며, 최소한의 정보공개 의무만을 부담
- 소비자가 명시적으로 동의하여 지정한 계좌에 대한 정보에만 접근할 수 있으며, 이와 관련된 민감한 지급 데이터*(sensitive payment data)를 요청할 수 없음
 - * 개인의 거래보안을 침해할 수 있는 수준의 개인거래정보로 정의되며, PISP 또는 AISP에게 제공되는 계좌 소유주명, 계좌번호는 “민감한 지급데이터”에 해당하지 않음
- 유럽 개인정보보호법(GDPR)에 의거하여 소비자가 명시적으로 요청하는 목적 이외의 목적으로는 동 정보를 사용, 접근, 저장하지 못함

(참고) PSD 2에 대한 유럽 개인정보보호법(GDPR)의 입장

- PSD 2에서 지급결제서비스 제공업자는 사용자의 명시적 동의*를 얻어 서비스 제공에 필요한 정보에 한하여 접근할 수 있도록 허용하고 있음
 - * “명시적 동의”는 GDPR에 근거한 개인정보처리의 요건임
- 따라서 서비스 제공업자가 보유하게 된 개인정보를 다른 용도로 사용하고자 할 때에는 GDPR에서 규정하는 용도 제한의 원칙, 데이터 최소화 원칙 등을 고려해야 하며 구체적인 사례별로 사용가능여부를 검토해야 함

□ 또한 GDPR에서 규정하고 있는 개인정보 이동요구권은 개인정보의 목적 외 이용 또는 제3자 정보제공 등과 보다 유사한 개념임

□ 제3자 지급결제서비스 제공업자에 대한 계좌접근(access-to-account, XS2A) 허용

○ (정의) 신용기관(은행)은 TPP가 소비자 계좌에 접근하는 것을 막거나 방해하지 않도록 해야 하며 각 제공업자가 차별 없이 해당 정보를 이용 가능하도록 보장해야 함 (제36조: 신용기관이 관리하고 있는 계좌에 대한 접근)

- 2019년 3분기 중 본격 적용

- TPP가 서비스 제공을 위해 신용기관으로부터 제공받을 수 있는 정보 요건 및 범위를 지침에 별도 규정하였으며, 정보교환 방식 등은 RTS를 준용 (제66조: 지급지시 서비스에서 계좌접근에 대한 규정, 제67조: 계좌정보 서비스 시 계좌접근에 대한 규정)

- 다만 개별 지급결제서비스 제공업자는 소비자가 명시적으로 동의한 범위의 정보에 접근하여 서비스를 제공할 수 있으며, 완전한 계좌접근권을 가지는 것이 아님

〈표 4〉 제3자 기관(TPP)과 은행간 계좌접근 정보교환 정보

구분	제3자 기관(TPP)이 은행에 제공하는 데이터 (Input data)	제3자 기관(TPP)에 대한 은행의 응답
지급지시	IBAN* from, IBAN to, 거래금액, TPP ID/인증서, 인증방법	지급지시에 대한 확인, 타임스탬프 및 에러코드 확인
자금여부	IBAN, 거래금액, 거래시각, TPP ID/인증서	Yes/No 응답, 타임스탬프
잔액정보	IBAN, 조회기준(기간, IBAN to, 금액), TPP ID/인증서, 인증방법	잔액, 거래내역
계좌검증	IBAN, TPP ID/인증서, 인증방법	Yes/No 응답 (계좌 존재 여부, 유효성)
신원 정보	ID 정보(연령, 우편번호, 휴대전화번호 등)	Yes/No(연령 검증)

* 국제은행계좌번호 (International Bank Account Number)

※ 자료 : PCM research, PSD2 and Europe’s Open Banking Mandate (2017. 11)

- **(접근방식)** TPP는 은행의 인프라를 통해 고객정보에 접근할 수 있으며 RTS에서는 각 금융회사가 계좌접근 인터페이스를 위한 API를 구축할 것을 권고
 - 유럽은행감독청은 API 구축 시 ISO20022를 통신표준으로 사용할 것을 제안했으나, RTS에서는 계좌접근 권이 구현되는 방법에 대해 구체적인 지침을 제공하고 있지 않음

(3) 소비자 보호 강화 및 투명성 제고

- **(지급결제기관에 대한 인허가 요건 강화)** PSD 2에서는 지급결제기관(P) 인가 시에 기관의 보안사고 조치절차, 업무지속성 유지절차 등을 포함한 보안정책 문서를 함께 제출해야 함
 - 각 국가별로 PISP의 경우 허가제, AISP의 경우 등록제로 운영
- **(거래에 관한 정보공개 의무 강화)** PSP는 고객에게 지침에서 제시하고 있는 거래정보 및 조건을 명시하고, 서비스 제공시에 추가적인 거래정보를 공개해야 함 (제45조: 정보 및 조건)
 - 고객에게 제공하는 지급서비스와 관련된 요건(지급지시에 필요한 정보요구사항, 최대 소요시간, 수수료 등 과금체계, 참조환율 등) 명시
 - 거래지시 및 거래가 완결됨에 따라 이에 따르는 거래액, 수수료, 지급인·수취인에 대한 정보를 추가적으로 명시해야 함
- **(지급결제서비스에 대한 보안조치 강화)** PSD 2 원칙에 대한 구체적인 보안규정 및 조치를 정의하고, 이해관계자들 간 효과적인 업무처리를 위해 하위 규제기술표준(RTS)을 수립하여 2019년 9월부터 시행 예정
 - ※ 세부 내용은 연관 법령의 (1) 규제기술표준(RTS) 참고
- 분실, 도난 등 미승인(unauthorized) 거래에 대한 소비자의 책임한도를 50유로로 하향(PSD에서는 150유로 한도)하였으며, 다만 소비자에게 고의 또는 중과실이 있는 경우에는 예외 적용

라. 연관 법령

(1) 규제기술표준 (RTS, Regulatory Technical Standards)

- EBA는 PSD 2에 의거하여 동 지침의 후속조치로 지급결제서비스에 대한 보안 요구사항을 규정하는 규제기술표준(이하 "RTS")을 마련 (제98조: 인증 및 통신에 관한 규제기술표준)
 - ASPSP와 TPP 등 PSP의 사용자 본인인증방식에 대한 보안요구사항 및 이들 제공업자 간 통신방식에 대한 기술적 규제내용이 포함
 - 2018년 3월 공표되어 18개월간의 유예기간을 거쳐 2019년 9월 시행 예정이며, 개별 국가의 입법이 필요한 지침(Directive)과는 달리 직접 적용되어 별도 법률을 통해 반영할 필요가 없음
- **(강력한 고객인증(SCA, Strong Customer Authentication))** 모든 지급결제서비스 제공업자는 소비자 보호를 위하여 전자금융 개시 및 처리 시 거래자의 신원을 파악해야 함
 - **(적용범위)** 지급인의 계좌에 온라인으로 접근하는 경우, 전자지급거래를 지시하는 경우, 기타 사기나 남용의 위험이 있는 원격채널을 통해 지급결제서비스 제공 시 SCA를 적용하도록 함 (제97조: 인증)
 - PISP, AISP의 업무처리 시에도 동일한 인증방식 적용
 - **(적용제외 범위)** 일정금액 이하의 소액거래, 이상거래 모니터링을 통해 평가한 사기발생율이 기준값 이하인 경우, 무인단말기 거래, 既인증된 수취인에 대한 거래 등

〈표 5〉 SCA 적용 제외범위

- 온라인/모바일 결제 시 건당 30유로 이하(최종 인증시점 기준 누적 100유로 이하)의 소액거래
- 비접촉식(Contactless) 카드 결제 시 건당 50유로 이하의 소액거래
- 통행요금·주차요금 등 무인단말기를 통한 거래
- 인증된 수취인(Trusted beneficiary)을 대상으로 한 온라인 거래
- 전용 결제프로세스 또는 프로토콜을 사용한 법인거래
- 온라인 지급거래 계좌에 대해서는 처음 그리고 매 90일마다 인증 필요

- **(적용방식)** SCA의 방식으로 2요소 인증, 동적요소 인증을 규정하고 적용 제외범위 거래에 대해서는 적용하지 않게 하여 소비자 편의가 저하되지 않도록 함
- **(2요소 인증)** SCA가 제시하는 2가지 또는 그 이상의 요소를 사용하여 인증프로세스를 구성해야 함

〈표 6〉 2요소 인증을 구성하는 인증요소

<ul style="list-style-type: none"> ◦ 지식기반 : 고객이 알고 있는 정보(패스워드, PIN) ◦ 소유기반 : 고객이 보유하고 있는 정보(카드, 기기생성 인증번호 등) ◦ 속성기반 : 고객의 신원에 관한 정보(지문, 음성인식 등) ◦ 기타 : 거래와 연계된 특정한 인증 코드
--

- **(동적요소 인증)** 특히 원거리(인터넷·모바일) 전자지급 거래 시 중간자공격, 세션 하이재킹 등의 위험을 최소화하기 위하여 거래에서 특정되는 금액·수취인과 연동되는 동적요소를 포함하는 보다 강력한 인증방식을 적용하도록 함

□ **(개방형 통신표준(CSC, Common and Secure open standards of Communication))**

- **(명시적 동의요건 및 인증)** 소비자는 PISP 또는 AISP에게 그들의 계좌정보 또는 거래 시기에 대한 명확한 동의의사를 밝혀야 하며, 이에 대한 인증절차가 필요함
- **(안전한 통신채널)** 금융회사는 새로운 지급결제서비스 제공업자가 적절한 서비스를 제공할 수 있도록 안전한 통신채널을 통해 계좌정보에 대한 접근권을 보장하여야 함
- 금융회사와 지급결제서비스 제공업자 간 통신을 위한 API를 구축하고, 해당 통신망에 대한 다중처리(Fall-back)시스템을 구축해야 함

(참고) PSD 2의 API 방식과 스크린스크래핑 방식에 대한 입장

- 스크린스크래핑은 시스템과 통신하기 위해 전용 인터페이스인 API를 사용하지 않고, 비공식적 익명 기술을 사용하여 온라인에서 데이터를 추출하는 형태임

- RTS에서는 은행이 전용 API를 제공하는 경우 서비스 제공업자는 원칙적으로 API를 사용해야 한다는 규정을 명시하였으며, API가 존재하지 않거나 API를 30초 이상 사용할 수 없는 경우에 한해 스크린스크래핑을 허용
 - 다만 데이터무결성 및 유출을 막기 위해 제공업자는 디지털서명 필요

□ (금융사기 정보 보고)

- EBA는 지급결제서비스 사용자의 과거 소비 패턴, 거래시점의 지급인·수취인의 위치, 비정상적인 지급패턴 등을 분석하여 위험도를 계산할 수 있는 세부 내용을 제공
- 또한 개별 PSP가 제공하는 서비스 가운데 의심되는 거래에 대한 데이터에 해당 국가 규제당국뿐만 아니라 EBA도 접근할 수 있는 권한을 가짐

마. 적용사례

- PSD 2는 2018년 1월부터 시행되고 있으며 영국, 독일 등 23개국이 동 지침의 내용을 자국 법률에 반영하였고, 네덜란드, 포르투갈, 스페인 등 4개국은 조치가 이루어지지 않은 상태 (2018년 9월 현재)
 - 또한 하위 연관법령인 규제기술표준(RTS)이 시행되는 2019년 9월까지 각국의 금융회사 및 서비스제공업자는 보안체계, 데이터공유 방식, 인증 등에 대한 구체적인 기술적 조치를 마련할 것으로 예상

(1) 영국 (오픈뱅킹 UK)

- 2017년 중 PSD 2의 주요 조항을 반영하여 지급결제서비스 법률(UK Payment Services Regulations)을 개정하였으며 2018년 1월부터 발효

- 공정경쟁당국(CMA) 주도로 영국 내 9개 대형은행*이 오픈뱅킹워킹그룹(OBWG)을 조직하고 산하에 OBIE(Open Banking Implementation Entity)를 설립
 - * Allied Irish Bank, Bank of Ireland, Barclays, Danske, HSBC, Lloyds Banking Group, Nationwide, RBS Group, Santander
- 동 워킹그룹을 통해 데이터 공유, 보안 프레임워크 등 표준화된 기술규격을 협의하고 정부 주도의 오픈뱅킹 체제를 정착시키고자 함

(2) 독일

- 2017년 11월 지급서비스의 건전성 감독에 관한 법률에 PSD 2의 핵심조항을 반영하여 2018년 1월부터 발효하였으며 Bafin(금융규제기관)은 PSD 2의 적용 범위 등을 포함한 안내지침서를 발간

〈표 7〉 유럽연합 주요 회원국 PSD 2 입법 현황

국 가	적용 법률 (implementing regulations)	하위 규제지침 (regulatory guidance)
영 국	PSD2 적용법안 시행 중 UK Payment Services Regulations 2017 (2018.01.13.~)	FCA가 정책 준칙을 발간 Payment services approach document, handbook, perimeter guidance manual (PERG)
독 일	PSD2 적용 완료 - Act on the Prudential Supervision of Payment Services (2018.01.13.~)	설명집과 가이드라인*을 발간 * UK PERG와 유사
프랑스	PSD2 적용 완료 - 법령 배포 (2017.08.10.) - 7개의 시행령 배포 (2017.09.02.)	별도 하위 지침은 없음
이탈리아	2차 시행규칙 초안 발간상태 1차 법령은 시행 중	기존의 PSD 지침을 변경할 것으로 예상
네덜란드	법령 초안이 하원 승인 대기 중 상원 통과 시 시행가능	별도 하위 지침은 없음
스페인	2018년 하반기 스페인 의회에서 승인예정	별도 하위 지침은 없음

(3) 베를린그룹

- 베를린그룹은 EU 내 주요 은행, 협회, 지급결제서비스 제공업자 등으로 구성되어 있으며, 역내 지급결제 관련 표준 등을 제정하기 위한 일종의 표준화기구임
- 베를린그룹에서는 PSD 2에 제시된 사례에 대해 “NextGenPSD2”라는 공통의 API 표준을 정의하고 계좌접근권(XS2A)에 필요한 보안 규칙 및 지침 등을 제정하여 배포하고 있음

III. PSD 2 시행이 금융권에 미치는 영향

가. 유럽연합 내 금융회사

□ 신용기관(은행 등)

○ 신규 PSP의 금융시장 진입 및 계좌접근 허용에 따른 영향

- 지침에서는 은행이 소유하고 있던 고객의 계좌정보 및 결제프로세스를 API 방식을 통하여 제3자 지급결제서비스 제공업자 등에게 제공하도록 권고하였으며 이는 EU내 오픈뱅킹을 가속화
- **(긍정적 전망)** 전통적인 금융회사는 기존 금융시스템 운영을 통한 노하우와 신뢰, 두터운 기존 고객층을 바탕으로 비즈니스 확장 가능
- ① 비즈니스 모델 발굴 : 기존의 금융회사(ASPSP) 또한 PSD 2에서 새롭게 허용하고 있는 지급결제서비스를 동일하게 수행할 수 있으므로 이를 통한 통합된 형태의 지급결제·자산관리 서비스 제공
- ② 수익창출 기회 포착 : 은행이 보유하고 있는 고객 데이터와 IT기업이 가지고 있는 데이터 분석 능력을 활용하여 고객 리스크관리, 고객맞춤형 교차판매 등 수익 창출 가능

〈표 8〉 은행 등 신용기관의 비즈니스 확장모델 예시

(소매금융)

계좌통합관리서비스	▶	계좌를 통합관리, 수입·비용 추적, 재무목표 설정
P2P 지급결제	▶	계좌를 통한 자금이체
소비자-판매자 지급결제	▶	계좌를 통한 자금이체 (온라인, 오프라인POS)
상품	▶	은행상품
교차판매	▶	비은행상품
라이프스타일 어플리케이션	▶	대출 또는 투자상품 권유
인증 서비스	▶	보험 또는 신용카드 등 권유
	▶	소비자의 금융, 모기지, 보험 및 투자측면을 통합하여 보여줌 대체 결제수단 제공 가능
	▶	디지털 인증수단 제공

(기업금융)

재무상태표 시뮬레이션	▶	재무상태표, 손익계산서 등 시뮬레이션
계좌통합관리	▶	기업의 계좌 통합조회 및 관리
현금관리	▶	현금 관리를 통한 유동성 관리
리스크 관리	▶	다계좌 관리를 통한 대출 리스크관리

※ 자료 : McKinsey & company, PSD2: Taking advantage of open-banking disruption (2018.01)

- (부정적 전망) 기존 금융회사의 서비스를 ICT, 네트워크를 기반으로 하는 핀테크 기업들이 기능별로 제공하면서 금융서비스가 분화(unbundling)되어 고객접점 상실 위험 존재

① 대체 금융상품·서비스 등장에 따른 고객 이탈 : 지급결제, 송금, 대출, 자산관리 등 기존 금융회사의 기능을 대체하는 상품·서비스가 비금융회사에 의해 제공되어 은행을 경유하지 않는 거래 발생

· 서비스 분화가 심화되는 경우 고객 접점의 서비스는 제3자 업체가 제공하고 은행의 역할은 계좌관리로 한정될 가능성도 존재

② 금융소비자와의 단절로 인한 수익 감소 : 고객 접점을 활용한 교차판매 채널을 상실함에 따라 수익 약화 가능성

· 핀테크업체가 빅데이터, 인공지능 등을 활용하여 고객 편의성을 극대화하고 보다 개인화된 금융상품 및 서비스를 제공함에 따라 교차판매의 기회는 축소될 것으로 전망

- 기존 은행들은 소규모 신생은행(Challenger bank) 또는 비금융회사와 같은 금융서비스 부문 신규진입자에 대응하여 자체 API를 개발하여 banking서비스를 오픈하거나 비금융업체와 직접 제휴하는 등 다양한 전략을 구사할 필요

○ 소비자 보호 강화 및 투명성 제고에 따른 영향

- (가격경쟁 심화에 따른 수익 감소) 지침의 제1단계인 거래투명성 강화 조치(2018.01) 시행에 따라 은행이 제공하는 서비스에 수반되는 각종 수수료·비용을 명시해야 하며 이는 가격경쟁을 심화
 - 로보어드바이저, 비대면상품가입 등 보다 저렴하고 편리한 금융상품·서비스로의 대체가 용이해져 시장내 가격하락 압박, 출혈경쟁으로 이어질 가능성 존재
- (관리비용 증가) 규제기술표준(RTS)에서 요구하는 지급결제서비스의 인증·보안 방침을 준수하고, 새로운 지급결제서비스 제공업자 진입으로 인한 리스크 관리에 따른 비용 증가 예상
 - 기존 은행은 강력한 고객인증방식을 구축하고 이를 지속적으로 유지·관리하여야 함
 - PISP, AISP에게 제공할 인터페이스(API)를 개발하는 등 개방통신표준 등을 준수하기 위한 관리비용이 증가할 것으로 예상

□ 신용카드업자

- (계좌간(A2A)지급거래로 인한 시장 축소) PISP를 통한 계좌간 지급결제가 가능해짐에 따라 SEPA 즉시계좌이체서비스*와 결합하여 EU내 카드 발급·매입 비즈니스를 잠재적으로 잠식할 가능성
 - * SEPA 즉시계좌이체서비스(SEPA Instant Credit Transfer, SCT Incl)는 2017년 11월 개시된 서비스로 단일유로지급결제지역(SEPA) 내 금융기관간 15,000유로까지 실시간 계좌이체가 가능하도록 한 서비스
- 다만 카드매입사(비자, 마스터)의 경우 전자상거래업자 또는 지급결제서비스 제공업자에게 카드결제 솔루션을 개발·제공하여 카드네트워크를 활성화할 수 있음
 - 자체 결제수단을 구축하기 어려운 소상공인을 대상으로 SCA 프로세스 등을 포함한 솔루션을 저렴한 비용으로 공급하여 보다 쉽게 지침을 준수할 수 있도록 하는데 초점

나. 유럽연합 내 비금융회사

□ 전자상거래업자

- **(대금결제에 따른 거래비용 절감)** 재화 및 서비스 판매에 따른 대금이체 프로세스를 계좌기반으로 손쉽게 구현할 수 있어 카드 등 여타 지급결제수단을 대체함으로써 거래비용 절감 가능
- **(소비자 정보를 활용한 빅데이터 모델 구축)** 구매 및 결제 프로세스에 대한 정보를 전자상거래업자가 보유함으로써 고객의 소비 패턴이나 구매성향 등을 파악하여 빅데이터를 활용한 마케팅이 가능
 - ※ 중국 전자상거래 기업의 경우 빅데이터 마케팅에 활용하는 데이터를 온·오프라인에서 사용되는 모바일 결제 플랫폼을 활용하여 축적
- **(규정 준수를 위한 간접비용 증가)** 전자상거래업자가 지급지시서비스를 제공하는 경우에는 PSD 2 규정을 준수해야 함
 - 동 지침에서 요구하는 강력한 고객인증, 배상책임보험 가입, 금융회사와의 데이터 공유를 위한 인프라 구축 등 간접비용이 증가
 - 또한 카드매입사(비자, 마스터 등)를 통해 결제가 이루어지는 경우에는 매입사가 구축한 보안정책(CV2, 3D secure)을 준수해야 하므로 보안정책을 능동적으로 결정하지 못함

□ 플랫폼기업

- **(생태계 구축을 위한 금융업 진출 기반 마련)** 검색엔진, 소셜네트워크, 제조업체 등 플랫폼 사업자들은 자체 비즈니스 생태계를 구축하고자 금융업 진출에 적극적인 상황
 - 사업자들은 핵심 콘텐츠 및 네트워크를 기반으로 하여 사업범위를 지급결제, 송금, 카드 등 금융서비스로 확장하고 있으며, PSD 2를 통해 플랫폼기업과 같은 TPP도 규제 범위 내에서 사업 영위 가능
 - 다만 금융서비스에 수반되는 운영·신용리스크 관리 역량을 내재화하고 보안·인증에 대한 소비자의 신뢰를 확보하는 것이 중요

□ 핀테크업체

- (금융서비스 시장 진입여건 개선) 당국의 인·허가, 감독규정 등 기존 지급결제서비스 제공업체와 동일한 규제 하에서 사업을 영위할 수 있으며, 지침범위 내 고객 계좌 등 금융정보에 대한 접근이 가능
- (혁신적인 지급결제 및 금융서비스 제공) 개인의 금융정보를 활용하여 업권(은행·증권·카드 등)별 정보를 통합하고, 이종업권간 데이터를 결합하여 개인화된 서비스를 제공함으로써 소비자 편의 제고

〈표 9〉 금융정보를 활용한 혁신서비스 예시

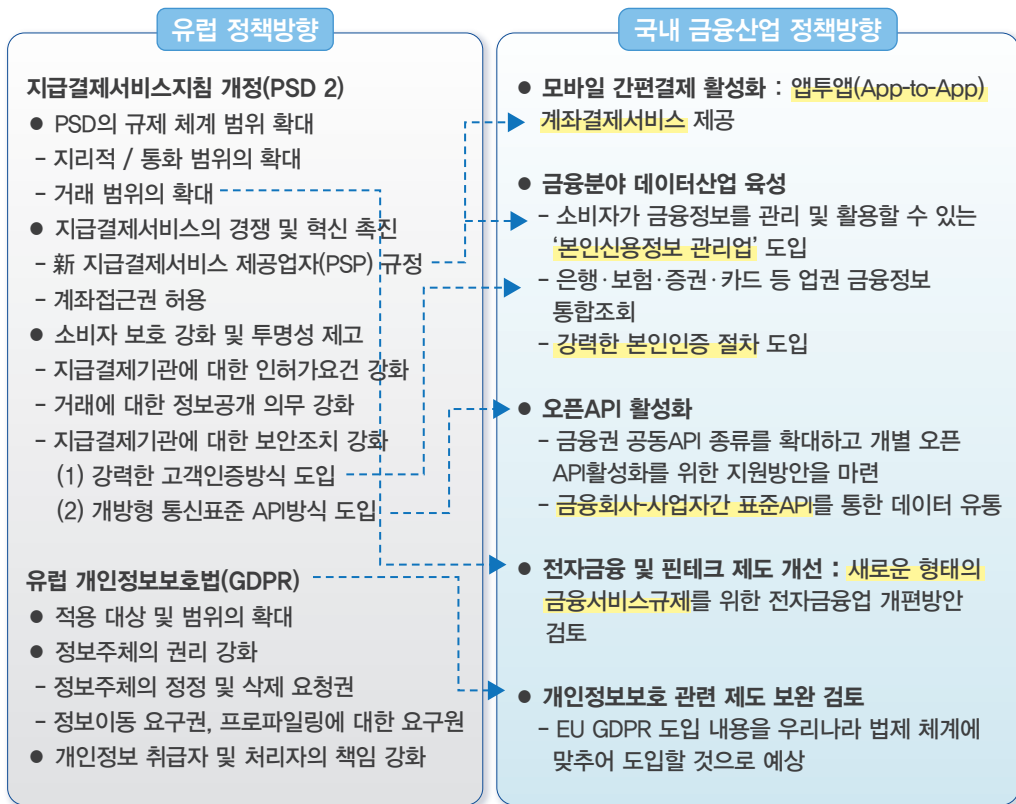
구분	활용영역	활용방안
금융업	금융상품 추천	◦ 금융권 정보를 통합 조회하여 예·적금, 대출 등 금융상품을 추천 (고객접점 확대)
	금융상품 개발	◦ 소비패턴, 자산현황 등의 금융정보를 활용하여 고객에 맞는 맞춤형 금융상품 개발
	상품가입 프로세스 개선	◦ 금융상품 가입 시 필요한 정보를 기 입력정보 또는 관련 기관 등으로부터 수신하여 가입 프로세스 개선 및 소요시간 단축
	신용평가모델 개발	◦ 개인의 지출내역, 금융상품 등을 활용하여 신용평가모델 고도화
비금융업	유통	◦ 타겟 마케팅, 제휴 금융상품 추천에 활용
	게임	◦ 앱 내 송금 및 결제기능 구현
	의료	◦ 의료 및 소비패턴을 활용한 개인별 맞춤 보험 추천
	부동산	◦ 개인 대출현황 및 상품정보 연동으로 담보대출 연계

다. 국내 금융권에 미치는 영향

- 국내 금융회사에 미치는 직접적인 영향은 제한적이거나, PSD 2의 시행으로 인한 금융서비스 및 산업의 지형 변화는 국내 금융권의 다양한 이해관계자에게 작-간접적인 영향이 있을 것으로 판단
 - 따라서 정책적·기술적·산업적 측면에서 국내 금융회사 및 금융서비스 제공업자, 금융소비자 등에 미치는 영향을 분석
- **(정책적 측면)** 금융당국은 효율적·안정적 금융서비스 제공을 위하여 다양한 정책을 입안하고 있으며, 이는 PSD 2 등 최근 유럽권의 정책방향 흐름과 유사한 것으로 판단됨
 - **(모바일 간편결제 활성화)** 전자금융업자 및 인터넷전문은행 등 금융회사가 애플투애플(App-to-App) 계좌결제 서비스*를 제공하도록 기반 조성
 - * 물품대금 결제 시 구매자-판매자간 앱을 통해 계좌이체 방식으로 결제하는 방식으로 일종의 계좌간(A2A)지급거래 방식임
 - **(금융분야 데이터산업 육성)** 금융 분야 빅데이터 활성화를 위한 신용정보산업의 진입규제 완화 조치로 소비자가 자신의 금융정보를 능동적으로 관리 및 활용할 수 있는 '본인 신용정보관리업' 도입
 - 2018년 7월중 '금융분야 마이데이터 도입방안'을 발표하여 신용정보법 개정을 통해 하반기 중 입법을 추진할 예정이며, 마이데이터 사업자는 PSD 2의 AISP 개념 및 유형과 유사
 - 금융소비자의 은행·보험·증권·카드 등 업권별 금융정보를 통합조회할 수 있도록 하고 강력한 본인인증 절차 도입 등을 통해 편리하고 안전한 데이터 유통에 초점
 - **(오픈API 활성화)** 금융권 공동API 종류를 확대하고 개별 오픈API 활성화를 위한 지원방안을 마련
 - 상기 '마이데이터 산업 도입방안'에서 금융회사와 사업자간 데이터 제공방식으로 표준API를 활용함으로써 개별 금융기관에 API 구축 의무를 부여할 예정
 - 다만 정보중계·유통 및 집적기관을 통해 구축된 기존의 인프라를 이용하여 오픈 API를 제공하는 방법도 고려할 필요

- (전자금융 및 핀테크 제도 개선) 새로운 형태의 금융서비스를 제도권으로 편입하고자 전자금융업 개편방안 등을 2018년 중 검토할 예정
- (개인정보보호 관련 제도 보완 검토) 현행 개인정보보호법에 대한 개정 검토를 2019년 중 수행할 예정
 - 유럽 개인정보보호법(GDPR)에서 새롭게 도입된 정보주체의 정보이동요구권, 프로파일링에 대한 거부권 등을 우리나라 법제 체계에 맞추어 도입할 것으로 예상

〈그림 8〉 유럽 및 국내 금융산업 정책방향 비교



* 금융위원회의 〈핀테크 혁신 활성화 방안〉(2018.03) 재구성

- 따라서 금융회사 또는 금융서비스를 제공하고자 하는 사업자들은 EU 등 주요국의 금융산업 규제 및 정책 입안 방향에 주목할 필요

- **(기술적 측면)** 금융기관간 또는 금융기관·비금융회사간 금융정보의 유통이 활발해지며 이에 대한 정보보호, 보안, 인증 등 기술적 규제에 대한 논의 대두
 - 특히 PSD 2 및 GDPR에서는 개인의 금융정보 활용 및 유통을 촉진하는 동시에 이에 대한 관리·보호 조치를 강화하고 있어 이를 구현하기 위한 오픈 API 및 인증 기술에 대한 구체적인 논의가 진행중
 - **(오픈 API 방식을 활용한 데이터 보안 강화)** 금융회사가 금융정보 제공 시 전용 인터페이스를 구축하도록 하고, 데이터 송수신 접근권한 및 거래 인증에 대한 기술 표준, 보안 조치를 구현해야 할 필요
 - 이는 고객의 인증정보를 직접 저장하여 대리 접속하는 기존의 스크린 스크래핑 방식을 제한*하고, 보다 표준화·정형화된 형태로 데이터 유통을 허용함으로써 관리·감독이 용이하도록 하는 것이 목적
 - * 한편 고객의 인증정보를 보관하지 않는 클라이언트형 스크래핑 등 보안성이 검증된 형태의 스크래핑 방식을 허용하는 방안은 논의 중
 - 따라서 금융분야 마이데이터 산업(본인신용정보관리업) 신설과 관련하여 오픈 API 방식에 대한 구체적인 보안 원칙, 고려사항을 신용정보업감독규정 등 하위 법령을 통해 규제할 가능성 존재
 - 일본의 경우 은행권 오픈 API 적용을 위해 위원회를 구성하여 API 접속, 인증 범위, 메시지 전송방식 관련 보안 원칙을 제시

〈표 10〉 일본은행연합회(JBA)의 은행권 오픈 API 보안 원칙

보안 원칙	주요 내용
제3자의 자격적합성 평가	사전평가, 사후 모니터링
외부 무권한 접근 방지 대책	접근권한 부여 관련 인증, 접근권한토큰 관리, 개별 거래 관련 인증, 통신방법, 시스템 견고성
내부 무권한 접근 방지 대책	은행/제3자의 내부 무권한 접근 방지 대책
무권한 접근 대응	시스템 설계·규격, 정보공유 및 대책 토론
보안대책 개선·검토·강화	보안대책의 지속적 개선, 검토 및 강화

※ 자료 : 금융보안원, EU PSD2 규제기술표준 및 일본 은행 오픈API 보안원칙 소개(2018. 5)

- **(금융소비자 보호를 위한 고객인증 강화)** 현행 전자금융거래법은 금융회사 및 전자금융업자에게 비대면실명확인 등을 통하여 강력한 고객 인증(SCA)과 유사한 수준의 고객확인 요건 등을 규정하고 있음
 - 다만 개인신용정보관리업자 등 제3자에게 금융정보를 유통하는 경우에는 동 사업자에 대해서 본인 인증을 의무화하는 동시에 개인의 인증정보는 보유·활용할 수 없도록 하고 있음
- **(금융데이터 중계를 위한 표준 및 규칙 설계)** 보다 효율적인 금융정보 유통을 위한 사용자 인증방식, 통신방식 관련 기술표준을 확립하여 업권간, 기관간 호환성 제고 필요
- **(산업적 측면)** 제3자에 대한 계좌접근 보장으로 새로운 형태의 금융서비스가 등장하여 금융산업의 범위가 확장되었으며, 업권간 경계 또한 모호해짐에 따라 다양한 서비스를 아우를 수 있는 법률·규제 등 산업적 기반 필요
- **(개인신용정보 이동권 도입)** 금융회사가 계좌정보 등 금융정보를 제한적인 목적·범위에서 허용하던 것과는 달리 정보주체가 자신의 금융·신용정보를 적극적으로 관리하고 활용할 수 있도록 보장

〈표 11〉 금융분야 개인정보 관련 법률

구분	소관법령	개인정보 관련 내용
일반법	개인정보보호법	<ul style="list-style-type: none"> ◦ 개인정보는 특정 개인을 알아볼 수 있는 정보로, 금융거래가 없는 고객정보를 포함 ◦ 특별법 적용대상이 아닌 모든 형태의 개인정보
특별법	신용정보법	<ul style="list-style-type: none"> ◦ 거래 상대방(개인기업)의 신용도 판단에 필요한 정보(금융거래기록 등) ◦ 개인신용정보는 개인의 신용도 및 신용거래능력 등을 판단할 수 있는 정보로 신용정보법을 우선 적용
	금융실명법	<ul style="list-style-type: none"> ◦ 금융실명 거래정보 등은 제한된 범위 내에서만 그 내용을 제공할 수 있음 (제4조 제1항)
	전자금융거래법	<ul style="list-style-type: none"> ◦ 전자금융거래와 관련한 업무 수행에 있어 이용자의 인적사항, 이용자의 계좌, 접근매체 및 전자금융거래에 관한 정보 또는 내용 (제26조) ◦ 금융실명법에 보장된 내용은 금융실명법이 우선

※ 자료 : 금융감독원, 금융분야 개인정보보호 가이드라인 개정본 (2017.02) 및 관련 법령

- **(금융정보 제공·활용에 대한 동의여부 관리 필요)** 개인의 계좌 및 금융정보에 대한 제3자 접근이 허용되면서 정보주체가 자신의 신용정보 제공·활용에 대한 동의여부를 관리할 수 있는 도구 필요
 - 개인신용정보의 수집·제공 시 필수와 선택사항을 구분하여 항목별로 정보주체의 동의를 받도록 하고 있음 (옵트인(Opt-in)방식)
 - 따라서 다수의 기관으로부터 수집된 신용정보가 본인신용정보관리업자 등에 제공되는 경우 하나의 채널을 통해 개인신용정보의 이용·제공내역을 조회하고, 개별 기관에 대한 동의여부를 선택·철회가 가능하도록 구현하는 것이 필요

- **(핀테크 관련 업종 범위 확대 및 규제 일원화)** 전자금융업자·보조업자 등 지급결제서비스를 제공하는 다양한 제공업자는 현행 업종별 혹은 지급수단별 법률의 규제를 받고 있음
 - ※ 은행(은행법), 신용카드사(여신전문금융업법), PG사(전자금융거래법), 이동통신사(전기통신사업법) 등
 - 다만 새로운 형태의 지급수단·서비스의 경우 열거주의(positive)형 규제로 인해 준수해야 하는 법령을 명확하게 지정하기 어려워, 핀테크 관련 규제의 업종 범위를 확대하거나 포괄주의로 전환할 필요
 - 또한 현행 업권별 인·허가, 감독체계 하에서는 서비스 모델에 따라 소관 법령 및 준수 의무사항 등이 차이가 있어 이를 기능 중심의 규제로 재편할 필요

IV. 시사점

- PSD 2는 핀테크·ICT기업 등 비금융회사가 고객의 금융정보에 접근하도록 허용하고, 기존의 금융회사와 동일한 규제 하에서 사업을 영위할 수 있는 지위를 부여한다는 점에서 금융의 패러다임을 크게 변화
 - 국내·외 금융 및 지급결제시장은 소비자의 편의성과 안전성을 우선으로 하는 혁신적인 금융서비스에 의해 주도되고 있으며 2019년 중 PSD 2가 본격적으로 시행됨에 따라 이러한 추세는 가속화될 전망
- 유럽연합 내 금융회사는 서비스 제공에 있어 독점적인 지위를 유지하기 어려워짐에 따라 기존의 사업기반을 바탕으로 비즈니스 모델을 발굴하는 등 신규 성장동력을 마련하기 위한 전략을 구사할 필요
 - 동시에 EU의 사례와 같이 신규 시장진입자에게 효율적으로 대응하고 개발 부담을 경감하고자 금융회사 간 협의체를 통하여 기술요건에 대한 표준을 제정하는 등 업권 간 공동대응의 필요성도 존재
 - 따라서 국내 금융회사 또한 PSD 2와 같은 해외 정책 사례 등을 기반으로 금융업의 진입장벽 완화 및 금융 서비스의 분화에 선제적으로 대응할 필요가 있다고 보여짐
- 아울러 향후 PSD 2 등 해외 정책사례의 지속적인 모니터링을 통하여 소관 업무와의 연관성을 살펴보고, 이를 선제적으로 검토하여 금융당국의 정책 입안과정에서 적시에 반영될 수 있도록 노력할 필요

[참고 문헌]

- 금융보안원, PSD2 규제 기술 표준 주요 내용 및 시사점, 2018. 05
- 금융보안원, EU PSD2 규제기술표준(RTS) 및 일본 은행 오픈API 보안 원칙 소개, 2018. 05
- 금융위원회, 금융분야 개인정보보호 가이드라인, 2016. 12
- 금융위원회, 핀테크 혁신 활성화 방안, 2018. 03
- 금융위원회, 금융분야 데이터 활용 종합방안, 2018. 03
- 금융위원회, 금융분야 마이데이터 산업 도입 방안, 2018. 09
- 한국금융연구원, EU 지급결제서비스지침 개정(PSD2)의 시사점, 2016. 12
- Deloitte, Open banking: How to flourish in an uncertain future, 2017. 06
- European Banking Federation, PSD2 Guidance: Guidance for implementation of the revised Payment Services Directive, 2016. 10
- McKinsey & company, PSD2: Taking advantage of open-banking disruption, 2018. 01
- PAYON, Driving change with PSD2 and the MIF regulation: creating opportunities in europe, 2016. 05
- PCM research, PSD2 and Europe's Open Banking Mandate, 2017. 11
- TEMENS, Payment Services Directive 2(PSD2), 2016. 11