ISSN(Print) : 1976-5304, ISSN(Online) : 2713-931X
https://kdfs.jams.or.kr, DOI : 10.22798/kdfs.2022.16.2.142

상품권 탈취형 메신저 피싱 대응 방안

박 조 원*, 이 상 진**
서울경찰청 서울강남경찰서 (사이버수사관)*
고려대학교 정보보호대학원(교수)**

Countermeasures against Messenger Phishing by Stealing Gift Certificates

Jowon Park*, Sangjin Lee**
Seoul Metropolitan Police Agency, Kang-Nam police station(Cyber Crime Investigator)*
Graduate School of Information Security, Korea University (Professor)**

요 약

전기통신금융사기의 대책으로 지연 이체, 지급 정지 등이 활성화 됨에 따라 이를 우회하는 수단으로 메신저 피싱 범죄에서 상품권을 탈취한 후 이를 상품권 매매업자를 통해 현금화 하는 사례가 증가하고 있다. 본 논문에서는 상품권 유통 경로에서 자금 세탁되는 방법을 검토하고, 메신저 피싱을 효과적으로 방지하기 위한 기술적, 제도적 대안을 제시한다. 제시한 상품권의 지급정지 제도가 도입되고 이상 거래 탐지 시스템과 정보공유시스템이 구축되면 메신저 피싱을 효과적으로 예방할 수 있을 것으로 보인다.

주제어 : 메신저피싱, 신유형 상품권, 온라인 상품권 핀번호, 돈세탁, 이상거래시스템

ABSTRACT

As countermeasures for telecommunications-based financial fraud such as delayed transfer and payment suspension are activated, there are increasing cases of stealing gift certificates from messenger phishing crimes and then converting them into cash through gift certificate traders, as a means of circumventing the countermeasures. This study aimed to examine how money is laundered in the gift certificate distribution channel and present technical and institutional alternatives to effectively prevent messenger phishing. It is expected that messenger phishing will be effectively prevented as the proposed gift certificate payment suspension system is introduced and an detection system for abnormal transaction and information sharing system are established.

Key Words Messenger phishing, Gift certificate, PIN number, Money laundering prevention, New types of Gift certifications, Fraud detection system

Ⅰ. 서 론

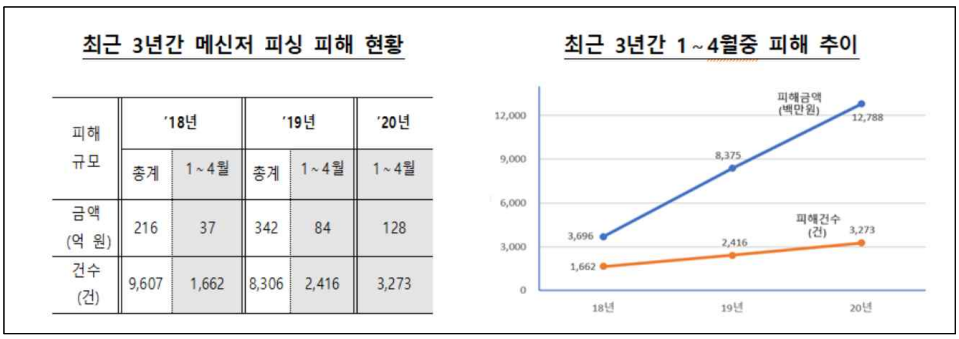
휴대폰이 일상 생활의 필수품이 됨에 따라 자연스럽게 문자메시지나 모바일 메신저를 통해 대상자를 기망하여 금원을 탈취하는 방식의 범죄가 발생하고 있다. 특히 카카오톡과 같은 메신저를 매개로 하여 발생하는 피싱 범죄를 '메신저 피싱'이라 말한다. 메신저 피싱은 피해자들에게 지인을 가장하여 접근하기 때문에 피해자와 지인 사이의 신뢰를 기망의 수단으로 악용하는 범죄이다.

메신저 피싱에서 범죄자들은 피해자와 가까운 지인의 메신저 계정을 도용하거나 사칭하여 금전을 요구하는

▪ Received 18 March 2022, Revised 24 March 2022, Accepted 27 June 2022
▪ 제1저자(First Author) : Jowon Park (Email : lapark77@gmail.com)
▪ 교신저자(Corresponding Author) : Sanjin Lee (Email : sangjin@korea.ac.kr)

메시지를 전달하여 이를 진실로 믿는 피해자로부터 재물을 갈취하거나 재산상 이익을 취한다. 메신저 피싱은 보이스피싱과 함께 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」(이하 '통신사기피해환급법') 에서 정한 전기통신금융사기의 일종으로 범죄에 이용된 금융계좌는 즉시 지급정지할 수 있다.

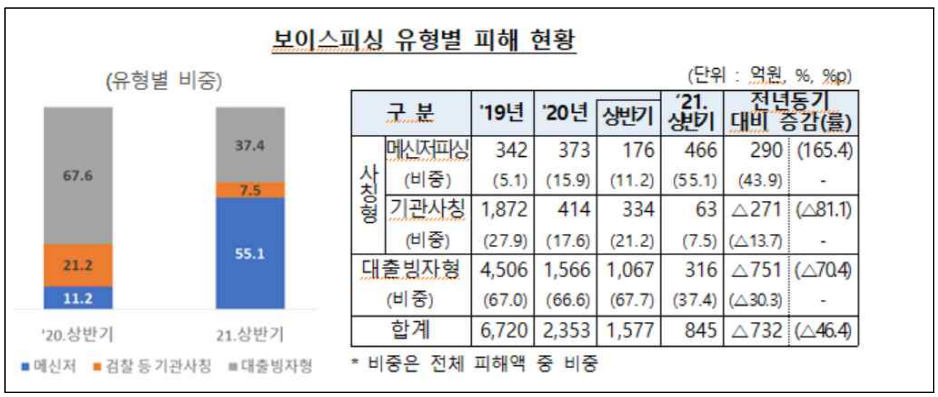
2020. 1월~4월 기준으로 국내 메신저 피싱 발생은 3,273건, 피해액은 128억원으로 작년 대비 메신저 피싱 범죄 발생이 가속화되고 있다.



피해 규모	'18년		'19년		'20년
	총계	1~4월	총계	1~4월	1~4월
금액 (억 원)	216	37	342	84	128
건수 (건)	9,607	1,662	8,306	2,416	3,273

〈Figure 1〉 2020. 6. 24. Korea Communications Commission Press Release

금융감독원 발표 자료에 따르면 보이스 피싱 전체 피해액은 2020년 대비 소폭 감소하였으나 메신저 피싱으로 인한 피해는 장년층을 중심으로 크게 증가하고 있다. 통신사기피해환급법으로 인해 전기통신금융사기의 피해금이 금융계좌로 송금되면 지연이체 및 지급정지로 이어지게 되고 세탁계좌로의 이체가 차단되기 쉽기 때문에 범죄자들은 이를 우회하려고 탈취한 신분증 및 금융거래정보 등을 사용하여 피해자 모르게 핸드폰 개통 및 비대면 계좌를 개설한 후, 예금 이체 및 비대면 대출 등 다양한 방법으로 자금을 편취하고 있다.



(단위 : 억원, %, %p)

구 분		'19년	'20년	'21. 상반기	'20. 상반기	전년동기 대비 증감(률)	
사칭형	메신저피싱	342	373	176	466	290	(165.4)
	(비중)	(5.1)	(15.9)	(11.2)	(55.1)	(43.9)	-
	기관사칭	1,872	414	334	63	△271	(△81.1)
	(비중)	(27.9)	(17.6)	(21.2)	(7.5)	(△13.7)	-
대출빙자형		4,506	1,566	1,067	316	△751	(△70.4)
(비중)		(67.0)	(66.6)	(67.7)	(37.4)	(△30.3)	-
합계		6,720	2,353	1,577	845	△732	(△46.4)

* 비중은 전체 피해액 중 비중

〈Figure 2〉 2021. 9. 6. Financial Supervisory Service's damage statistics in the first half of 2021

2020년 기준 보이스피싱 피해액은 2,353억원으로 전년 대비 65.0%(▽4,367억원) 감소하였다. 반면 지인사칭형 메신저피싱 피해액은 2021년 상반기 기준 466억원으로 전년동기(同期) 대비 165.4%(△290억원) 증가하였고 보이스피싱 유형 범죄의 피해액 중 차지하는 비중이 55.1%로 43.9%나 상승하였다.

'20.1. ~ '20.7.까지 경찰청 형사사법정보화시스템(KICS)의 메신저 피싱 발생 현황을 보면 피해금 수취 유형에 핀(PIN)번호를 요구하는 건수가 금융계좌를 이용한 유형과 비슷하게 발생하였다. 2021년 메신저 피싱의 발생률은 전년 대비 비약적으로 증가하였다. 이렇듯 상품권 발행번호(이하 "핀번호(PIN)"라 한다)")를 탈취하는 피싱범죄가 증가하는 근본적인 이유는 금융계좌 지급정지 시스템에 적용받지 않으면서 비실명거래로 손쉽게 범죄 수익자금을 세탁할 수 있기 때문이다.

□ '20. 1~7월 기준, 발생 및 검거 세부 현황

발생(건)	피해액
6,667	26.5억 원

사칭 유형			
가족	지인	수사기관	기타
5,579	1,009	0	79

피해금 수취 유형				
계좌이체	핀번호	카드이용 직접결제	원격제어 앱 설치 유도	기타
3,058	2,768	624	157	60

검거한 피의자 유형						
합계	총책·관리책	인출책	하부조직원	계좌모집책	계좌명의자	기타
1,620	4	18	10	10	1,516	62

〈Figure 3〉 2020. Number of cases of messenger phishing by the National Police Agency

메신저 피싱에서 범죄자들은 피해자의 개인정보를 확보한 후 피해자의 휴대전화를 원격조정할 수 있는 애플리케이션을 미리 설치해 피해자 명의의 카드를 이용하여 모바일 상품권을 소액결제하게 한 후, 해당 모바일 상품권을 전달받는 형태로 갈취한다. 모바일 상품권은 발행인이 소유자에 대하여 일정한 가액에 상당하는 물품을 인도하거나 용역의 제공을 약속하고 공중에 대하여 매출하는 일람 출급의 무기명 유가증권을 말한다. 모바일 상품권은 거래시장이 비약적으로 성장하고 있는 반면 불법적인 자금세탁의 용도로도 사용되고 있다.

그러나 온라인 상품권에 대한 관계부처들의 규제 논의는 현재까지 나오지 않아 범죄 피해는 지속되고 있는 것이 현실이다. 상품권 할인이나 상품권을 현금화하는 것이 우리나라 금융시스템에 심각한 위험을 끼치지는 않지만, 이러한 행태들로부터 발생하는 불투명한 자금흐름은 범죄에 악용되고 있다는 점에서 매우 우려스럽다. 또한, 자금의 원천이나 사용이 불법임에도 불구하고 추적 자체가 현실적으로 매우 힘들다.

이 논문에서는 온라인 상품권(모바일 상품권)이 자금세탁의 용도로 유통되는 사례를 분석하고, 상품권 거래시장의 신뢰성 및 안전성을 확보할 수 있는 규제방안을 검토해 보고자 한다. 그 방안으로 모바일 상품권이 범죄자금을 세탁하는 용도로 사용되지 않게 하는 정책모델을 수립하고, 범죄 발생시 상품권 발행사가 상품권을 추적할 수 있는 정보시스템 구축을 제안한다. 온라인 상품권(모바일 상품권)은 이미 우리 사회에 널리 보급되어 있으며 여러 문제점을 불러일으키고 있으므로 이를 제도화함과 동시에 향후 범죄수익으로 인한 관계자를 처벌할 수 있는 규제는 시급히 도입할 필요가 있어 보인다.

Ⅱ. 선행 연구

메신저 피싱은 메신저상에서 피해자의 신분증, 은행 계좌번호 등을 전달받아 이를 이용하여 금품을 훔치는 행위를 말한다. 메신저 피싱에서는 카카오톡, 네이트온와 같은 메신저 상에서 ID 도용·무작위 접속 등의 방법을 통해 피해자의 지인인 것처럼 행동하면서 '급전을 요구'하여 금전을 가로채는 수법을 사용한다.

이런 전자금융 범죄는 전기통신을 이용하여 타인을 기망(欺罔)·공갈(恐喝)함으로써 획득한 개인정보(금융거래정보)를 알아내어 자신 혹은 제3자에게 재산상 이익을 취득하게 한 행위는 사기의 구성요건에 해당(전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법 제15조의2 제2항)하여 형사처벌 대상이다. 그리고 타인 명의를 도용하여 공인인증서를 발급받거나 보안카드 번호를 탈취하여 예금을 이체하는 행위 또는 악성프로그램을 유포하는 등 권한 없는 자에 의한 정보처리 업무를 통해 재산상 이익을 취득하게 행위도 형법(刑法)상 컴퓨터등사용사기죄(형법 제347조의2)로 처벌받는다.

전기통신금융사기는 '전기통신금융사기를 목적'으로 한 정보 등의 입력 행위를 구성요건으로 하고 있고 송금·이체할 때 정보 등 입력 행위만으로도 기수(旣遂)에 이른 것으로 본다. 피싱범죄의 특성상 범죄조직을 검거하거나 편취 금액을 환수하기 어려운 사정과 피싱범죄가 우리 사회에 미친 악영향을 고려하여 반듯이 재산상 이익을 취득하여야만 처벌이 가능한 사기죄(혹은 컴퓨터등사용사기죄) 보다 그 구성요건을 완화하여 강력하게 처벌하고 있다[23].

통상적으로 전기통신금융사기 조직은 피해자를 기망 또는 공갈하여 피해자가 사기이용계좌로 금전을 송금하게 하고, 사기이용계좌에서 이를 인출하거나 또 다른 계좌로 이체하는 행위로 재산상의 이익을 실현한다. 2012년 1월 "금융소비자 보호를 위한 보이스피싱 피해방지 종합대책"을 살펴보면 전기통신금융사기를 방지하기 위해 금융권에서는 지연이체, 입금계좌 지정서비스, 해외IP 차단, 지급정지 제도 등을 운영하고 있다.

그러나 이러한 강화대책에도 불구하고 피싱 조직들은 취약계층을 상대로 원격제어 애플리케이션을 설치하게 유도하고 피해자의 신분증 이미지, 계좌번호, 신용카드 번호 등을 확보하여 비대면 계좌를 신규 개설하고, 개설된 계좌로 피해금을 송금하여 강화된 본인인증을 회피하는 방식으로 피해금을 갈취하는 형태가 나타나고 있다.

피해금을 이체하여도 피해자는 지급정지 신청을 통해 피해구제를 받을 수 있다. 〈표 1〉은 이러한 추세를 보여준다. 따라서 보이스 피싱 조직은 계좌이체를 통한 금품 갈취를 벗어난 새로운 범죄 수법을 모색하게 되었다.

〈Table 1〉 Voice phishing damage status according to 「Telecommunication Fraud Damage Refund Act」

구분	'17년	'18년	'19년	'20년	증감률
피해금액	2,431	4,440	6,720	2,353	△4,367 (△65.0)
환급액	598	1,011	1,915	1,141	△773 (△40.4)
환급률	24.6	22.8	28.5	48.5	20.0
피해건수	50,013	70,218	72,488	25,859	△46,629 (△64.3)

〔2021. 4.16. 금감원〕 피해구제신청접수 (1차계좌)기준임, 〔환급률〕 환급액/피해금액

최근에는 상품권이나 구글 기프트카드 등 상품권을 대신 구매한 후 핀번호를 전송해 달라고 요구하는 수법이 사용되고 있다. 이는 보이스 피싱의 대책으로 도입된 지급정지제도로 인해 계좌이체 방식으로 범죄수익금 확보가 어려워지자 손쉽게 돈세탁을 할 수 있는 방식으로 범죄 수법이 변한 것으로 볼 수 있다.

메신저 피싱을 차단하기 위해 해외접속 IP를 필터링하는 기법[4]이 제안되었으나, 최근에는 국내외 인터넷 사용자들이 VPN을 이용한 인터넷 접근이 일반화되었고 메신저 사용자들의 실제 접속지 IP의 정보를 특정하여 차단하는 데는 실익이 없으며, 해외 IP임을 경고하는 알람을 제공하더라도 심리적 압박으로 인하여 피해자들은 해외 접속에 따른 피싱이라는 사실을 망각하여 피해를 입고 있다. 따라서 IP 필터링을 통한 피싱을 예방하는 것은 한계가 있다.

그리고 메신저 대화에서 추출된 단어들의 연관성 패턴 룰에 기반한 메신저 피싱 예방에 관한 연구[10]가 있었으나, 이를 구현하기 위해서는 대화 내용의 데이터베이스화가 필수적인 요건이기에 메신저 이용자들의 대화 기록을 처리・보관하는 경제적인 이슈와 메신저 대화에 포함된 개인정보의 비식별화 과정에서 서비스 이용자들의 법률적 분쟁 소지가 발생할 우려가 있다.

이외 메신저 피싱의 자금세탁에 관련한 상품권의 규제를 논한 연구는 없으나 상품권 거래가 가지는 고유한 사회적인 문제점들을 고찰한 문헌으로는 상품권 법제 개선방안에 대한 연구[2][5][6]가 있다. 논의된 상품권의 법제 개선방안 연구들은 돈세탁 관점에서 상품권의 현금거래 문제점을 구체적으로 검토하여 법제를 개선하는 방안의 제시는 미미하고 과거 폐지된 상품권법의 일부를 인용하거나 자율경쟁 시장의 과도한 규제를 적용하고 있어 구 상품권법이 재개정 되지 않는 한 적절한 해법을 제시하는 데는 무리가 있다.

본 논문은 메신저 피싱에서 탈취된 상품권의 돈세탁 과정을 분석함으로써 상품권 유통구조 및 문제점을 확인한다. 이로부터 상품권을 이용한 돈세탁 규제 방안과 사이버 범죄예방 방안을 제안하고자 한다.

Ⅲ. 메신저 피싱의 범죄 수법 및 수사의 한계

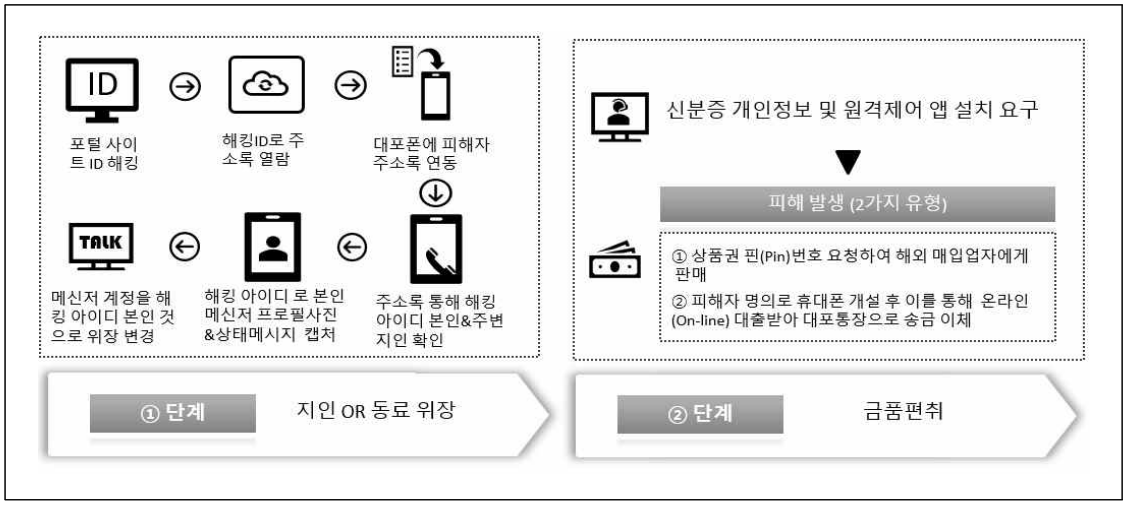
이 장에서는 온라인 상품권을 탈취한 메신저 피싱 사건의 실제 사례를 바탕으로 범죄 수법과 상품권이 가지는 특수성으로 인한 수사의 한계점을 살펴보고자 한다. 이에 앞서 상품권의 유통 체계를 설명함으로써 메신저 피싱 사건를 수사할 때 발생하는 한계를 살펴보고자 한다.

3.1. 메신저 피싱 범죄수법

메신저 피싱은 메신저상에서 피해자에게 자신을 가족이나 지인으로 사칭하면서 피해자로부터 개인정보와 금전을 요구하는 방식의 사회공학적 해킹을 사용하는 신종 사이버 범죄이다. 일반적으로 범인들은 지인을 사칭해 공격 대상자의 심리 상태를 파악하고, ②휴대폰 파손 혹은 모바일 결제 불가한 이유를 대며 "제3자 명의의 휴대폰 번호로 메시지(카톡 등)을 보낸다"며 ③긴급송금, 혹은 상품권 결제를 유도한다. 최근에는 과거 보이스피싱 범행에서 유행했었던 원격지원 프로그램을 악용하는 수법[1]에 온라인 상품권의 핀번호를 요구하는 방법이 결합된 형태가 나타나고 있다. 즉, 스마트폰에 '원격제어 애플리케이션'을 설치하게 하여 직접 온라인 상품권을 구매하는 새로운 변종 수법들이 나타나고 있다.

〈Table 2〉 New types of messenger phishing crimes

신종 유형	설 명
상품권 구매 후 핀번호 전송 요구	계좌에 대한 지급정지를 피하기 위해 최근 주로 이용되는 수법으로, '상품권을 구매해야 하는데 카드 문제로 결제가 되지 않으니, 상품권 구매 후 핀번호를 보내주면 구매대금을 보내주겠다'고 속이는 방식
스마트폰에 '원격제어 어플'을 설치하도록 유도	스마트폰 사용이 익숙하지 않은 피해자에게 '팀뷰어' 등 원격제어 애플리케이션을 설치토록 유도한 후 해당 휴대폰을 직접 제어하거나 개인정보를 탈취해 온라인 결제 등을 통해 금전을 편취하는 방식
신용카드의 사진과 비밀번호 전송 요구	스마트폰 계좌이체나 온라인 상품권 구매 등에 익숙하지 않은 중장년층을 주된 대상으로 삼는 수법으로, 카드 정보와 비밀번호를 요구한 후 이를 이용해 범인이 직접 상품권 등을 구매하는 방식



〈Figure 4〉 Messenger phishing crime stages

〈Figure 5〉 Case of hijacking Contacts and stealing messenger profile

메신저 피싱 범죄는 크게 피해자를 포섭하기 위해 지인의 개인정보를 파악하고 지인의 자격을 모용하기 위한 사전 정보를 획득하는 단계, 습득한 정보를 가공하고 이를 이용해 피해자로부터 금품을 편취하는 범행 단계로 범죄가 구성된다[11].

3.1.1. 준비 단계

준비 단계는 범죄 실행 전 준비 과정을 말하는 것으로, 공격자는 개인정보가 유출된 사이트 계정의 유효성을 검증하고 해당 계정 사용자와 특수한 관계가 있는 잠재 피해자를 물색하는 과정이다. 메신저 피싱의 범행 준비 단계에서는 가장할 메신저 계정을 흉내낼 때 필요한 프로필사진, 잠재 피싱 피해자가 될 대상자를 물색하기 위한 주소록 정보가 필요하다. 또한, 공격자는 유출된 개인정보를 분석하여 가장할 사람과 피싱 피해자의 관계를 파악한다.

국내외 포털사이트들은 여러 기능을 통합한 클라우드 서비스를 제공하고 있다. 그런데 이런 클라우드 서비스에서 제공되는 이미지 저장 서비스, 스마트폰 주소록 백업 서비스는 피싱 공격에 필요한 데이터 유출 통로가 된다. 메신저 피싱의 피해사례를 공개한 누리꾼들의 인터넷 블로그를 보면 공격자는 가장할 사람의 메신저 계정 사진, 피해자의 스마트폰 번호를 통해 지인을 사칭하여 송금을 요청하기 위한 대화형 스크립트를 연출한다는 사실을 확인할 수 있다.

공격자는 불법적으로 취득하거나 SNS에서 제공되는 다이렉트 메시지에 로그인 페이지로 유도하는 다이렉트 메시지를 전송하여 해당 로그인 페이지에 사용자가 아이디와 패스워드를 입력하면 그것을 가로채는 수법[17], '코로나 긴급재난 지원금'과 같은 스미싱 문자를 전송하고 문자 속 URL을 클릭할 경우 스마트폰에 악성코드가 설치되어 저장된 주소록, 문자메시지 등 개인정보가 고스란히 공격자에게 넘어가는 수법[21], 포털사이트 계정을 노려 '차단한 해외 지역에서 로그인 시도가 있었다'는 허위 메일을 보내 추가 본인 인증하게 함으로써 아이디, 패스워드 정보를 탈취하는 이메일 피싱 수법[18]등으로 개인정보를 도용하여 피싱 준비에 필요한 정보를 수집한다[13].

2019년 기준, 경찰청에 접수된 메신저 피싱 사건에서는 국내 유명한 메신저 프로그램인 카카오톡과 네이트온[22] 등이 주로 접수되었다. 공격자는 탈취한 개인정보 등을 이용해 특수한 관계가 확인되는 대상자(부모, 직장 상하 관계, 이모 등)를 메신저 피싱 표적대상자로 선택한다. 실제 2020년 금감원 보이스피싱 피해 현황 분석에 따르면 준비 단계에서 수집한 개인정보를 이용하여 대상자의 기존 대인관계를 쉽게 식별할 수 있는 직장동료 및 가족을 사칭한 경우가 많았다. 이는 피해 대상자가 가해자를 상대로 별도의 신원 확인을 요구하지 않는 특수한 지인 관계를 역이용하는 것이다. 그 후 관계에 맞는 시나리오 스크립트(대본)를 사용하여 공격 대상자를 상대로 최종 범행을 실행한다.

3.1.2. 범행 실행 단계

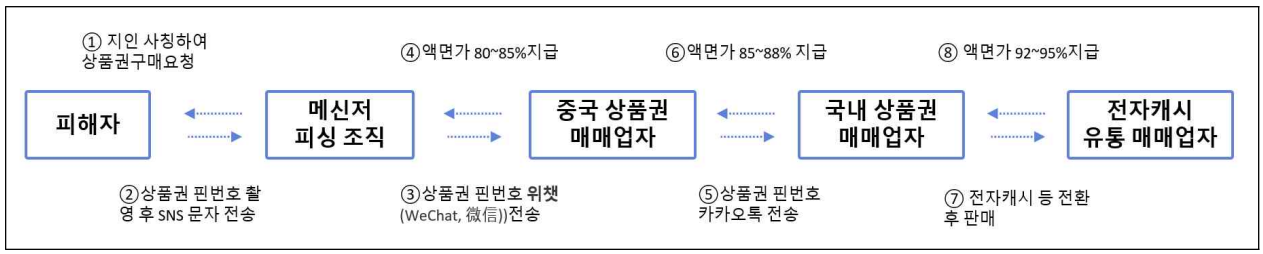
범행 단계는 준비 단계에서 수집된 공격 대상자와 사칭하는 개인정보를 이용해 관계 유형에 맞는 시나리오 대본을 토대로 미리 작성된 메시지를 보내는 것으로 범행을 시작한다. 범행 진행은 ① 공격 대상자 응답유도, ② 사전 질문차단, ③ 대상자의 금품 탈취, ④ 회유 후 종료 단계로 구성된다.

〈Table 3〉 Classification of script types by stage

단계		스크립트 유형
1단계(응답유도)		호칭을 특정하기 쉬운 공격 대상자를 파악하고, 피해자 상태를 탐색. "엄마, 지금 뭐해?", "형수님", "자기자기!"
2단계(질문차단)		핸드폰 오류(액정파손, 충전단자 파손, 공인인증서 오류)로 인해 임시로 PC용 메신저(카톡)를 사용하여 상황이 절실하다며 암시 "지금 급하게 문상 쓸거 하나 있는데 폰이 없어서 못하고 있어~... 온라인 문상 사야 되는데 폰인증 안되니까 힘드네. 엄마 명의로 회원가입하고 구매하면 안될까?"
3단계	(악성앱 설치 유도 및 결재 수단 탈취)	결제 또는 회원인증을 빌미로 피해자의 신분증(촬영본), 계좌번호, 비밀번호, 신용카드번호 등을 요구하여 탈취하고, 원격제어 어플 설치유도 *※ 피해 대상자가 결제 어려움을 호소할 경우 선택 옵션*
	(금품탈취)	대리로 상품권의 구매를 유도하거나 직접 원격제어 어플을 설치해(*해외IP 결재 차단 등을 회피) 송금이체 또는 상품권 핀번호를 직접 구매하여 편취
4단계(회유/종료)		상품권 핀번호에 대한 구매대금이나 송금한 현금에 대해 '저녁에 바로 입금하여 주겠다'며 범행을 종료함. "한국 들어가면 바로 이체시켜 드릴게요 85만이요, 제 이름으로 해서 부탁 좀 드립니다."

공격자는 스크립트 1단계에서 메신저를 통해 피해자에게 친밀성을 과시하는 응답유도 메시지를 보낸다.이로써 공격자는 자신의 신원을 밝히지 않고 대화를 시작한다. 공격자는 대상 피해자에게 상황의 긴급성을 설명하고 자신이 직접 결제하거나 송금할 수 없는 이유를 제시하고 금전 혹은 온라인 상품권 핀번호를 요청한다(스크립트 2단계). 최근에는 피해자의 스마트폰에 원격제어 애플리케이션을 설치하고, 원격에서 피해자의 카드번호 및 비밀번호와 같은 민감한 정보를 자연스럽게 전달받아 대포계좌로 송금하거나 상품권을 구매하는 방식을 사용한다. 특히, 원격제어 애플리케이션을 설치한 경우, 공격자는 피해자에게 다양한 형태의 금전적인 피해를 입힌다(스크립트 3단계).

메신저 피싱사건에서 피해자로부터 편취한 온라인상품권 핀번호의 이동내역을 확인하면 일반적으로 〈그림 6〉과 같이 공격자와 결탁하고 있는 중국에 상주하는 상품권 매입업자에게 액면가 80%로 우선 판매된다. 그후 중국 매입업자는 국내 상품권 매입업자에게 다시 3% 수수료를 받고 판매하고 국내 상품권 업자는 국내 전자캐시 전문 매입업자를 통해 약 4%의 수수료를 받아 최종 전자캐시(구글기프트 코드)로 변환하여 판매한다. 메신저 피싱으로 인한 온라인 상품권 핀번호의 이동 경로는 최초 피해자 → 범인(피셔,Phisher) → (범인과 공모관계로 추정되는) 중국 상품권 매매업자 → 국내 상품권 매매업자 → 구글기프트 코드 전문 매입업자의 순으로 유통된다. 결국, 피해 온라인 상품권 핀번호는 국내 상품권 매입업자가 중국내 업자에게 매입대금인 액면가 85~88%의 판매대금을 송금하여 피해금이 국외 계좌로 반출된다.



〈Figure 6〉 Damaged Gift Certificate Distribution Channel

3.2. 상품권 개념 및 유통 체계

3.2.1. 상품권의 정의

상품권을 취급하는 자(공정거래위원회(표준약관 제10073호, 신유형 상품권 표준약관) 구매자, 또는 구매자로부터 이전받은 자, 발행자, 발행자와 가맹계약을 맺은 가맹점이라고 정의하고 있음.(2020. 12. 4. 개정))들을 규제하기 위해서는 상품권의 법적인 의의를 이해하고 있어야 한다. 1999년 폐지된 상품권법의 연혁을 보면 1961년에 상품권에 대한 정의 조항 없이 재정되었고, 1963년에 동법(제1조의 2)에서 "발행인이 소유자에 대하여 일정한 가액에 상당하는 물품을 인도하거나 용역을 제공할 것을 약속하고 공증에 대하여 매출하는 일람 출급의 무기명 유가증권"이라는 조항이 신설되었다. 이후 1994년 개정된 정의에서는 "그 명칭 또는 형태에 관계없이 발행자가 일정한 금액이나 물품 또는 용역의 수량이 기재(전자 또는 자기적 방법에 의한 기록을 포함)된 무기명증표를 발행·매출하고 그 소지자가 발행자 또는 발행자가 지정하는 자에게 이를 제시 또는 교부하거나 기타의 방법으로 사용함으로써 그 증표에 기재된 내용에 따라 상품권 발행자 등으로부터 물품 또는 용역을 제공받을 수 있는 유가증권"[5]으로 개정되었다. 이후 폐지 전까지는 개정된 정의를 따르고 있었다[2].

이후 2000년 초반부터 유가증권은 인터넷 기술의 발달과 증권시장의 전산화 등 IT의 일상화로 인해 점증적으로 종이 형태에서 전자증서로 대체되기 시작하였다. 이렇게 전자화된 형태의 유가증권을 지칭하여 "전자유가증권"이라 일컫는다[12]. 상품권은 종이 문서의 형태(이하 '지류상품권')와 전자문서의 형태(이하 '신유형 상품권')로 발행되고 있다[6]. 이에 따라 공정위는 소비자 분쟁을 규제하기 위해서 종이 상품권에 대해서는 지류 상품권 표준약관, 전자증서로 대체되는 상품권에 대해서는 신유형 상품권 표준약관을 구분하여 공시하고 있다.

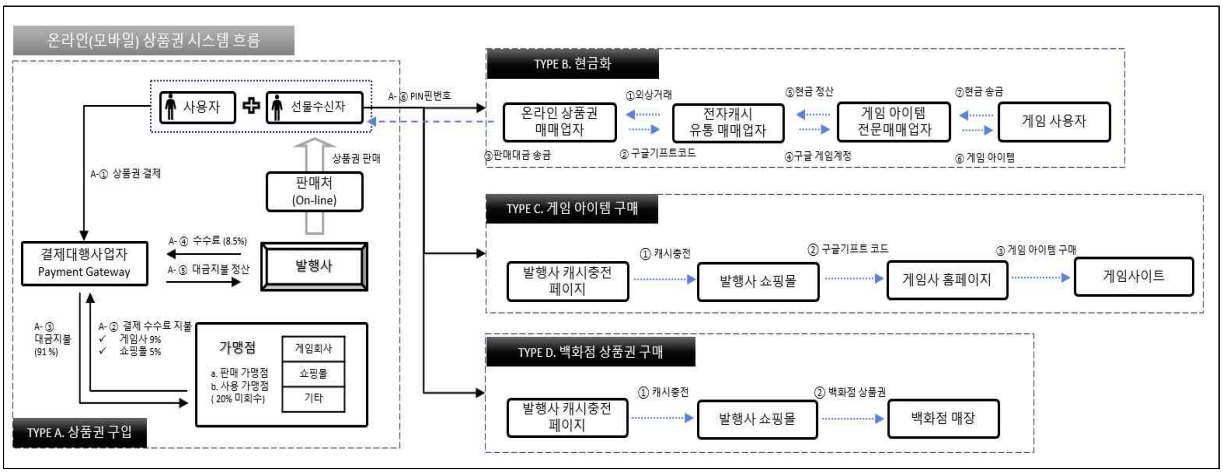
'신유형 상품권 표준약관'에 따르면 제2조에 상품권 발행증표의 전자정보가 모바일 기기에 저장되면 '모바일 상품권', 발행사 상품권 발행 서버에 저장되면 '온라인 상품권', 그 외 발행증표 정보가 전자카드(IC칩 혹은 마그네틱) 물리적 형태로 저장되면 '전자형 상품권'으로 신유형 상품권의 종류를 구분하고 있다[12].

온라인 상품권은 온라인 사이트에서 이용하기 위해서 지류(紙類) 혹은 카드형 상품권에 기재된 온라인 전용 인증번호를 입력하거나 전자상거래 온라인 전용 상품권 구매시 문자메시지로 핀번호(PIN)를 전송받아 해당 금액으로 전환하여 사용할 수 있고, 모바일 상품권은 모바일 기기에 저장된 바코드·QR을 가맹점 포스단말기에

제시하여 사용할 수 있다.

3.2.2. 상품권 유통 체계

온라인 상품권은 2만여 개의 쇼핑, 영화, 온라인게임, 도서교육 사이트에서 사용 가능하다. 통상적으로 온라인 상품권은 발행사 홈페이지와 판매대행사 사이트에서는 액면가의 7~9% 정도 할인되어 판매되고 있다. 이 할인율로 인해 상품권 발행사는 온라인 가맹점 고객을 상대로 전자상거래에서 구매를 유도하는 등 온라인 상거래 활성화에 보탬이 되고 있다. 상품권 발행사는 가맹점과 사용계약이 체결된 제휴사에서 사용 가능한 온라인 상품권을 일괄 발행한다. 〈그림 7〉은 상품권을 구매한 사용자의 사용 유형에 따른 온라인 상품권 처분과정을 설명한 것이다.



〈Figure 7〉 Flow Chart of Online Gift Card System

소비자들은 온라인 상품권을 선(先)구매하고 증표에 화체된 재화 또는 용역을 제공받을 때 온라인 상품권을 가맹점에 제시하여 사용한다(TYPE A.). 상품권 발행사는 제휴사와 사용계약 체결을 통해 이용자가 온라인 상품권을 사용함에 있어 이용자와 발행자 및 발행자와 가맹계약을 맺은 자(이하 '가맹점'이라 함)간에 준수할 사항을 규정한 사용계약을 체결한다. 또한, 이 계약서에는 판매수수료 및 대행 결제수수료 지분율(持分率)을 명시하고 있다.

우선 사용자들은 온라인 판매처에서 ①개인 스마트폰 켜기 → ②판매대행사 사이트 접속 → ③상품권 선택 → ④온라인결제 → ⑤상품권 수신(이미지가 포함된 MMS형태의 핀번호(PIN) 정보 전송) 과정을 통해서 온라인 상품권을 구매한다. 구매한 온라인 상품권을 이용해 사용자들은 ①온라인 가맹점 사이트 방문 → ②결제(상품권 핀번호 입력) → ③상품 및 서비스를 구매한다. 이 과정에서 상품권 발행사와 사용자 사이에서 전자지급결제를 대행하는 결제대행사가 개입하게 된다.

인터넷 상거래에서 전자지급결제대행사(Payment Gateway, PG)들은 지급결제 수단(신용카드, 계좌이체, 가상계좌, 휴대폰결제, ARS결제, 상품권결제)에 따라 전자지급결제대행서비스를 제공하고 있다. 사용자가 상품권 발행사 계정(id) 혹은 온라인 상품권 PIN번호를 입력하여 상품구매 대금을 결제하게 되면 PG사는 가맹점과 상품권 발행사 사이에서 수수료를 공제하여 가맹점에는 수수료를 제외한 대금을 지불하고 동시에 상품권 발행사에게 대행 수수료를 청구한다.(TYPE A.)

위와 같이 발행된 상품권은 할인된 가격에 판매되고 사용자는 가맹점에 상품이나 서비스를 이용할 때 구매(이용) 요금을 상품권으로 결제한다. 사용된 상품권은 가맹점이 발행회사에 제시하여 수수료를 제외한 현금을 지급받는다. 결제대행사(PG)들이 매월 발행사에 대금 지불정산을 요청하면 발행기업은 가맹점에 판매수수료를 제한 부분(예, 게임사 9%를 제한 91%)의 현금을 결제대행사(PG)에 입금하고 결제대행사는 결제 수수료(0.5%)를 제한 현금을 가맹점에게 송금한다. 이런 '상환' 과정을 통해 온라인 상품권은 상품권 발행사로 되돌아오고 상품권의 소비는 종료된다.

온라인 상품권을 온라인 쇼핑 제휴 가맹점에서 사용하기 위해서 지류 상품권이나 온라인 상품권에서 확인되는 상품권 핀번호(PIN)를 상품권 발행사 홈페이지에 등록하고 이를 선불전자지급 결제수단인 '캐시'로 전환하면 온라인 사용처의 유료서비스를 이용할 수 있다.

현재 상품권 발행사 쇼핑몰에서는 백만개 이상의 안드로이드 앱과 게임 컨텐츠를 제공하는 구글플레이스토어

의 온라인 컨텐츠를 구매할 수 있는 '선불전자지급수단'인 구글기프트 코드를 '캐시'로 구매할 수 있다. 구글기프트 코드는 공식 온오프라인 판매처에서 보통 3% 할인받아 구매할 수 있다. 만약 온라인 상품권을 8%에 할인받고 구글기프트 코드를 구매수수료 3%를 지불하여 구매하게 된다면 공식 판매처보다 많은 할인율(5%)로 구매할 수 있다(TYPE C.).

그 외 온라인 상품권은 백화점 상품권을 구매하는 용도로도 이용된다. 일반적으로 지류형 백화점 상품권은 오프라인 매장에서 2% 할인된 금액으로 구매할 수 있다. 그러나 온라인 상품권 판매대행사 사이트를 통해 구매하면 보다 저렴하게 구매할 수 있다. 지류형 백화점 상품권은 상품권 발행사 쇼핑몰에서 '캐시'를 이용해 5%의 수수료를 지불하여 구매 가능하며 배송업체를 통해 등기 우편물로 배송받을 수 있다.(TYPE D.)

또한 이런 거래를 지속하는 사용자들은 무통장입금으로 캐시를 충전할 때 지급되는 추가 지급 캐시로 백화점 상품권 구매 수수료를 절약할 수도 있다.

〈그림 7〉에서 가장 눈여겨 볼 부분은 온라인 상품권이 현금화하는 수단으로 활용되는 방법(TYPE B.)이다. 급전이 필요한 사람들은 자신의 신용카드 현금서비스를 5~23%대의 고리로 이용한다. 그런데 온라인 상품권 판매처에서 상품권을 8%에 할인받아 카드로 구매하고 해당 온라인 상품권 핀번호를 다시 상품권 매매업자에게 88%에 재판매하면 약 4% 할인받으면서 고리의 현금서비스 수수료 지급 없이 현금을 수중에 넣을 수 있다. 카드 매출 진작으로 카드사와 카드 소비자 모두에게 이익이다.

이런 소비형태를 일컬어 속칭 '상테크'라는 말로 손쉽게 상품권을 이용하여 현금을 만드는 방법이 인터넷에 공개되어 있다. 또한 메신저 피싱 조직은 이런 상품권 유통경로를 악용한 '상품권깡' 수법을 이용해 피싱 피해 수단으로 상품권을 편취하고 상품권 매매업자들을 통해 현금화하고 입금된 현금을 피싱 조직이 관리하는 대포통장으로 입금받아 피해금을 국외로 송금하는 수법을 사용하고 있어 문제가 심각하다.

3.3. 상품권을 이용한 메신저 피싱의 특징과 수사의 한계

3.3.1. 상품권을 이용한 메신저 피싱범죄의 특징

온라인 상품권 핀번호가 탈취된 사건의 초동 조사는 ①온라인 상품권 핀번호를 등록한 계정의 본인인증 정보 및 접속정보, ②온라인 상품권 핀번호 거래(이동)내역 자료를 확보하는 것부터 시작된다.

최근에 발생하는 원격제어 애플리케이션을 설치하게 한 사건의 경우, 온라인 상품권 핀번호를 편취한 후에 메신저 대화기록을 삭제함과 동시에 범행에 사용한 상품권 발행사 홈페이지 계정을 스스로 '탈퇴'하여 증거를 인멸한다. 이를 통해 메신저 서버에 저장된 접속 IP, 통신 식별번호 확인을 어렵게 만들며 '본인인증'(상품권 발행사에서는 사이버머니('캐시') 보유금을 제3자에게 상품권 번호로 선물하기 위해 본인인증이 필요하다. 사용자는 일반사용자, 휴대폰인증 사용자,휴대폰 본인인증 사용자가 있다) 정보를 확인할 수 없어 온라인 상품권 핀번호의 이동내역에 따른 최종 핀번호를 수취한 제3자의 계정을 수사하게 하여 수사를 어렵게 만든다.

상품권 발행사들은 가입자가 '탈퇴'하면 본인인증 기록을 즉각 삭제하고 있는데, 이 또한 수사를 어렵게 하는 요인이다. 상품권 발행사에게 탈퇴 처리된 회원의 본인인증 정보 '보관기간'을 강제하는 규정은 없다. 본인인증에 관한 정보는 상품권 발행사의 방침에 따라 해당 개인정보 또한 '삭제'되어 계정의 정보를 확인할 수 없는 것이 일반적이며 탈퇴하지 않은 계정이 확인되더라도 이는 '대포계정' 명의자로 혐의 관련성 있는 정보를 얻는 경우는 거의 없다.

온라인 상품권을 이용한 메신저 피싱의 특징 중 하나는 편취한 상품권 핀번호를 즉시 중국에 결탁하고 있는 중국 상품권 매입업자에게 전달한다. 중국 상품권 매입업자는 이를 다시 국내 매입업자에게 판매하여 편취한 상품권 판매대금을 신속히 회수한다. 〈그림 8〉과 같이 공격자는 범행 개시일에 온라인 상품권을 매입하여 줄 수 있는 국내 상품권 매매업자를 미리 확보하고 있다. '국내 상품권 매매업자'를 선정하고 예상 처분 시간을 예측함으로써 누적된 온라인 상품권 핀번호를 국내 매입업자에게 처리할 수 있는 수량을 나누어 전송한다. 만일, 피해자가 메신저 피싱 피해를 인지하여 상품권 발행사를 상대로 피해 접수하게 될 때까지도 편취 온라인 상품권을 처분하지 못하면 '통신사기피해환급법'에 따라 상품권 발행사는 피해자에게 '환불처리'되어 범행은 수포로 돌아가게 된다. 이 과정에서 최소한 피해 온라인 상품권 핀번호가 특정 계정에 등록되면 피해가 접수되더라도 상품권 발행사는 사용된 핀번호에 대해서는 환불을 거부한다. 반대로 미사용된 상품권 핀번호의 환불 요청 건에 대해서는 직권으로 청약을 철회하여 준다.

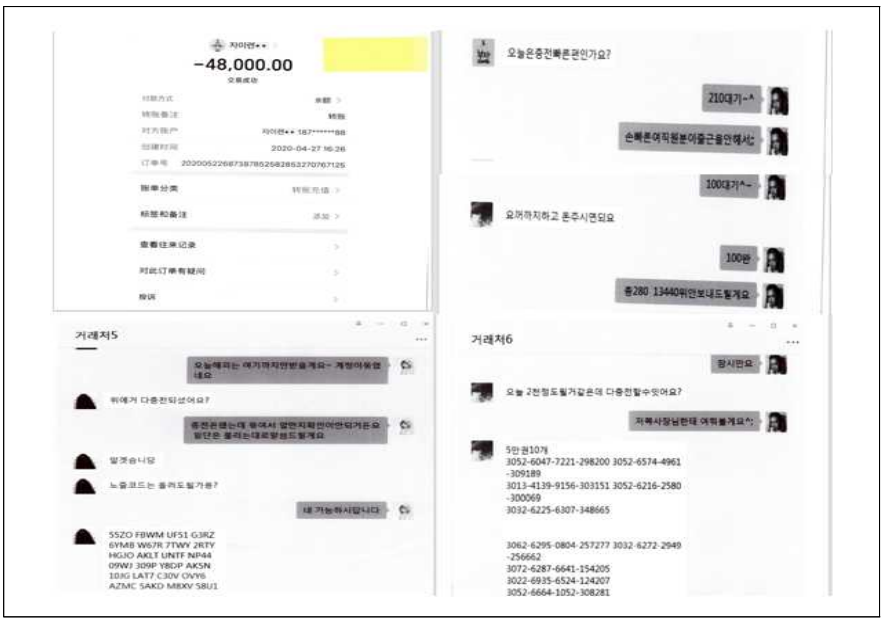
공격자는 국내 상품권 매입업자를 통해 처분하지 못한 수량에 대해 공격자 스스로 본인 명의의 상품권 발행사 사이트 계정을 통해 온라인 상품권 핀번호를 등록하여 사이버머니('캐시')로 전환하고 이를 이용하여 상품권 발행사 사이트에서 판매하는 전자캐시(ex, 구글기프트코드)를 구매하여 이를 국내 전자캐시 전문 매입업자에게

재판매하여 현금화한다. 국내 온라인 상품권 매매업자들은 공격자들로부터 거래가 요청된 건에 대해 사기 범행에 편취된 물건이라는 점을 모르는 채로 매입한다. 공격자는 판매대금을 중국 매입업자가 관리하는 대포계좌로 송금하게 하고 다시 이를 국내에 있는 인출책이 입금받아 국외로 반출하고 있다. 숙련된 공격자는 되도록 빨리 온라인 상품권 핀번호를 처분하기 위해 제3의 전기통신금융사기 피해자 명의를 도용한 상품권 발행사 계정을 이용해 편취한 온라인 상품권 핀번호를 상품권 발생회사 홈페이지에 등록한다. 일반적으로 메신저 피싱에 사용된 상품권은 피해 발생 직후 30분 내로 상품권 핀번호가 충전되는 것으로 확인된다.

편취된 온라인 상품권 핀번호는 국내 상품권 매매업자 명의의 상품권 발행사 계정에 등록되거나 공격자가 이용한 도용계정에 등록되고 이를 전자캐시로 전환한다. 결국, 편취된 온라인 상품권 핀번호는 '외부결제'에 따라 구글 기프트코드(메신저 피싱 범죄에서는 구글페이먼트(Google Payments)에서 판매하는 기프트코드로 세탁하는 경우가 일반적이다)와 같은 전자캐시로 변환되고 이를 구매한 국내 전자캐시 전문 매매업자의 이메일 계정으로 전송된다. 전자캐시 구매내역을 토대로 구글 기프트코드를 구글페이먼트에 제시하여 이용자 정보 및 사용 내역을 회신받는다. 그러나 이 계정 또한 〈그림 6〉과 같이 구글기프트 코드를 전문 매입하는 업자이어서 혐의 관련성을 확인할 수 없다.

3.3.2. 익명거래로 인한 수사의 한계

국내 상품권 매매업자는 편취된 온라인 상품권 핀번호를 적법하게 입수하였다고 하며 공격자가 제시하였던 사업자등록증, 구매대금 송금 내역을 제시한다. 일반적으로 메신저 피싱의 피해 온라인 상품권 핀번호을 충전한 계정의 명의자들은 대부분 국내 상품권을 매매하는 사업자로 확인되며 핀번호를 판매한 자는 중국에 상주하는 신원 미상의 자들이 대부분이다. 조사된 사건에서 중국의 매매업자들은 상품권 핀번호를 액면가의 80%로 매입하고, 거래증명을 하기 위해 중국 메신저 앱 채팅내역, 중국 계좌로 송금한 내역을 제시하며 사기 혐의 관련성을 부인한다.



〈Figure 8〉 Pin number transaction conversation record between Chinese messenger phishing organization vs Chinese acquirer

현실적으로 중국 온라인 상품권 매매업자들은 ①통상 거래 시중가보다 저가로 거래하고, ②하루 충전 목표치를 정해 거래하며, ③상품권 충전계정이 상품권회사로부터 동결되거나 동결해제 되는 시점을 예측하고 있기 때문에 메신저 피싱 조직 일원으로써 혐의 관련성을 부인하기는 어렵다. 중국 매매업자들의 이런 거래 행태는 메신저 피싱 조직의 일부로써 이들이 한국에서 벌어지고 있는 전기통신금융사기로 인한 피해 상품권 핀번호를 유통하여 범행하고 있다는 사실을 미필적으로나마 인식할 수 있는 요건으로 볼 수 있다.

중국 매매업자의 피해 상품권 매입거래 건에 관한 송금 내역이 확보되면 상품권 판매대금은 피싱 총책이 운영하는 대포계좌로 유입되고 다시 이를 '환치기' 역할을 하는 '자금세탁책' 계좌를 통해 최종 중국 위안으로 세탁되어 피싱 조직에게 최종 전달되는 것으로 추정된다.

일반적으로 편취된 상품권 핀번호에 대한 거래(이동)내역을 토대로 온라인 상품권을 처분한 자들의 혐의 관련성 있는 자들에 대한 조사는 아래와 같은 절차대로 진행되며 합동 수사를 하더라도 수개월 이상 소요된다.

〈Table 4〉 Investigation procedure of 'messenger phishing using gift certificate PIN number'

단계 1. 상품권 핀번호 충전계정의 계정정보, 접속기록, 충전내역, 외부결제내역 등 확보
단계 2. 상품권 사이트 계정명의자를 상대로 협의 관련성 확인
단계 3. IP 접속기록에 대한 통신자료제공요청자료 확인(90日內)
단계 4. VPN 접속기록 대한 역(逆) IP로 국내포털사이트 및 전자금융거래 접속확인
단계 5. 구글기프트 코드 사용자 확인
단계 6. 위 5.로부터 핀번호를 판매한 국내 상품권 매입업자 특정
단계 7. 위 6.의 사업자로부터 거래내역, 사업등록정보, 금융거래내역 확보 및 분석(국제형사사법공조 필수)
단계 8. 7.의 환치기 업자 특정(외국환거래법 위반 및 금융실명거래및비밀보장에관한법률위반 입건여부 검토)

온라인 상품권을 갈취한 범행에서 사용된 상품권 발행사 사용자 계정이 '탈퇴처리' 되면 '본인실명인증' 정보는 해당 상품권 발행사의 개인정보관리 지침에 따라 자체적으로 삭제 처리한다. 이로 인해 범행에 사용된 계정의 추가 범행 파악이 불가하여 추가 피해의 여부를 확인할 수 없다.

피해자와 공격자(Phishier)간의 메신저 대화기록 상 확보된 통신식별번호(휴대폰 번호)는 대부분이 다른 사건의 피해자 명의의 대포 명의이며 인터넷 접속 IP 등은 가상사설망을 통해 접속한 정보로써 실제 의심 국가에 파견된 영사의 도움 없이는 IP 수사가 어렵다.

결국, 인터넷 접속을 이용한 조사는 한계가 있으므로, 최종 상품권을 수취한 대상자들을 식별하고 이 대상자 중 협의자를 특정할 수밖에 없다.

이처럼 메신저 피싱의 범인들은 대포 명의 계정을 이용하고 이마저 추적을 회피하기 위해 가입한 인터넷 사이트를 탈퇴하는 경우가 대부분이다. 메신저 피싱의 범인을 특정하기까지 국내 온라인 상품권 사이트에서 이루어지는 방대한 양의 상품권 유통거래를 확인하는 데는 수사의 한계가 있다.

Ⅳ. 상품권을 이용한 자금세탁 방지를 위한 방법

앞서 본 바와 같이 상품권 매매업자들이 거래하는 상품권 핀번호가 전기통신금융사기에 관여되어 유통되는 거래 건일 것이라는 인식에 관해 그 미필적 고의를 입증하더라도 '상품권 핀번호'가 장물죄의 객체로 인정되지 않는 한 범죄 성립이 불가하여 처벌할 수 없다[3].

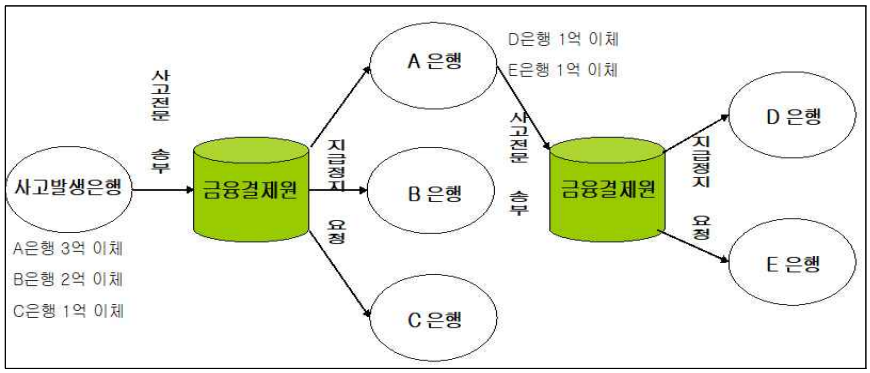
이에 포괄적인 범주에서 상품권 매매업자들이 전기통신금융사기의 자금세탁으로 유입되는 거래를 방지하기 위해 상품권 거래시 상품권 판매업을 취·등록한 사업자의 매입 후 재판매거래, 상품권 매입 직전의 판매자에 관한 실명인증을 위한 기록을 의무화하여 범죄로 발생한 상품권의 자금세탁을 방지하고 이를 통해 예방적 차원에서 피해를 최소화 할 수 있는 규제정책이 마련되어야 할 필요성이 있다.

이 장에서는 범죄로 기인한 온라인 상품권 핀번호가 상품권 유통망에 유입되는 사례를 방지하기 위한 정책 및 기술적 방법을 조사하고 이를 통해 지급정지 제도, 이상거래탐지시스템(Gift-Card Fraud detection system) 도입, 상품권을 거래하는 자들을 위한 정보공유시스템을 구축하는 등 기술적 방안에 대한 해법을 모색하고자 한다.

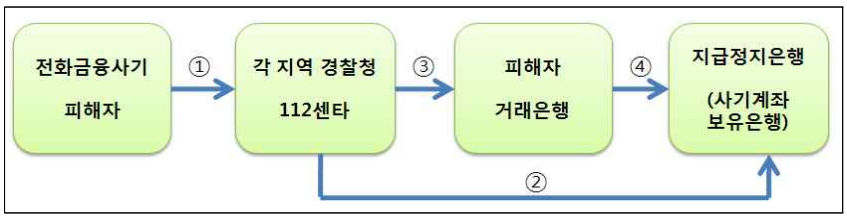
4.1. 지급정지 제도 도입

4.1.1. 지급정지 제도의 개요 및 도입사례

지급정지제도는 금융회사 내에서 사고가 발생한 경우, 사고발생 은행에서 금융결제원을 통해 사고자금이 이체된 경로를 실시간으로 추적 확인하여 즉시 지급정지시킴으로써 사고피해를 최소화시키는 제도이다. 금융당국, 금융결제원, 각 은행 등 협력 기관을 통해 은행연합회의 자율적인 규제 아래 금융회사 내부의 금융사고로 인한 피해를 막고 이체된 사고자금을 원할히 회수할 수 있도록 2005. 9. 도입된 제도로 '2007년 상반기 은행연합회와 은행이 시스템을 공동으로 구축하였다.



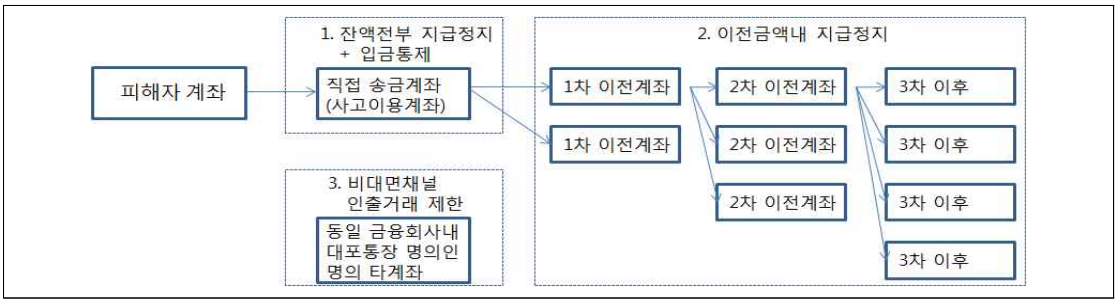
〈Figure 9〉 2005. Financial Accident Payment Suspension System



〈Figure 10〉 Flow of voice phishing damage payment suspension through 112

2009년 2월 17일 금융감독원은 인터넷뱅킹 사고에 신속 대응하기 위한 조치로 현재 운영되고 있는 전화사기자금 지급정지제도에 인터넷뱅킹, 폰뱅킹 등에 의한 전자금융사고도 포함해 은행, 증권사, 보험사 및 카드사에 확대 적용하였다. 피해금은『통신사기피해환급법 시행령』(11.9.30 시행)에 따라, 보이스피싱 피해자가 소송절차 없이 환급을 받을 수 있다.

또한 2014년 2월 14일에는 인터넷을 통한 금융거래시 정보통신망 등에 침입하여 부정한 방법으로 획득한 접근매체(보안카드, 공인인증서 등)의 이용으로 피해금의 타계좌 이전(이전계좌) 및 피해금 인출 피해가 증가하였는데 이를 억제하기 위해서 은행 권역 이외 인터넷뱅킹 서비스를 제공하는 타 금융권*에도 지급정지제도 적용 대상을 확대하였고 적용 범위도 해킹에 직접 이용된 1차 계좌와 이전계좌까지 확대하였다.



〈Figure 11〉 Flow of payment suspension for accounts used in hacking accidents

〈표 5〉와 같이 2013년 7월 3일 금융감독원이 발표한 자료에 의하면 2011년경부터 2013년 5월경까지 시행한 지급정지 피해구제로 인하여 실제 환급 결정된 금액은 신고된 피해액 1,543억 대비 21.7%에 달하였고, 〈표 1〉과 같이 2020년 기점으로 피해액 대비 환급율이 48.5%(20% 상승)대로 현저히 높게 상승되었다.

이를 통해 지급정지제도가 피싱 피해로 인한 피해자들의 피해를 최소화할 수 있는 제도라는 것은 확인된다.

〈Table 5〉 Status of Compensation for Phishing Scams

(단위 : 건, 억원)

	채권소멸 개시공고			채권소멸 사실공고		환급결정	
	피해액	건수	소멸액	건수	소멸액	건수	결정액
'11	392.2	6,884	117.8	1,155	23.9	509	10.6
'12	1,025.8	21,364	238.1	23,287	264.0	26,002	271.5
'13.1~5	125.0	6,434	60.3	5,500	53.8	6,485	53.5
합계	1,543.0	34,682	416.2	29,942	341.7	32,996	335.6

또한 금융감독원에 따르면 2015년 3월 기준 6.3만명의 피해자들이 지급정지 신청한 총 1,137억원의 채권에 대한 시간 경과별 환급금의 반환 실적보고에 따르면 범행 발생 직후 20분 내로 신고하면 피해금의 50% 이상을 환불받을 수 있다는 통계 데이터가 측정되었다.

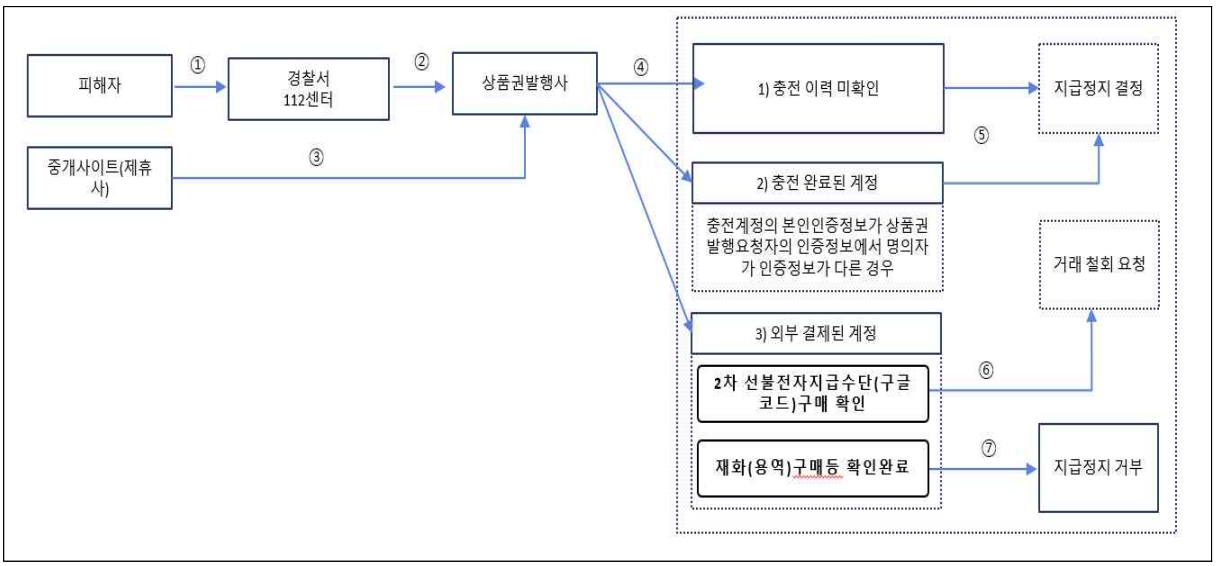
〈Table 6〉 Trend of refund rate by time of payment suspension after accident

구 분	10분	20분	30분	1시간	2시간
피해액 대비 환급금 비율	76%	53%	46%	36%	23%

4.1.2. 지급정지(외부결제 중지) 제도 제시 및 도입효과

일반적으로 상품권은 사용 가능한 가맹점의 확대로 사실상 유사통화 기능을 하고 있음에도 불구하고 한국은행의 통화지표에는 포함되지 못하고 있는 실정이다. 금융권 및 증권사에서 한정적으로 시행되고 있는 지급정지 제도를 선불전자지급 수단을 발행하는 상품권 발행사를 상대로 확대 적용한다면 상품권을 이용한 메신저 피싱의 피해를 구제할 수 있는 직접적인 구제 방법이 될 것으로 기대된다.

상품권 발행사는 이용자가 상품권 핀번호를 충전하면 이를 금전적 가치를 가지는 캐시로 전환하여주고 재화 또는 용역의 구입에 사용할 수 있는 선불형 전자지급수단을 제공하고 있다. 또한 금융감독원 전자금융감독규정 제2장 제5조(전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준)을 살펴보면 선불전자지급수단 발행 및 관리업을 영위하는 전자금융업자는 전자금융거래법상 전자화폐 혹은 선불지급수단의 미상환 등에 대비하여 약 1억~10억 수준의 보험에 의무적으로 가입하고 있다. 상품권 발행사에서도 해당 보험금을 활용하여 온라인 상품권 핀번호를 매개로 한 메신저 피싱 피해자들의 환급금으로 활용할 수 있는 시스템을 제안하고자 한다.



〈Figure 12〉 Payment suspension application plan at the stage of recharging and external payment by the gift certificate issuer

온라인 상품권이 상품권 권면에 부여된 핀번호를 앱(App) 이나 웹(Web)에서 접속하여 등록하는 경우 캐시(포인트)가 적립 또는 충전되고, 충전된 캐시는 신청법인과 제휴한 사용처에서 사용되는 경우를 가장하였다. 온

라인 상품권 핀번호가 유출된 사고에 대한 지급정지 시스템의 운영은 상품권 발행사에서 관리하고 콜센터는 피해 식별번호로 상품권 핀번호, 단말기 식별번호를 전달받아 지급정지를 접수한다. 콜센터로 접수받은 요청에 인터넷사고 전문 대응팀에 전달되고 연쇄적으로 해당 핀번호의 이동내역을 조사하여 해당 핀번호를 등록한 계정에 대해서 상품권 발행 사이트에서 상품권 핀번호의 사용거래를 일시 정지한다. 그리고 상품권 발행사와 제휴사는 상품권 이용에 대한 실효를 정지하기 위해서 채권소멸 절차에 관하여 상호 협력체계 시스템을 구성한다.

또한, 외부결제를 통해「전자금융거래법」상 '선불전자지급수단'으로 변환되어 유통된 제휴사는 지급정지를 연계하여 채권을 소멸하는 등 협력 체계를 구축한다.

4.2. 상품권 발행사를 위한 Fraud Detection System 도입

4.2.1 전자상거래에서의 FDS 개요 및 도입사례

인공지능 기술기반의 FDS는 인공지능 모델에 금융거래 '전체' 데이터를 주고 이중 의심거래가 어떤 것인지 알려주면 인공지능이 사기거래 패턴을 파악하여 새로운 금융거래가 사기 패턴과 얼마나 유사한지를 판별하여 사기거래를 식별하는 시스템을 말한다.

2001년 미국의 온라인 결제대행사인 '페이팔'은 해커의 공격으로 인해 피해자들의 계정에서 소액을 이체하는 사건이 반복으로 발생하여 FDS를 도입하였다. 2019년 부산은행은 '보이스피싱 이상거래 탐지시스템(V-FDS)'으로 수상한 자금을 탐지하는 이상거래시스템을 시험 도입하여 1개월 동안 50건의 사기 의심거래를 적발하여 4억 원의 이상거래를 방지한 바 있다.

실시간 온라인 전자거래가 발달한 국내에서는 액티브X 방식의 금융보안 모듈과 공인인증서 사용 의무화가 폐지되었고 2014년 심각한 전자금융사기 피해가 속출하여 모든 OS, 모든 브라우저에 공통적으로 적용할 수 있는 FDS 구축을 금융권에 의무화 하도록 한 바 있다. 또한, 핀테크 산업의 발전에 발맞춰 안전하고 간편한 새로운 금융 시스템과 FDS 고도화에 대한 수요가 비금융권으로 확산되고 있다. 전자금융거래의 거래량 증가와 간편 결제 수단의 다양화, 동시에 나날이 고도화되는 사이버 금융사기 방법들은 금융회사의 사기 탐지를 어렵게 만들고 있다.

최근에는 대량의 정보를 학습하여 예측 분류의 정확도를 높이는 머신러닝 기술이 발전하면서 금융회사는 FDS 성능 고도화 방안으로 머신러닝 기술기반으로 정확도를 향상하고 있다.

전자금융거래에서 이용자의 매체환경 정보, 거래정보, 사고유형의 정보 등을 수집하고 금융서비스의 특성에 맞는 탐지모델을 적용하여 이상거래를 차단, 추가 인증 등을 세분화하여 실질적인 탐지 및 탐지패턴을 유형화할 수도 있다.

사고로 판명 또는 분류된 이상거래가 타 금융회사로 전이되는 것을 방지하기 위해 적발된 이상금융거래 정보는 상호 공유된다. 예를 들어, 신규 계정을 생성하여 타인의 계정으로 전자상거래 사이트에서 결제시 이를 결제대행사(PG)에서는 도용된 계정의 승인 내역을 결제의뢰사에 통보해 사실을 확인할 수 있게 하여 사후 사기피해에 관한 환불을 요청할 때 근거정보로 제공하는 것도 FDS의 한 역할이다.

금융권에서는 2014. 7. 까지도 FDS 시스템이 신한은행과 부산은행만 적용되어 활발하지 않았으나[19], FDS 시스템 가동을 통해 인터넷 전문은행과 카드사의 앱(App)카드 고객 명의를 도용한 부정결제 건이 탐지되어 금융감독원은 시스템 구축을 권고하였으며 금융권과 수사당국은 2차 피해방지를 위한 추가 대응조치를 강화하고 있다[20].

금융권에 적용된 FDS 탐지룰의 예를 살펴보면 ①이용자의 전자금융의 이용환경(IP, MAC 등)의 고유정보가 변화되는 경우,②비정상적 사전행위(개인정보의 변경, 로그인, 오류한도 초과 발생) 시도, ③신규 계좌로 규칙적으로 정액(100~300만원)으로 반복 입출금되거나 해당 계좌와 연결된 거래에 직후 연결계좌에서 CD/ATM에서 인출되는 경우, ④급격히 증가된 로그인 시간과 로그인의 위치변화((사고의심 정보로 등록된 고유정보(IP/MAC)가 다수 명의의 계좌에서 로그인 시도하는 경우)의 변화 등을 들 수 있다[8][9][19].

2020. 10. 금융위원회는 오픈뱅킹 안정성을 강화하는 측면에서 기존 사전 정의된 규칙인 스코어링 방식에서 탈피하여 실시간 데이터 수집에서 탐지/분석/차단이 이루어지는 FDS 고도화를 2021년 하반기까지 추진하고 있다. 또한, 중소기업청은 지류상품권의 부정 유통 모니터링(FDS)을 통한 상품권깡으로 유입되는 거래를 단속하고 있고, 상품권을 불법 유통하고 할인한 가맹점에 대해서는 과태료를 부과하고 있다. 한국조폐공사는 지역사랑상품권의 부정 유통을 근절하기 위해서 이상거래 탐지기능을 탑재한 FDS을 구축하여 종이 및 모바일 상품권을 추적·관리하는 등 비정상적인 범주를 벗어난 행위를 모니터링 하고 있다.

그러나 일반적으로 유통되고 있는 국내 주요 상품권 발행사들이 발행하는 상품권 핀번호를 이상거래시스템으로 탐지하여 불법 행위를 적발한 사례는 확인된 바 없다.

4.2.2 상품권 이상거래 탐지시스템 도입 및 기대효과

메신저 피싱 조직은 불법하게 획득한 상품권 핀 번호를 현금화하기 위해 국내 온라인 상품권 매입업체를 통해 현금화하여 해당 자금을 대포계좌로 이체받는다. 메신저 피싱 조직 입장에서도 편취된 온라인 상품권은 중국에서 사용할 수 없는 유가증권이기 때문에 국내 전문 매입업자를 통한 매개 통로를 거칠 수밖에 없다.

국내 상품권 매입업체는 매입한 상품권 핀번호를 상품권 발행사 홈페이지에 등록하여 정상적인 상품권인지 확인한 후 결제수단인 '캐시'로 적립한다. 상품권 매매에 있어 상품권 핀번호를 상품권 발행사 사이트에 등록하는 행위는 필수적인 작업임이 분명하다. 이렇듯 범죄로 인해 거래되는 상품권 핀번호는 먼저 캐시로 충전되고 사후 '선불전자지급수단'으로 재판매하여 수수료의 차익분(豫 88%매입하여 91%에 매도하여 상품권 액면가의 3~4% 취한다)에 해당하는 수익을 창출한다.

상품권 발행사 사이트에서 상품권 핀번호의 유효성을 체크하고 캐시로 전환되는 작업이 필요하므로 상품권을 이용한 이상 거래는 상품권 발행사의 거래명세에 포집될 수밖에 없다. 만일, 국내 상품권 매입업체를 통해서 현금화된 범죄자금은 자금세탁책이 관리하는 불특정 다수의 대포 금융계좌로 입금되고 단기간에 다시 모계좌로 포집된다. 자금세탁책들이 움직이는 다수의 금융계좌에 관련된 인터넷뱅킹 접속주소, 접속 단말기(MAC), ARS 요청번호의 공통적인 속성을 연관 분석한다면 동일 메신저 피싱 조직에 의해 움직이는 금융계좌를 확보할 수 있고 이를 통해 피싱 조직이 접속하는 물리적인 위치를 특정할 것이다. 메신저 피싱 범죄의 결과자료를 분석하여 보면 범인들은 상품권을 세탁하기 위해 피해 상품권 핀번호를 충전하기 위한 용도로 타인 혹은 피해자 명의로 일시적으로 인증정보를 갱신하여 계정을 활성화(혹은 생성)하여 이용한다. 또한 해당 계정의 점유인증을 하기 위해서 해외에서 대포폰을 사용하였다[7].

메신저 피싱 발생으로 인한 상품권 발행사 사이트의 거래 특성은 신규 가입한 상품권 발행사 계정으로 ①상품권 권면금액 일회 최대 충전량으로 반복 충전, ②해외(VPN)에서 접속하여 충전하고 해당 해외 접속 IP 주소로 다른 계정들이 반복하여 충전을 반복, ③충전 직후 외부결제로써 구글기프트 코드를 구매, ④구매한 선불전자지급수단을 일일 최대한도로 선물하기 거래횟수가 보통 이용자들의 거래 평균치보다 월등히 높다. 만약, 이런 조건에 충족되는 상품권 이용자 계정은 자금세탁을 비롯한 사이버 범죄에 사용될 가능성이 농후하다.

메신저 피싱 조직이 이용하는 금융서비스에 관한 데이터를 누적하여 범죄정보를 프로파일링할 수 있다면 사후 의심거래로 인한 누적된 스코어를 반영하여 사전 탐지를 할 수도 있을 것이다.

따라서, 타인계정에 의한 부정 로그인 이벤트, 신규 계정 생성시 도용된 개인정보를 사용한 거래를 탐지하고 동종 상품권 발행사와 해당 정보를 공유하는 정보공유사이트로 이상거래 정보를 전파하고 이를 기존 금융 FDS 시스템에 연계한다면 온라인 상품권 발행 사이트에서 메신저 피싱 피해로 유입된 온라인 상품권 핀번호를 이용한 자금세탁을 방지할 수 있을 것이다.

구체적으로 신고 접수된 아이디의 상품권 매매 관련 정보(상품권 거래업체 사업자번호, 매입대금 송금계좌), 이용자 정보, 접속정보, 충전 및 외부결제로 이전된 선불 전자지급수단을 전달받은 계정정보, 거래패턴(충전 및 외부결제의 시간차), 접속IP(Geolocation), MAC, IMEI 등의 정보를 분석하여 의심거래 패턴을 학습하여 누적된 의심거래에 경보시스템을 구축하여 상품권 이상거래 패턴이 파악되면 이상 거래를 정보공유 시스템에 공유하거나 차단, 중지하는 등 강력한 대응도 가능할 것이다.

결과적으로 이런 이상거래 탐지 및 대응 프레임을 구성하기 위해서는 상품권 거래 사고 발생 또는 위험 발견에 따른 상품권 발행사와 금융사 간의 공동대응 체계를 구성하여야 할 필요성이 있다. 이처럼 상품권 거래에서도 상품권 거래의 특성과 상황을 고려하여 이상거래탐지시스템을 적용한다면 상품권을 매개로 한 부정이용거래 및 범죄자금의 세탁경로를 사전 차단하여 돈세탁을 방지하는 데 큰 도움이 될 것이다.

4.2.3 상품권 이상거래 탐지시스템(Gift-Card Fraud Detection System)에서의 지연결제 도입

상품권 핀번호를 상품권시스템에서 등록하여 사용하려는 자는 자신의 거래정보를 이상거래정보공유시스템상에 기본적으로 정보를 제공(이하, Opt-out방식)하여야 한다. 만약 해당 옵션을 철회하고 이용하는 자라도 사후 자신의 사고정보를 등록하는 시점에 '거래정보'는 이상거래정보제공시스템에 제공하는 것에 대해 동의를 받아 정보공유시스템상 거래정보를 G-FDS에 제공할 수 있다.

G-FDS 시스템에 상품권 거래정보 제공 옵션을 선택하는 사용자는 제3자로부터 전달받은 상품권 핀번호를 이용(충전·외부결제·환불)할 때 상품권 핀번호(PIN)에 관한 기존 사고 이력을 회신받는다. 상품권 거래정보에

대한 정보를 회신받지 못하는 상황에서는 최소 3시간 경과 후 해당 상품권에 대한 사용 권한이 부여되며, 만약 해당 상품권 발행번호의 사고이력이 확인되지 않는다면 하자 없는 개체로 취급하여 모든 권한이 부여된다. 또한, 이런 경우에는 사고정보 이력은 존재하지 않기 때문에 정보공유시스템에 사고정보는 전파(propagation)되지 않는다.

또한 한번이라도 사고정보가 등록된 발행번호라도 ①발행사, ②채권자(피해자 및 가맹점)의 요청으로 해당 상품권 핀번호에 대한 사고등록은 철회 가능하며 사고등록을 철회 요청으로써 정상 상태로 변경된다고 하더라도 정보공유시스템 상에는 해당 상품권 핀번호에 대한 사고이력 정보는 정상전이('사고->정상')로 정보가 유지되어 지속적으로 기록이 확인되어야 한다.

상품권 발행번호를 등록하여 사용하려는 이용자는 거래에 앞서 사고정보공유시스템으로부터 사고 이력에 대한 응답을 회신하여야 하기에 '지연결제 프로세스'가 상품권 발행사 홈페이지에 기본적으로 제공되어야 할 것이다. 이용자들의 온라인 상품권 등록 요청을 처리하는 웹 어플리케이션 서버(WAS)는 상호적으로 상품권 이상거래탐지시스템과 사고정보를 송수신하여 이상 거래에 관한 정보를 상시 업데이트하고 해당 정보를 통해 사용자가 요청한 상품권 발행번호에 관한 사고정보를 제공한다.

4.3. 상품권 핀번호의 공조시스템 도입

4.3.1. 정보공유시스템의 개요 및 도입사례

상품권 이상거래로 탐지된 정보는 타 정보공유기관들이 이상 거래에 대처할 수 있도록 공유되어야 한다. 상품권 이상거래 탐지상에서 정보공유시스템(Information Sharing System)이란 위 'G-FDS 이상거래탐지'의 프레임워크에 기술한 정보공유시스템을 통해 정보 가치적인 측면에서 하나의 새로운 이상거래 패턴을 생성하거나 업데이트, 혹은 삭제되어 공유 정보로써 현재성을 유지하는데 그 의의가 있다. 또한, 유관기관 간의 정보공유 서비스를 위하여 상품권 사고정보에 관한 통합 오프라인 문서가 관리되어야 할 것이다.

기존 금융보안원에서 운영되고 있는 이상금융시스템(FDS)에서 동일한 기능을 제공하고 있으므로 상품권 이상거래 탐지를 위한 시스템은 각 상품권 발행사에서 주체적으로 관리하되 사고정보를 능동적으로 금융기관의 이상금융시스템에 제공하여야 할 것이다.

실례로 상품권 발행사 사이트 이용자가 최근 다른 금융 도메인(ex, 휴대폰 별정 통신사 개통사이트)의 추가 인증이 발생한 사실을 인지하고 있었다면 추가 인증에 대한 이벤트는 이상거래의 가능성이 있고 이를 통해 파생된 탐지정보는 정보공유시스템의 공유정보를 송수신하는 프로토콜을 통해 사전 탐지될 수 있게 되는 것이다.

이런 이상금융 공유시스템에 관한 기준안으로는 'ITU-T 이상금융거래 탐지시스템 관련 표준(안)'의 부정사용방지 시스템의 단계별 세부 기능 정의에 '탐지단계'에서 '다른 조직과 규칙을 공유 가능할 수 있음'이라고 명시되어 있다.

4.3.2. 상품권 이상거래 정보공유시스템의 도입효과

온라인 상품권 핀번호가 이용된 전기통신금융사기 피해자의 보호 측면에서 세탁된 자금이 유입된 금융계좌에 대한 이상거래를 탐지하여 금융기관에 공유되는 정보는 수사기관의 적법한 영장에 기해 자금세탁을 차단하거나 피해자금을 추적하는 기능을 제공할 수 있다. 부수적으로 상품권 발행기업의 발행행위, 상품권 유통업자의 상품권 거래행위, 통신판매로 인한 상품권이 부당하게 거래되는 경우('상품권깡'), 사후 미상환 상품권에 대한 부당한 낙점 수입에 대한 규제로도 이상금융시스템이 도입되어야 할 이유이기도 하다.

폐지된 '상품권법'에서는 상품권의 거래에 관해 실명 거래를 보존하기 위하여 거래자 정보 및 실명을 위한 최소한의 정보, 상품권 발행번호 등을 거래장부에 기재하게 되어 있었다. 현재, 상품권 발행사는 상품권 발행에 관한 기록은 전자적으로 보관하고 있으며 회사규정에 따라 보관하고 있어 관리하는 정보의 종류도 상이하고 기업 자체 규정에 의해서 개별적으로 기록되고 있어 통제가 어렵다.

이렇게 상품권법이 폐지됨에 따라 상품권의 거래에 관한 기록 의무가 시행되지 않고 있는 상황에서 상품권 매매업체 스스로 소득세를 증빙하기 위해 기록하는 정보(매입대금 거래액, 구매대금을 지불한 은행계좌)를 관리하고 있다. 온라인 상품권의 투명한 거래를 보장하기 위해서는 최소한 거래정보에 대한 규격을 제시할 필요가 있다. 또한, 상품권 거래에 관한 정보를 공유하는 사이트는 현재까지 없다. 이에 온라인 상품권 이상거래탐지지스템(G-FDS)에 이상거래를 공유하기 위해 정보공유시스템을 도입하여야 한다.

4.3.3. 상품권 이상거래 정보시스템의 공유 정보

전기통신금융사기 혹은 '상품권깡' 등 상품권을 이용한 이상거래 패턴에 관한 정형화된 룰을 적용하여 탐지된 거래(case)에 대한 정보는 다른 상품권 발행사 및 금융회사, 혹은 통신회사에 상호 공유하여 해당 사고에 연관된 정보로 기인한 전자금융매체 혹은 도용된 계정으로 확인된 거래를 적시에 차단하여야 한다.

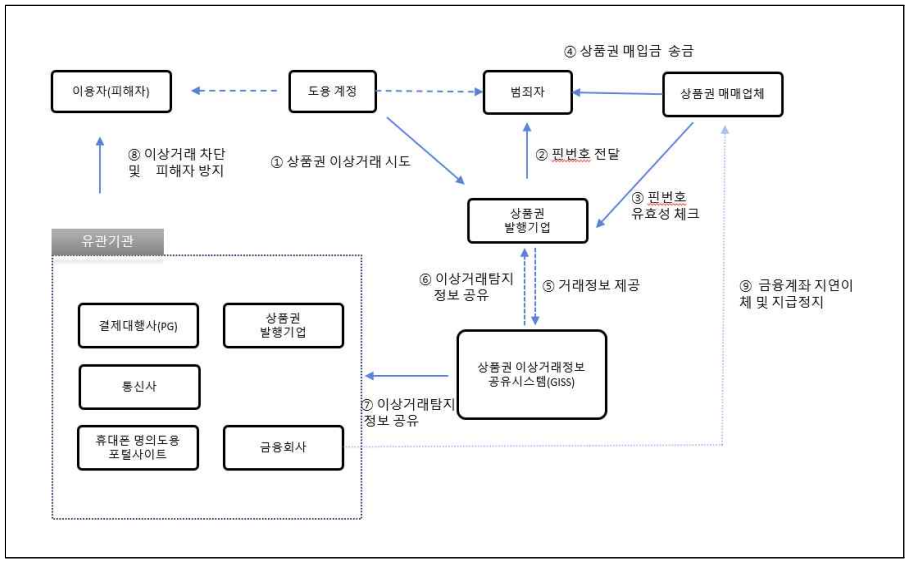
이상거래 사고등록을 하는 채널은 ①경찰서 사건접수(KICS), ②상품권 발행기업 콜센터, ③상품권 발행기업 홈페이지(상품권 매매사업자), ④금융감독원 홈페이지 등 4가지 경로로 사고정보가 최초 입력될 수 있다.

〈그림 13〉에 제시된 상품권 정보공유시스템의 개요도는 전기통신금융사기에 관련된 이벤트에 따라 정보공유의 기능을 나타낸 것이다.

공유되는 상품권 이상금융거래 정보가 지체없이 전파될 수 있도록 전문 규격을 표준화하고, 공유 절차는 유관기관 및 금융위원회 표준안의 권고 내용에 적시하거나 IETF의 'Sharing Transaction Fraud Data'[24] 의 내용을 토대로 적용되어야 할 것이다.

〈Table 7〉 Shared information of gift certificate abnormal transaction information sharing system

정보 유형	공유 정보
사고 정보	사고일시, 사고정보(디바이스 정보, 상품권발행사, 핀번호, 사고소유자식별번호(CI), 생년월일, 국가〈Geolocation Info〉 등), 사고유형, 사고 경중도, 사고로 전이된 결제서비스, 사고가 유발된 매체정보(OS, Browser, IMEI/MAC), 피해금액
이용자 정보	계정정보, 외부결제정보, 충전내역, 매매정보(계좌정보, 본인인증값(CI)),선불전자지급내역, 구매정보, 구매가격
상품권 정보	PIN 번호, 발행자정보, 발행가, 유효기간, 사용조건, 상환유무, 구매고객정보, 소멸시효 완성, 환불유무, 재발급 발송 유무, 구매 인증정보〈비식별화〉



〈Figure 13〉 System of Gift Certificate Abnormal Transaction Information Sharing System

Ⅴ. 결 론

지금까지 메신저피싱 사건에 상품권이 사용된 범죄 추적의 문제점과 이와 관련한 전기통신금융사기 사례 및 자금세탁 과정, 상품권 거래의 익명성으로 인한 상품권 매매의 문제점과 해결방법에 대해 정리하였다. 범죄자들이 상품권 거래를 통해 축적된 캐시를 쉽게 현금화할 수 있다는 점을 악용한 자금세탁의 경로를 봉쇄하기 위해서는 비정상적인 상품권 계정이 보유한 캐시가 현금화되는 것을 차단하는 것이 매우 중요하므로, 상품권 충전 사이트에서 캐시 결제에 대한 인증을 강화하고, Gift-card FDS 도입을 통해 이상거래 및 상품권 충전 계정을 탐지 대응하며, 상품권 현금거래와 관련하여 발생하는 범죄수익에 대하여 자금세탁방지제도를 도입할 것을 제안하였다.

본 논문에서 제안한 사항을 상품권 사이트에 적용하면, 정상적인 상품권 사용자들에게 불편을 주고, 가맹점의 수익 하락 및 상품권 매매시장의 침체, 범죄사례가 공론화될 경우 이미지 타격을 우려할 수 있을 것이다. 상품권 발행사에서 상품권을 재태크 내지 범죄로 기인한 온라인 상품권 거래 유입이 차단되면 발행량이 줄어들어 상품권 발행사의 수입이 감소할 것이라는 우려와 달리 장기적으로는 건전한 온라인 상품권 사용환경을 조성

할 수 있을 것이다. 그러한 예로 '휴대전화로 전송되는 모바일 상품권' 인지세 과세대상에서 제외되었던 모바일 상품권에 대해 2020년부터 3만원 이상 모든 모바일 상품권들은 모바일에서 구매할 때 인지세 부과가 시행됨으로써 건전한 문화 소비 혹은 재화를 소비하기 위한 상품권의 순기능을 하도록 하여 온라인 상품권 유통 시장의 투명성을 높여 선량한 시민들의 기회비용 손실을 감소시킨 사례가 있다[14][15]. 그리고 경찰청과 한국편의점협회 공동으로 편의점 손님과 직원을 대상으로 일정 금액 이상의 상품권이나 구글 상품권 카드를 구매하는 경우 포스(POS)기를 통해 메신저피싱 예방 경고 안내 화면 음성을 송출하여 상품권을 이용한 범죄가 발생하지 않도록 하는 범죄예방 활동이 긍정적으로 평가된 사례가 있다[16].

온라인 상품권 거래가 피싱범죄 및 자금세탁에 매개수단으로 악용되는 것을 방지하여 건전한 상품권 유통 시장 환경이 마련된다면, 범죄 피해를 구제할 수 있을 뿐 아니라 불법한 자금이 세탁되어 해외로 빠져나가지 못하게 할 것이다. 또한, 상품권 유통시장을 이용한 사이버 범죄의 감소와 피해금 회수에도 효과가 있을 것이며 상품권 발행사 및 매매업에 관련된 사업자들 또한 책임에서 자유로워질 수 있을 것이다.

참 고 문 헌 (References)

[1] Geum-Yeon Jeon,In-Seok Kim. (2016). A Study on the Institutional Limitations and Improvements for Electronic Financial Fraud Detection. The Journal of the Institute of Internet, Broadcasting and Communication, 16(6), 255-264.

[2] Sung-Cheon KIM, Dae-Pyo Jeon.(2012).A Legislative Study on Gift Certificate in Korea. Korean Consumer Agency, policy research report,1-224.

[3] Seok Soon Im I. S.-S. Necessity and Limit of the punishment of the Stolen Information Dealing. Korean Institute of Criminology and Justice, [s. l.], v. 27, n. 2, p. 23 - 48, 2015.

[4] SUNG KYU CHO; JUN MOON SEOG. : A Study on Countermeasures against Messenger Phishing using ARIT Technique. KIPS Transactions on Computer and Communication Systems, [s. l.], v. 2, n. 5, p. 223, 2013.

[5] Youn-Hee Jung. (2019). A Review about the Security of New types of Gift certifications. DONG-A LAW REVIEW(84), 325-346.

[6] HyoungSuk Ko. A Study on the New Gift Certificate Standardized Clause. National Assembly Research Service, [s. l.], v. 7, n. 1, p. 459 - 500, 2015.

[7] Hak-Jae KIM, Soo-Mee KIM.(2015).A Study on the System of Interception of Phone Number to Be Used In Criminal.Journal of Digital Forensics ,9(2),43-62.

[8] Eun Young Park, Ji Won Yoon.(2014).A Study of Accident Prevention Effect through Anomaly Analysis in E-Banking.The Jounal of Society for e-Business Studies,19(4),119-134.

[9] Eui-seok Jeong, Jong-in Lim.(2019).Study on Intelligence (AI) Detection Model about Telecommunication Finance Fraud Accident.Journal of the Korea Institute of Information Security & Cryptology,29(1),149-164.

[10] Bae Ji Hyo, Chae Su Yeol, Song Myeong Jun, Bang Kyeong Chan.(2019).Detection method through analysis of messenger phishing conversation.Proceedings of Symposium of the Korean Institute of communications and Information Sciences,(),537-538.

[11] Choi Kwan,Kim Minchi. (2016). A Study on the Modus Operandi of Smishing Crime for Public Safety. Jouranl of Information and Security, 16(3), 3-12.

[12] Jinhwa Son. (2009). The Nature of Electronic Negotiable Certificates. Journal of Payment and Settlement, 3(1), 44-76.

[13] Yeon-Jun, Choi,Seoung-Won, Choi. (2021). Messenger Phishing Modus Operandi in South Korea. Journal of Korean Public Police and Security Studies, 18(3), 241-258.

[14] Tax on paper gift certificates and mobile gift certificates for equity, Available: https://www.joongang.co.kr/article/22848782, 2022. 3. 16., confirmed

[15] In the case of reissuance of mobile gift certificates, whether stamp duty is excluded and whether joint payment by the issuer is made, etc., Available: https://txsi.hometax.go.kr/docs_new/customer/case/qna_view_answer.jsp, 2022. 1. 4., confirmed.

[16] Cooperation with the convenience store industry to prevent messenger phishing, Available: https://www.korea.kr/news/pressReleaseView.do?newsId=156454774, 2022.3. 16., confirmed

[17] Watch out for Twitter phishing...Note the DM that induces login, Available: https://www.bloter.net/newsView/blt200910290006, 2022. 1. 4. , confirmed

[18] Phishing aimed at Naver account is currently ongoing! How do I improve my account security?, Available: https://www.boannews.com/media/view.asp?idx=100560」, 2022. 2. 20. , confirmed.

[19] Simple payment "Security issue solved by FDS" Available:

https://www.ajunews.com/view/20141008105026783, 2022. 2. 20., confirmed.
〔20〕 570,000 cases of credit card information leaked, Available: https://www.boannews.com/media/view.asp?idx=81824, 2022. 2. 20., confirmed.
〔21〕 'Voice phishing' advances with malicious app phishing, Available: https://www.cctoday.co.kr/news/articleView.html?idxno=2094375, 2. 20., confirmed.
〔22〕 "Your NateOn KakaoTalk is dangerous", Available: https://www.enewstoday.co.kr/news/articleView.html?idxno=1292562, 2022. 1. 4., confirmed.
〔23〕 Seoul Central District Court 2015. 9. 10. 2015노2516
〔24〕 https://datatracker.ietf.org/doc/html/rfc5941, 2. 20., confirmed.

저 자 소 개

박 조 원 (Jowon Park)
준회원

2005년 8월 : 서울과학기술대학교 산업공학과 졸업
2016년 8월~2020년 1월 : 서울시경찰청 서울광진경찰서 수사과 사이버수사팀
2020년 2월~ 현재 : 서울시경찰청 서울강남경찰서 지능수사과 사이버수사팀
2018년 9월~현재 : 고려대학교 정보보호대학원 디지털포렌식학과 석사과정
관심분야 : 디지털포렌식, 모의해킹, 악성코드, 정보보호 등

이 상 진 (Sangjin Lee)
평생회원

1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
관심분야: 디지털포렌식, 심층암호, 해쉬함수