금융감독원	**보 도 자 료**	금융보안원 FINANCIAL SECURITY INSTITUTE

보도	2023.10.5.(목) 10:10	배포	2023.10.4.(수)

담당 부서					
	금융감독원 디지털금융혁신국 디지털금융총괄팀	책임자	국 장	김부곤	(02-3145-7120)
		담당자	팀 장	안태승	(02-3145-7125)
	금융보안원 금융보안관제센터	책임자	센터장	김영태	(02-3495-9300)
		담당자	팀 장	이신일	(02-3495-9370)

전자금융사고 예방을 위해 「이상금융거래탐지시스템(FDS) 운영 가이드라인」을 마련하였습니다.

'23.10.5.(목), **금융감독원**과 **금융보안원**은 전자금융사고 예방을 위해 **「이상금융거래탐지시스템(FDS) 운영 가이드라인」**을 **발표**하였습니다.

비대면 금융거래가 지속적으로 확대됨에 따라 사고예방을 위해 은행권을 중심으로 이상금융거래 탐지시스템(이하 'FDS')을 자체 구축·운영 중입니다.

그러나, 금융거래에 대한 외부 위협이 계속해서 확대되고, 지능화되는 추세를 보임에 따라 업계가 **공동으로 대응할 필요성**이 증대되었고, 이에 금감원 및 금보원은 업계 **T/F를 구성**하여 **「FDS 운영 가이드라인」 마련**을 준비해 왔습니다.

※ [참고1] 그간의 T/F 논의 경과

◈ 금융감독원은 금융보안원 및 주요 7개 은행과 함께 '22.12월부터 'FDS운영 가이드라인' 제정을 위한 T/F를 구성·운영해 왔으며,

○ TF 실무회의(4회) 및 전체은행 실무자 간담회(4회) 등을 통해 FDS 적용범위, 운영 프로세스 및 주요 피해유형별 탐지조건 등을 담은 가이드라인을 마련

※ [참고2] 「FDS 운영 가이드라인」의 성격

◈ 동 가이드라인은 법령·행정지도 등 금융규제에 해당하지 않으며, 금융회사의 전자금융사고 예방을 위해 업계의 모범사례(Best Practice) 등을 취합하여 마련·권고한 것으로 금융회사의 가이드라인 적용여부는 회사판단의 자율사항임

동 가이드라인은 FDS 운영 전반에 대해 정의하고 있으며, 주요 피해 사례를 고려한 **시나리오 기반의 '이상거래탐지룰'(51개)과 대응절차** 등을 포함하고 있습니다.(붙임 참고)

< 가이드라인 주요 내용 >

□ **(대상)** 전자금융서비스를 제공하는 **국내은행**

□ **(적용 업무범위)** 전자금융거래의 **시작단계**부터 **수행 및 종료**에 이르기까지 **전자금융거래 진행과 관련된 모든 업무**

○ 금융회사의 앱(App)상 인증서 등 **접근매체 발급·갱신**, **금융서비스 로그인**과 같은 절차에서부터, 금융거래 **지시·승인 및 서비스 로그아웃** 절차까지를 **포괄**

<FDS 적용업무의 범위>

□ **(FDS 운영 프로세스)** FDS 탐지기법을 통해 **의심거래 탐지후**, 이를 **분석**하고 **대응**하는 **일련의 과정**을 수행

○ 은행 거래 데이터에서 ❶의심거래건을 **탐지**하고 ❷이상금융거래 여부를 **분석**하여 최종적으로 금융소비자를 보호하는 ❸**대응** 절차를 수행

<FDS 운영 프로세스에 따른 데이터 변화 과정>

기대효과 1

앞으로, 국내 은행업권에서는 주요 피해유형이 반영된 '**이상거래탐지룰**'이 **공통 적용**되고, 이에 더하여 개별 은행의 거래특징 등을 반영한 **자체 탐지룰**이 **추가적으로 적용**되어 전자금융거래의 **안정성이 크게 높아질 것**으로 기대됩니다.

기대효과 2

특히, 유출된 피해자의 개인정보를 악용하여 별도의 휴대전화(일명 '대포폰')를 개통한 뒤 **ARS, SMS 등의 본인확인 절차를 우회**하는 수법이 빈번하게 사용됨에 따라, 관련 의심거래 시나리오에 의해 탐지 시 **아웃바운드 콜, 화상통화, 생체인증 등** 보다 **강화된 본인확인 방법을 권고**하여 유관 피해 예방을 도모하였습니다.

기대효과 3

뿐만 아니라, 금융회사가 악성앱이 설치된 단말기를 통해 의심거래가 발생하는 등 **이상금융거래**로 판단할 수 있는 **합리적인 근거**가 있는 경우 **즉각 해당 계좌를 거래정지** 할 수 있도록 안내하여, 금융회사의 **이상금융거래에 대한 조치 강화**를 유도하였습니다.

한편, 강화된 FDS가 적용되면서 이상거래 여부를 확인하기 위해 일시적으로 거래 정지되는 일부 정상거래가 발생할 수 있으나, 신속한 확인 절차를 거쳐 즉시 해제되게 됩니다.

금감원 및 금보원은 앞으로도 「**FDS 운영 가이드라인**(공동이상거래탐지룰)」에 대한 **업계의 피드백을 지속적으로 반영·개선**할 예정입니다. 이를 통해서, 이후 **새로운 위협 발생시에도** 그에 대한 업계 전반의 **대응력이 향상되어** 금융분야의 **전자금융거래 안전성이 한층 강화**될 것으로 **기대**합니다.

※ 「FDS 운영 가이드라인」 적용시 예상 효과(예시)

구 분	피해 사례	적용 후
【본인 확인 강화】 **휴대폰 탈취 / 대포폰 활용 대응**	ARS 또는 SMS 추가인증 시, **본인 여부와 관계없이** 기기 확보자가 **추가인증 통과 가능**	IP가 해외이거나, 새로운 기기로 접속을 시도하여 의심거래로 확인되면 **추가인증***을 **필수 진행** * 본인확인 강화를 위해 **아웃바운드 콜, 화상통화** 또는 **생체인증** 등을 적극 권고 [은행별 단계적 추진]
【스미싱 → 대출】 **악성앱(원격제어) / 대출 연계**	스미싱 사기문자 클릭후 악성앱 설치, 대출실행 후 타인계좌 이체	탐지룰(**악성앱 + 대출실행후 단시간내 타인계좌이체**) 확인후 **(자동) 거래정지** 등 조치

붙 임 이상거래 탐지룰(Rule-Set) (예시)

※ 탐지룰은 비공개 자료이기 때문에 이해를 돕기 위해 일부만 소개

□ 시나리오 기반의 탐지조건으로 **세부 임계치(값) 설정** 등은 금융회사의 **고객 및 거래특징** 등을 **감안**하여 **개별 회사별**로 **적용**

시나리오 명	**과거에 사용하지 않았던 단말기를 이용하여 짧은시간동안 특정금액 이상을 이체한 경우 탐지**
피해사례	□ 공격자가 보이스피싱을 통해 피해자 이용 단말기로부터 개인정보 획득, 별도 개통한 대포폰에서 해당 정보를 이용하여 뱅킹앱에 접속, 자금 탈취
탐지룰 및 대응 시나리오	□ **(의심거래 탐지)** ❶기존 미사용 단말에서 ❷특정 금액 이상을 ❸기존에 거래한적이 없는계좌로 (단시간에) 송금하는 경우 의심거래로 탐지 □ **(확인 및 대응)** ① FDS 탐지 이후, 고위험군으로 분류, 본인 거래 확인을 위해 추가인증 실시(아웃바운드콜) ② 특정 횟수 이상 전화 미수신 또는 통화 내용 상 사고로 판단될 경우, 전자금융거래 차단 등록 ③ 차단 통지 및 사고신고 접수 안내(SMS) ④ 사후 모니터링 하여, 필요시 이상거래 정보 공유

시나리오 명	**미성년자 또는 고령자 보유 계좌에서 단시간 내 과거에 거래내역이 없던 계좌로 소액 다수 이체 탐지**
피해사례	□ 신분증 등 개인정보유출 된 고령자 또는 미성년자 계좌에 접근하여 평소 이체하지 않던 계좌로 다회 이체
탐지룰 및 대응 시나리오	□ **(의심거래 탐지)** ❶미성년자 또는 특정 나이 이상 고객 계좌에서 ❷단시간 내 ❸최초 입금 계좌로 ❹특정 횟수 이상 이체 시 의심거래로 탐지 □ **(확인 및 대응)** ① FDS 탐지 이후, 본인 거래 확인을 위해 아웃바운드콜 등 추가인증 실시 ② 추가인증 미실시의 경우, 거래차단(이용제한) 등록 ③ 차단사실 및 차단 해지 요청 방법 통지(카카오톡 및 SMS)