개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2023-017-216호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치 등에 관한 건

피 심 인

대표이사

의결연월일 2023. 10. 25.

주 문

1. 피심인에 대하여 다음과 같이 과징금 및 과태료를 부과한다.

   가. 과 징 금 : 906,000,000원

   나. 과 태 료 : 16,200,000원

   다. 납부기한 : 고지서에 명시된 납부기한 이내

   라. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대한 과태료 부과의 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 조사 개요

1. 조사 배경

개인정보 보호위원회(이하 '위원회')는 (이하 '피심인')이 자신이 제공하는 서비스에서 송금 기능 해킹, 내부직원 이메일 피싱 및 크리덴셜 스터핑 공격 등을 통해 이용자의 개인정보가 유출되었다고 신고[1]해옴에 따라 사실관계 확인 및 조사에 착수하였다.

2. 피심인 현황

피심인은 온라인 송금 등 온라인 지불 서비스인 을 한국을 비롯한 다수 국가의 이용자에게 제공[2]하면서 개인정보를 수집·이용하고 있는 「개인정보 보호법」[3](이하 '보호법')에 따른 개인정보처리자이자 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른 정보통신서비스 제공자에 해당하며 사업자 일반현황 및 최근 3년간 재무현황은 아래와 같다.

< 사업자 일반현황 >

사업자등록번호 (법인등록번호)	설립일자	대표자	상시 종업원 수	자본금
				-
주소				

< 최근 3년간 재무현황 >

(단위 : 백만 달러)

구 분	2019년	2020년	2021년	평 균
전 체 매 출 액				
관 련 매 출 액[4]				

1) 송금 기능 해킹 및 내부직원 이메일 피싱 관련 2021.12.7. 신고, 크리덴셜 스터핑 공격 관련 2023.1.2. 신고
2) 피심인은 미국·유럽을 제외한 다수 국가에 서비스를 제공하고 있으며, 미국은 유럽은 이 서비스를 제공
3) 피심인의 위반행위는 2023.9.15. 전 종료되어 보호법은 [법률 제16930호, 2020.2.4., 일부개정]을 적용(이하 '舊 보호법'), 시행령은 [대통령령 제32813호, 2022.7.19., 일부개정]을 적용
4) 한국 이용자 추정 비즈니스 계정(상품·서비스 대금 수령 등) 및 개인 계정(상품·서비스 구매 등)에서 발생한 매출액을 합산

서비스의 한국 이용자 수는 명[5]이고, 이용자는 개인 프로필 및 계정을 생성하는 과정에서 핸드폰 번호, 이메일 주소, 이름, 국적, 생년월일, 운전면허증 혹은 여권(고유 식별정보 포함), 주소(우편번호, 도로명 주소 포함), 비밀번호를 입력하며, 계정 생성 후, 계정과 신용카드를 연결하여 쇼핑, 결제 등 서비스를 이용할 수 있다.

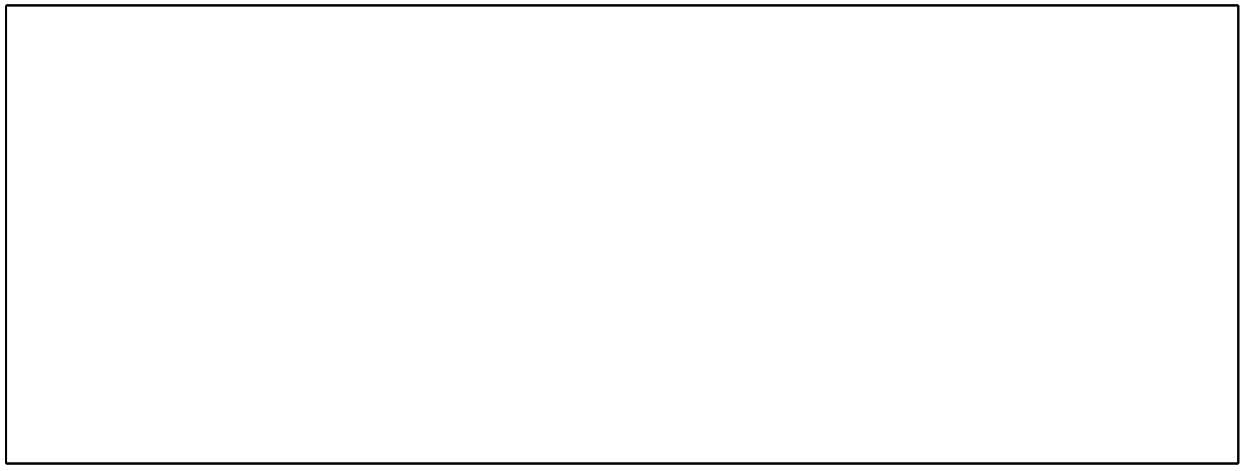
Ⅱ. 사실조사 결과

1. 개인정보 유출 관련 사실관계

가. 송금 기능(API Call) 해킹 관련

신원미상의 자(이하 '해커')는 3개의 가맹점 계정을 생성하여 에 접속하였고, 불특정 전화번호 또는 이메일을 송금 기능(Send Money API Endpoint[6])에 입력(이하 'API Call')하여 서버로부터 해당 전화번호 또는 이메일에 해당하는 이름, 국가코드, 프로필 사진을 유출하였고, 이로 인해 핸드폰 번호 혹은 이메일 주소에 연결된 이름, 국가코드가 유출된 한국 이용자는 22,067명이고, 프로필 사진이 유출된 이용자는 1,185명이다.

<참고1> 송금 기능 해킹을 통해 유출된 개인정보



5) 피심인은 한국 이용자와 직접적으로 이용관계를 형성하는 한국 법인이 없기 때문에 한국 이용자의 계정 수를 직접 추적하지 않고 있어 이용자 계정 중 한국IP를 기준으로 이용자 수를 추정(2022년 활성 이용자 수)

6) 잘못된 송금 방지를 위해 이용자가 송금을 요청시 이름·프로필 사진·국가코드를 띄워 요청이 적정한 것인지 확인

해커는 2021년 9월부터 상대적으로 적은 양의 API Call을 시작하였고, 2021년 10월 22일 대량의 API Call을 하였으며, 피심인은 대량의 API Call이 발생한 사실을 2021년 10월 30일 인지하였다.

이에 피심인은 해커가 생성하여 사용한 가맹점 계정 3개를 차단하고, API Call에 대한 속도 제한을 하였으며, 정상 트래픽 여부 확인을 위해 HTTP Header[7]의 유효성을 검증하도록 하였다.

피심인은 송금 기능 관련 개인정보 유출 사고가 발생하기 전에는 특정 IP에서 API Call이 1초에 1,000건 이상인 경우, 10초에 4,400건 이상인 경우, 15분간 해당 IP에서의 API Call을 차단하고, 2분에 190,000건 이상인 경우, 30분간 해당 IP에서의 API Call을 차단하였으나, 유출 사고 이후 특정 IP에서 API Call이 1분에 15건 이상만 되어도 해당 IP의 API Call을 완전히 차단하는 등 아래와 같이 API Call 차단·탐지 정책을 변경하였다.

<참고2> API Call 탐지·차단(속도 제한) 정책

유출 사고 이전			유출 사고 이후('21.11.15.)			유출 사고 이후('21.11.17.)		
시간	건수	정책	시간	건수	정책	시간	건수	정책
1초	1,000건	15분 차단	**1분**	**15건**	**차단**	**1분**	**15건**	**차단**
10초	4,400건	15분 차단	**6분**	**90건**	**차단**	**6분**	**120건**	**차단**
2분	190,000건	30분 차단	**1시간**	**360건**	**차단**	**1시간**	**720건**	**차단**

피심인은 2021년 11월 4일부터 2021년 11월 29일까지 유출된 이용자 및 개인정보 유형을 확인하기 위한 분석을 진행하였고, 2021년 11월 30일 유출 통지 초안 작성 및 통지 이후 고객 문의에 대한 대응을 준비한 후, 2021년 12월 7일 유출 통지 및 위원회 개인정보 포털에 신고하였다.

나. 직원 이메일 피싱 관련

피심인의 직원에게 총 471건의 피싱 이메일이 수신되었고, 30명이 피싱 링크를 클릭하였으며, 13명이 피싱 사이트에 로그인 정보를 입력하였다.

7) 클라이언트(이용자 기기)와 서버가 통신할 때 주고받는 정보 : 통신 일시, 브라우저 종류·버전, 운영체제, 접속경로 등

해커는 그중 한 명의 로그인 정보를 이용하여 내부시스템(아웃룩 365 이메일, SharePoint)에 대한 접속을 시도하였고, 그 한 명은 해커가 내부시스템 접속을 위해 요청한 인증 메시지를 승인하였다.

내부시스템 접속에 성공한 해커는 한국인 개인정보가 포함된 3개 MS오피스 파일을 열람[8]하였고, 이로 인해 한국인 가맹점주 및 파트너[9] 1,186명의 이름, 업무용 이메일, 업무용 전화번호, 업무용 주소 등 개인정보가 유출되었다.

피심인은 2021년 11월 5일 11:17 직원 대상 피싱을 시도하는 이메일(471건)에 대한 경고 메시지를 수신하였고, 2021년 11월 6일 데이터 접근을 인지하였다.

이후 피심인은 직원들의 메일함에서 피싱 이메일을 제거하고, 링크를 클릭한 직원(30명)을 파악 후 해당 계정을 차단 및 재설정하였으며, 피싱 피해 직원 계정 및 모든 파일에 대해 포렌식 분석을 진행하였다.

피심인은 2021년 11월 25일부터 2021년 12월 7일까지 유출 통지서 작성 및 고객 문의에 대한 대응을 준비하였고, 2021년 12월 7일 유출 통지 및 위원회 개인정보 포털에 신고하였다.

다. 크리덴셜 스터핑 공격 관련

해커는 알 수 없는 방법으로 확보한 계정정보(아이디와 비밀번호)를 이용하여 2022년 12월 6일부터 2022년 12월 8일까지 서비스에 로그인을 시도(크리덴셜 스터핑 공격)하였고, 로그인에 성공하는 경우 이용자의 개인정보를 유출하였으며, 이로 인해 한국 이용자 336명의 이름, 생년월일, 주소, 핸드폰 번호 등 개인정보가 유출되었다.

해당 기간 동안 서비스에는 총 2억 6,354만 건의 로그인 시도가 있었고, 이 중 96%는 차단되었으며, 나머지 4% 중 336개 한국 이용자 계정이 로그인에 성공하였다.

8) 개인정보가 포함된 파일이 다운로드 또는 삭제되지는 않음
9) 결제가 가능한 해외 오픈마켓 등에 입점한 '한국인' 판매자

세부적으로 살펴보면, 유효한 아이디로 로그인을 시도하여, ①비밀번호가 일치한 경우는 전체 시도의 0.37%, ②비밀번호가 불일치하여 실패한 시도는 3.83%, ③"2단계 인증" 및 기타 이유로 차단된 시도는 0.28%이다.

피심인은 일자별로 로그인 시도 건수, 유효 계정 수, 성공 수 등에 대한 자료 제출 요구에 대해 데이터 보존 정책에 따라 질문에 답변하기 위한 분석에 필요한 자료를 가지고 있지 않으며, 위원회가 요구하는 세부 수준을 정리해두지 않았다고 답변한바, 이러한 분석은 별도로 수행하지 않는 것으로 판단된다.

참고로 유출 당시 시간당 최대 약 78,000회의 로그인 시도가 있었으며, 피심인은 사고 이후 특정 IP 또는 계정에서 1분에 3건, 6분에 4건, 1시간에 5건 이상인 경우 로그인 시도를 제한하고 캡차를 적용하였다.

<참고3> 크리덴셜 스터핑 공격을 통해 유출된 개인정보

피심인은 2022년 12월 6일 텔레그램에 온라인 포털 사이트[10] 공격과 관련된 메시지가 게시된 것을 확인하였고, 사건 조사를 진행하던 중 2022년 12월 7일 크리덴셜 스터핑 공격 발생을 인지하였으며, 이후 2022년 12월 20일 한국 이용자의 개인정보가 유출된 것을 확인하였다.

피심인은 유출 사고 이전에는 이용자가 서비스에 아이디, 비밀번호만으로 로그인하는 경우 개인정보(전화번호, 주소, 생년월일)에 대한 열람이 가능하도록 하였으나, 사고 이후 로그인 시 개인정보를 볼 수 없도록 마스킹 처리[11]하였고, 유출 대상 계정이 악용되지 않도록 조치하였으며, 유출된 정보가 다크웹에 게시

10) https://
11) 마스킹 날짜 : ① 전화번호 - '22.12.9. ② 주소 - '22.12.12. ③ 생년월일 - '22.12.16.

되는지 여부를 지속 모니터링하였다.

그리고 피심인은 계정에 대한 선택적 계정 보안 기능으로 “2단계 인증[12]”을 제공하고 있는 것으로 확인되나, 이용자에게 “2단계 인증”을 활성화할 것을 안내한 일자 및 방법을 모두 답변하라는 위원회의 자료제출 요구에 대해 2023년 1월 2일 한국 이용자에게 “2단계 인증” 기능을 안내하였다고 하며, 전체 이용자 중 5%, 한국 이용자 중 2%가 “2단계 인증”을 사용하고 있다고 답변하였다.

피심인은 로그인 유효성 확인 조사, 유출된 이용자 식별, 유출 통지 초안 작성, 제출자료 준비, 고객 문의 대응 준비, 한국어 번역 등을 진행하였고, 2023. 1. 2. 유출 통지 및 위원회 개인정보 포털에 신고하였다.

12) 선택 기능, 로그인 시 이메일이나 전화번호 발송된 6자리 숫자 코드 입력

Ⅲ. 피심인의 행위에 대한 위법성 판단

1. 관련 규정

舊 보호법 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”라고 규정하고 있다.

또한, 제39조의4 제1항은 정보통신서비스 제공자는 개인정보의 유출 사실을 안 때에는 24시간 내 유출된 개인정보 항목, 유출이 발생한 시점, 이용자가 취할 수 있는 조치, 정보통신서비스 제공자의 대응 조치, 이용자가 상담 등을 접수할 수 있는 부서 및 연락처를 해당 이용자에게 알리고 신고하도록 규정하고 있다.

동법 시행령 제48조의2 제1항 제2호는 정보통신서비스 제공자등은 이용자의 개인정보를 처리하는 경우 개인정보에 대한 불법적인 접근을 차단하기 위한 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영, 그 밖에 개인정보에 대한 접근 통제를 위하여 필요한 조치를 하도록 규정하고 있다.

舊 개인정보의 기술적·관리적 보호조치 기준[13](이하 ‘고시’) 제4조 제5항은 정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한, 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지 기능을 포함한 시스템을 설치·운영하도록 규정하고, 제4조 제9항은 “정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”라고 규정하고 있다.

13) [시행 2021. 9. 15.] [개인정보보호위원회고시 제2021-3호, 2021. 9. 15., 일부개정]

2. 보호법 적용 대상 여부

피심인은 한국 대상 별도 도메인( ) 사용 및 한국어로 서비스를 제공하고, 개인정보 처리방침에 한국 사용자를 위한 추가 정보를 기재 및 수수료 페이지에 한국 시장/지역과 관련한 수수료를 공개하는 사실 등으로 미루어 보아 피심인이 한국 대상 서비스를 제공하는 것이 명확하며, 실제 한국 이용자 수 또한 명에 이르므로, 보호법 적용 대상이다.

<참고4> 피심인의 개인정보 처리방침

3. 舊 보호법상 의무 위반

가. 안전조치의무 위반

총 3차례에 걸친 유출과 관련하여 송금 기능 해킹과 크리덴셜 스터핑 공격의 경우 시차는 존재하나, 피심인의 안전조치의무 위반이 지속되며 동일한 서비스(이용자DB)에서 개인정보 유출이 발생하였고, 직원 이메일 피싱의 경우 개인정보 유출 경위 등을 조사한 결과, 특정 직원의 대처 소홀로 발생한 것으로, 피심인의 안전조치의무 위반과 관련된 사실관계는 확인되지 않았다.

1) 舊 고시 제4조 제5항 관련

피심인은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하고, 접속한 IP주소 등을 재분석하여 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영하여야 한다.

피심인은 2021년 11월 15일 전 특정 IP에서 반복적인 API Call이 있는 경우, 해당 IP에서의 API Call을 탐지·차단하는 조치를 취하였다고 하나, 피심인이 취한

조치[14]는 DoS 공격[15]을 방어하기 위한 것으로 판단될 뿐, 개인정보에 대한 불법적인 접근을 탐지·차단하는 데 목적이 있었던 것으로 볼 수 없으며, 실제로 피심인이 대량의 API Call을 즉시 인지하지 못한 점[16], 사고 이후 변경한 탐지·차단 조치[17] 등을 고려하였을 때, 피심인이 API Call로 인한 불법적인 개인정보 유출 시도를 탐지·차단하도록 시스템을 설치·운영하였다고 볼 수 없다.

또한, 크리덴셜 스터핑은 널리 알려진 공격 기법이고, 이를 통한 로그인 성공 시 개인정보 유출도 쉽게 예상되며, 특히 2021년 API Call을 통한 개인정보 유출 사고가 있었음에도, 크리덴셜 스터핑을 통한 개인정보 유출을 탐지·차단하기 위하여 일자별로 로그인 시도 수, 유효 계정 수, 성공 수 등을 분석[18]하거나, 특정 IP에서 반복적인 로그인 시도를 하는 경우 이를 제한하는 등 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 하지 않았으며, 사고가 발생한 이후에야 특정 IP 또는 계정에서 1분에 3건, 6분에 4건, 1시간에 5건 이상이면, 로그인 시도 제한 및 캡차를 적용하였다.

특히, 법원 판결문에 따르면 특정 IP의 반복 로그인 시도가 초당 29건 이하인 경우에도 악의적인 행위로 판단하였고, 정상 로그인 분석 등을 통해 그에 맞는 탐지룰을 설정할 수 있다고 판시한바, 피심인이 특정 IP의 API Call이 1초에 1,000건 이상 발생하여야 탐지 및 일시 차단되도록 한 것은 이에 비추어 합리적이지 않으며, 로그인 시도 분석 및 그에 맞는 제한 정책 등을 적용하지 않은 것 또한 보호조치 미흡으로 판단할 수 있다.

즉, 피심인이 API Call 및 크리덴셜 스터핑을 통한 개인정보 유출을 탐지·차단하기 위한 조치를 충분하게 수행하지 않은 것은 침입탐지 및 침입차단 시스템의 설치·운영 의무를 규정하고 있는 舊 고시 제4조 제5항을 위반한 행위에 해당한다.

14) 특정 IP에서 1초 1,000건, 10초 4,400건, 2분 190,000건 이상인 경우 해당 IP를 15분간 탐지·차단하도록 한 것
15) 시스템을 악의적으로 공격해 해당 시스템의 리소스를 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격
16) 피심인은 '21.10.22. 발생한 대량의 트랙픽을 '21.10.30. 인지함
17) 특정 IP에서 API Call이 1분에 15건 이상만 되어도 해당 IP의 API Call을 완전히 차단, HTTP Header 유효성 검증
18) 피심인은 일자별로 로그인 시도 건수, 유효 계정 수, 성공 수 등에 대한 자료 요구에 대해 의 데이터 보존 정책에 따라 분석에 필요한 데이터를 가지고 있지 않고, 사고 후 영향 분석을 수행할 때에도 위원회가 요구하는 세부 수준을 날짜별로 정리해두지 않았다고 답변한바, 상시적으로 이러한 분석을 하지 않는 것으로 판단함

<참고5> 크리덴셜 스터핑 관련 판례(서울고등법원 2020. 11. 4., 선고 2019누43964, 판결)

(…) 2시간 26분 동안 930번으로 가장 로그인 시도가 많았던 IP주소의 경우에는 **사람이 할 수 없는 속도로** (…) 15시 00분 198회의 경우에도 39초에 19회, 40초에 27회, 41초에 27회, 42초에 28회, **43초에 29회,** (…) 로그인을 시도 (…)

(…) 전체 사용자의 **로그인 시도 횟수, 성공된 로그인 횟수, 실패한 로그인 횟수, 로그인 성공/실패율을 실시간으로 확인**하는 것은 기술적으로 구현이 가능

(…) 특정 IP 또는 특정 계정 단위로 나누어 해당 IP나 계정에 누적하여 몇 번의 로그인이 성공하였고 실패하였는지 여부도 분석할 수 있다.

2) 舊 고시 제4조 제9항 관련

피심인은 개인정보가 인터넷 홈페이지 등을 통하여 유출되지 않도록 개인정보처리 시스템 등에 조치할 의무가 있으며, 조치 여부는 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지를 기준으로 판단하여야 한다.

<참고6> 대법원 2018. 1. 25., 선고 2014다203410 판결

(…) 보호조치를 이행하였는지 여부를 판단함에 있어서는, 해킹 등 침해사고 당시 보편적으로 알려져 있는 정보보안의 기술 수준, 정보통신서비스 제공자의 업종·영업규모와 정보통신서비스 제공자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 그 효용의 정도, 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해 발생의 회피 가능성, 정보통신서비스 제공자가 수집한 개인정보의 내용과 개인정보의 누출로 인하여 이용자가 입게 되는 피해의 정도 등의 사정을 종합적으로 고려하여 정보통신서비스 제공자가 해킹 등 **침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부를 기준으로 판단**하여야 한다. (…)

앞서 살펴보았듯이 크리덴셜 스터핑은 널리 알려진 공격 기법으로 이를 통한 유출은 이용자가 아이디, 비밀번호만으로 로그인하는 경우 개인정보가 열람되지 않도록 조치하거나, 2단계 인증 등을 도입하여 쉽게 차단할 수 있으며, 실제 피심인은 이용자에게 선택적 계정 보안 기능으로 2단계 인증 기능을 제공한다.

그러나, 피심인은 이번 사고가 발생한 이후에야 아이디, 비밀번호로만 로그인한 경우, 해당 정보가 열람되지 않도록 마스킹하였고, 2단계 인증 기능은 유출 사고 이후인 2023년 1월 2일 처음으로 한국 이용자에게 안내하였다.[19]

19) 한국 이용자 중 2%만 2단계 인증을 사용하고 있었음

이러한 조치가 고시에 명문화되어 규정되어 있지 않지만, 피심인은 전 세계적으로 서비스를 제공하는 글로벌 기업으로 온라인 지불 시스템을 운영하는바, 다른 기업에 비해 개인정보처리시스템에 대한 보호조치를 강화할 필요가 있다.

따라서 피심인이 크리덴셜 스터핑을 통한 개인정보 유출을 방지하기 위하여 舊 고시 제4조 제9항에서 규정한 충분한 조치를 다 하고 있다고 평가하기 어려우며, 이는 舊 보호법 제29조의 안전조치의무 위반을 판단할 때 고려할 요소에 해당한다.

3) 소결

따라서 피심인은 舊 고시 제4조 제5항을 명백히 위반하였고, 동조 제9항에 따른 조치를 충분히 하였다고 평가하기 어려운바, 이는 舊 보호법 제29조 위반에 해당한다.

나. 개인정보 유출 등의 통지·신고 의무 위반

피심인은 개인정보 유출 사실을 안 때에는 24시간 내 해당 사실 등을 이용자에게 알리고 위원회 또는 한국인터넷진흥원에 신고하여야 한다.

그러나, 피심인은 송금 기능 해킹 관련 유출은 2021년 11월 29일에 인지하였고, 직원 이메일 피싱과 관련한 유출을 2021년 11월 6일에 인지하였음에도 약 1개월이 지난 2021년 12월 7일에 통지·신고하였으며, 크리덴셜 스터핑 공격 관련 유출은 2022년 12월 20일에 인지하였음에도 10일 이상 지연하여 2023년 1월 2일에 통지·신고하였다.

피심인은 이와 관련하여 유출 통지문 작성, 고객 문의 대응 준비, 로그인 유효성 확인, 유출 이용자 식별, 제출자료 준비 및 한국어 번역 등의 통지·신고 지연 사유를 소명하였으나, 이는 유출 통지를 위해 필수적으로 수반되는 조치이므로, 특별한 사정으로 볼 수 없고, 필요시 위원회와 협의할 수 있는 점[20] 등을 고려하면 정당한 사유로 받아들일 수 없다.

따라서 피심인은 3차례 모두 유출 사실 인지 후 정당한 사유 없이 24시간이 지나서 통지·신고하였고, 이는 각각 舊 보호법 제39조의4 제1항을 위반한 것이다.

20) 개인정보 유출 대응 매뉴얼(2020. 12.) 13P

Ⅳ. 피심인 주장에 대한 검토

1. 개인정보의 안전조치의무 위반 관련

가. 피심인 주장

피심인은 개별적 조치에 일부 미흡한 사항들이 발견되더라도, 전체적으로 사고 발생을 방지하기 위한 보안조치를 성실하게 취한 경우 제29조의 안전조치의무를 위반하지 않은 것으로 판단하여야 한다고 주장한다.

이와 관련하여 피심인은 ISO 27001[21]를 비롯한 다수의 정보보호 인증을 취득하고 PCI 및 FIDO 등 결제 및 로그인에 관한 국제 보안 표준 마련[22]하였음을 소명하였다.

또한, 피심인은 송금 기능 해킹 관련 사용자 행동 분석 도구와 방화벽 도입·운영하였고, 크리덴셜 스터핑 공격 관련 엔드포인트 모니터링 기술 등 다양한 조치 및 2단계 인증 기능 제공하였으며, 사고 이후에도 속도 제한 및 차단 정책을 강화하였고, API 코드를 수정 배포하였으며, 세금 신고 포털의 개인정보를 마스킹 및 CAPTCHA를 확대 적용하였음을 소명하였다.

나. 검토의견 : 불수용

피심인의 소명을 검토하였을 때, 피심인이 다수의 정보보호 인증을 취득하고, 개인정보 유출 방지 등을 위해 다양한 보호조치를 하였으며, PCI 및 FIDO 등 정보보호 관련 국제 보안 표준 마련에 기여하는 등 피심인의 정보보호 노력은 인정할 수 있다.

그러나, 피심인이 일반적으로 정보보호를 위한 조치를 한 것과는 별개로, 이 사건 송금 기능 해킹 및 크리덴셜 스터핑 공격을 통한 유출 상황과 이와 관련한 피심인의 침입탐지 및 침입탐지시스템 설치·운영 등 보호조치, 피심인의 사업 규모

21) ISO 27001 : 정보보호 관리체계에 대한 국제 표준이자 정보보호 분야에서 가장 권위 있는 국제 인증

22) PCI(Payment Card Industry) : 신용카드 데이터에 대한 통제를 강화하여 사기를 방지하도록 고안된 글로벌 정보보안표준
FIDO(Fast IDentity Online) : 비밀번호의 문제점을 해결하기 위해 제안된 사용자 인증 프레임워크로 비밀번호 없이 인증(UAF, 지문·홍채 등 생체인증) 또는 비밀번호를 보완해서 인증(U2F)으로 구성

등을 종합적으로 고려하면, 피심인이 사회통념상 합리적으로 기대가능한 정도의 보호조치를 다하였다고 보기 어렵다.

2. 과징금 부과 시 매출액 산정 관련 : 불수용

가. 피심인 주장

피심인은 송금 기능 관련 매출액을 별도로 제출하고, 직원 피싱 및 크리덴셜 스터핑과 관련한 매출액은 없다고 소명하였다.

또한, 피심인은 고의·중과실이 없고, 어떠한 이익을 얻지도 않았으며, 피해를 시정하기 위해 상당한 자원을 투자한 점, 위반행위로 처벌받은 적이 없는 점, 조사에 적극 협력한 점 등을 고려해줄 것을 요청하였다.

나. 검토의견 : 일부 수용

크리덴셜 스터핑과 관련한 매출액이 없다는 주장과 관련하여 대법원은 “위반행위로 인하여 직접 또는 간접적으로 영향을 받는 서비스의 범위는 유출사고가 발생한 개인정보를 보유·관리하고 있는 서비스의 범위를 기준으로 판단”하여야 한다고 판시[23]하였다.

<참고7> 대법원 2023. 10. 12., 선고 2022두68923 판결

> (…) 정보통신서비스 제공자가 적절한 보호조치를 취하지 않은 개인정보를 자신의 영업을 위해 보유함으로써 얻은 이득이라 보아야 한다. 이에 따라 위 과징금 부과를 위한 관련 매출액을 산정함에 있어 “위반행위로 인하여 직접 또는 간접적으로 영향을 받는 서비스”의 범위는, **유출사고가 발생한 개인정보를 보유·관리하고 있는 서비스의 범위를 기준으로 판단**하여야 한다. (…)

따라서 이 사건 개인정보 유출사고가 발생한 개인정보를 보유·관리하고 있는 서비스는 서비스이므로 피심인의 주장은 타당하지 않다.

다만, 피심인이 자료제출 요구 등 조사에 적극 협력한 점은 인정되므로, 과징금 산정 시 이를 반영하여 추가적으로 감경한다.

23) 대법원 2023. 10. 12. 선고, 2022두68923 판결

Ⅴ. 처분 및 결정

1. 과징금 부과

피심인의 舊 보호법 제29조 위반에 대한 과징금은 같은 법 제39조의15 제1항 제5호, 같은 법 시행령 제49조의11제1항과 제4항, [별표 1의5] (과징금 산정기준과 산정절차) 및 「舊 개인정보보호 법규 위반에 대한 과징금 부과기준」(고시 제2020-6호) (이하 '舊 과징금 부과기준')에 따라 다음과 같이 과징금을 부과한다.

과징금은 ①위반행위와 관련한 매출액 산정, ②관련 매출액에 부과기준율을 곱하여 기준금액 산정, ③기준금액에 필수적 가중·감경, ④추가적 가중·감경을 거쳐 산정한다.

가. 과징금 상한액

피심인의 舊 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제39조의15 제1항 제5호에 따라 위반행위와 관련된 정보통신서비스의 직전 3개년도의 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액

1) 고의·중과실 여부

舊 과징금 부과기준 제5조 제1항은, 舊 보호법 시행령 〔별표 1의5〕 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리 목적의 유무, 영 제48조의2에 따른 안전성 확보조치 이행 여부 등을 고려하여 판단하도록 규정하고 있다.

이에 따를 때, 피심인의 舊 보호법 제29조 위반행위와 관련하여 2차례에 걸쳐 이용자의 개인정보가 유출되는 등 중과실이 있다고 판단한다.

2) 중대성의 판단

舊 과징금 부과기준 제5조 제3항은, 위반 정보통신서비스 제공자등에게 고의·

중과실이 있으면 위반행위의 중대성을 '매우 중대한 위반행위'로 판단하도록 규정하고 있으나, 단서 조항에서, ①위반행위로 인해 직접적으로 이득을 취득하지 않은 경우(제1호), ②위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우(제2호), ③이용자의 개인정보가 공중에 노출되지 않은 경우(제3호) 중 모두에 해당할 때에는 '보통 위반행위'로, 1개 이상 2개 이하에 해당할 때에는 '중대한 위반행위'로 규정하고 있다.

위 기준을 적용하여 ①피심인이 위반행위로 직접적으로 이득을 취하지 않았고, ②위반행위로 인한 개인정보의 피해 규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내( )인 경우인 점, ③ 이용자의 개인정보가 공중에 노출되지 않은 점 등을 종합적으로 고려할 때, 위반행위의 중대성을 '보통 위반행위'로 판단하였다.

3) 기준금액 산출

舊 과징금 부과기준 제4조(관련 매출액 산정) 제1항에 따라 "관련 매출액은 위반 정보통신서비스 제공자등의 위반행위로 인하여 직접 또는 간접적으로 영향을 받는 서비스의 직전 3개 사업연도의 연평균 매출액으로 한다."라고 규정되어 있으며, 또한 같은 조 제3항에는 "서비스에 대한 매출액은 회계자료를 참고하여 정하되, 이를 통해 위반행위와 관련한 서비스의 매출액을 산정하기 곤란한 경우에는 해당 정보통신서비스 제공자등의 과거 실적, 동종유사 역무제공사업자의 과거 실적, 사업계획, 그 밖에 시장상황 등을 종합적으로 고려하여 매출액을 산정할 수 있다." 라고 규정하고 있다.

피심인의 서비스를 통해 한국의 비즈니스 계정(상품·서비스 대금 수령 등) 및 개인 계정(상품·서비스 구매 등)에서 발생한 매출액의 위반행위 종료 직전 3개 년도(2019~2021) 평균, 달러를 피심인의 관련 매출액으로 산정한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 백만 달러)

	2019년	2020년	2021년	평균
관련 매출액				

피심인의 위반행위는 舊 보호법 시행령 [별표 1의5] 2. 가. 1)에 따라 '보통 위반행위'에 해당하므로 부과기준율 1천분의 15을 적용, 관련 매출액에 부과기준율을 곱한 달러를 기준금액으로 산정한다.

< 舊 보호법 시행령 [별표 1의5] 2. 가. 1) 부과기준율 >

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	1천분의 21
일반 위반행위	**1천분의 15**

다. 필수적 가중 및 감경

피심인의 위반행위 기간이 2년을 초과하므로 기준금액의 100분의 50에 해당하는 달러를 가중하고, 최근 3년간 과징금 부과 처분을 받은 적이 없으므로 조정을 거친 금액에서 기준금액의 100분의 50에 해당하는 달러를 감경한다.

라. 추가적 가중 및 감경

舊 과징금 부과기준 제8조는 사업자의 위반행위의 주도 여부, 조사의 협조 여부 등을 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위 내에서 [별표]에 따라 추가적으로 가중·감경할 수 있다고 규정하고 있다.

이에 따를 때, 피심인이 조사에 적극 협력한 점을 고려하여 필수적 가중·감경을 거친 금액의 100분의 10에 해당하는 달러를 감경한다.

마. 과징금의 결정

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15조 제1항 제5호 및 같은 법 시행령 제48조의11 제4항 [별표 1의5] 2. 가. 1)(과징금의 산정기준과 산정절차) 및 舊 과징금 부과기준에 따라 상기와 같이 단계별로 산출한 금액인 67만 4,500달러를 최종 과징금으로 결정한다.

〈과징금 산출 내역(안)〉

부과 대상	관련매출액	기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금
					$674.5천 906백만원[24]

2. 과태료 부과

피심인의 舊 보호법 제29조(안전조치의무) 및 같은 법 제39조의4(개인정보 유출 등의 통지·신고에 대한 특례) 제1항 위반행위에 대한 과태료는 같은 법 제75조 제2항 제6호·제12호의3, 같은 법 시행령 제63조, 같은 법 시행령 [별표2] '과태료의 부과기준' 및 「舊 개인정보 보호법 위반에 대한 과태료 부과기준」(이하 '舊 과태료 부과지침')에 따라 다음과 같이 부과한다.

가. 기준금액

舊 보호법 시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 각 위반행위별 기준금액을 각각 600만 원으로 산정한다.

〈 舊 보호법 시행령 [별표2] 2. 개별기준 〉

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4 제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
도. 법 제39조의4제1항을 위반하여 이용자·보호위원회 및 전문기관에 통지 또는 신고하지 않거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 경우	법 제75조 제2항 제12호의3	600 (3건 총1,800)	1,200	2,400

24) '23.10.25.(의결일) KEB하나은행(舊 외환은행)에서 최초 고시한 매매기준율(1,343.90)을 적용하여 원화로 환산

나. 과태료의 가중 및 감경

1) 과태료의 가중

舊 과태료 부과지침 제8조는 '사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다'라고 규정하고 있다.

피심인의 경우, 舊 과태료 부과지침 제8조 및 [별표2]의 가중기준에 따라 舊 보호법 제29조 위반행위의 경우 '법 위반상태의 기간이 3개월 이상'이므로 기준금액의 100분의 10에 해당하는 60만 원을 가중하고, 같은 법 제39조의4제1항 위반행위(3건)는 '제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우'로 기준금액의 100분의 10에 해당하는 60만 원씩을 각각 가중한다.

< [별표2] 과태료의 가중기준(제8조 관련) >

기준	가중사유	감경비율
위반의 정도	2. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내
위반 기간	법 위반상태의 기간이 3개월 이상인 경우	기준금액의 10% 이내

2) 과태료의 감경

舊 과태료 부과지침 제7조는 '사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다'라고 규정하고 있다.

피심인의 경우, 舊 과태료 부과지침 제7조 및 [별표1] 과태료의 감경기준에 따라 舊 보호법 제29조 위반행위의 경우 '위반행위에 대해 시정을 완료한 경우', '조사에

적극 협력한 경우'에 해당하여 위반사항에 대해 기준금액의 100분의 50에 해당하는 300만 원을 감경하고, 같은 법 제39조의4 제1항 위반행위(3건)는 '조사에 적극 협력한 경우'에 해당하여 위반사항에 대해 기준금액의 100분의 40에 해당하는 240만 원씩을 각각 감경한다.

< [별표1] 과태료의 감경기준(제7조 관련) >

기준	감경사유	감경비율
조사 협조 · 자진 시정 등	1. 과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우	기준금액의 50%이내
	2. 보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우	기준금액의 40% 이내

다. 최종 과태료

피심인의 舊 보호법 제29조 및 같은 법 제39조의4 제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 1,620만 원의 과태료를 부과한다.

< 최종 과태료 산출내역(안) >

사업자명	근거법령		과태료 금액 (단위 : 만원)			
	위반 조항	위반내용	기준금액 (A)	가중액 (B)	감경액 (C)	최종액(D) =(A+B-C)
	법 제29조	• 안전조치의무(접근통제)	600	60	300	360
	법 제39의4조 제1항	• 개인정보 유출등의 통지·신고에 대한 특례	1,800 (총3건)	180	720	1,260
	계					1,620

3. 결과 공표

舊 보호법 제66조제1항 및 「舊 개인정보보호위원회 처분결과 공표기준」[25] 제2조(공표요건)에 따르면 피심인의 위반행위는 舊 보호법 제75조 제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우(제4호) 및 위반행위가 6개월 이상 지속된 경우(제5호)에

25) 개인정보보호위원회 지침, 2020. 11. 18. 시행

해당하므로 피심인이 과태료 부과를 받은 사실에 대해 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표

개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.

순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1		법 제29조	안전조치의무 위반	2023. 10. 25.	과태료 부과 360만원
		법 제39조의4 제1항	개인정보 유출등의 통지·신고에 대한 특례 위반		과태료 부과 1,260만원

2023년 10월 25일
개 인 정 보 보 호 위 원 회

Ⅵ. 결론

피심인의 舊 보호법 제29조(안전조치의무) 및 같은 법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례) 제1항을 위반한 행위에 대하여 같은 법 제39조의15(과징금의 부과 등에 대한 특례) 제1항 제5호, 제75조(과태료) 제2항 제6호·제12호의3, 제66조(결과의 공표) 제1항에 따라 과징금·과태료 부과 및 결과 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 위원회의 과징금 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조 제2항의 규정에 따라 그 효력을 상실하고 관할법원(당사자 주소지의 지방법원 또는 그 지원)이 과태료 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료 납입 의무를 부담한다.

2023년 10월 25일

위 원 장　　고 학 수　(서 명)

부위원장　　최 장 혁　(서 명)

위　　원　　김 일 환　(서 명)

위　　원　　김 진 욱　(서 명)

위　　원　　김 진 환　(서 명)

위　　원　　박 상 희　(서 명)

위　　원　　윤 영 미　(서 명)

위　　원　　조 소 영　(서 명)