개인신용정보이용 신용카드범죄에 대한 대처방안

김 종 수*

〈목 차〉

〈요 약〉

현재 개인신용정보이용 신용카드범죄는 그 특성상 고도의 전문화와 광역화로 인해 피해 발생후 원상회복이 어렵고 범죄인의 신속한 검거와 처벌 또한 쉽지 않다. 소수의 범죄인들에 의해서 발생하던 예전의 신용카드 위·변조 범죄들은 현재의 신용카드 관련 범죄와는 유형과 양상이 사뭇다르다. 현대신용사회에서 개인신용정보의 중요성은 굳이 강조할 필요가 없다. 따라서 개인신용정보이용 신용카드범죄가 국민 생활에 끼치는 악영향은 한 개인과 신용카드가맹점, 그리고 신용카드회사 모두에게 엄청난 경제적 손실과 피해를 유발하는 것이다.

이 연구에서는 개인신용정보이용 신용카드범죄와 개인신용정보 부정이용범죄에 대한 효율적 대처방안들을 다음과 같이 제시하였다. 먼저, 신용카드정보 유출의 방지를 위한 대책으로서 카드사용자의 사용의식 전환, 신용카드매출전표의 인쇄내용 개선, PG(Payment Gateway) 업체 등을 통한 카드정보 암호화의 법제화를 들었다. 그리고, 비밀번호 입력에 대한 보완, 키보드 프로텍션(해킹방지) 시스템의 보급, 결제내역 즉시통보의무의 법제화를 들었다. 또한 다양한 본인 인증 방법으로서 전자인증서를 통한 인증, 생체인식 기술을 이용한 인증을 들었으며, 개인신용정보를 보호받지 못하는 나라에서의 신용카드사용을 제한하여 신용카드관련 피해 발생을 최소화하는 방안을 제시하였다. 그러므로 개인신용정보이용 신용카드범죄에 대한 효율적인 대처를 위해서는 카드사용자, 카드사, PG 업체, 정부 기관, 공인인증기관 등의 종합적인 협력과 노력이 요구되며, 경각심을 고취시키기 위한 처벌법규의 강화와 정책적 대안을 수립하여 현대사회에서의 건전한 신용문화를 형성하여야 할 것이다.

【주제어: 신용카드범죄, 개인신용정보, 전자인증서】

* 경운대학교 경찰행정학부 연구교수

Ⅰ. 서 론

1. 연구의 목적

최근 경기침체의 장기화에 따른 실업율의 증가와 이로 인해 양산된 신용불량자가 급증하여, 신용카드 관련 범죄가 갈수록 그 양상이 다양해지고 지능화된 수법으로 발전하고 있다. 이는 비단 어제 오늘의 일이 아니다. 특히 카드깡 등 신용카드 범죄는 신용불량자를 확대 재생산하는 악순환의 고리로 이어지고 있고, 카드빚을 갚기 위한 납치나 강도 등 강력범죄로 증폭되는 사례마저 빈번히 발생하고 있어 사회적 파장이 심각한 실정이다.

경찰백서에 따르면 신용카드관련 총범죄의 발생이 2003년 12월을 기준으로 전년 대비 7.7% 감소한 반면에 물품판매가장 현금대출 일명 '카드깡'은 4,780건으로 45.7% 증가하였고, 신용카드 부정발급은 2,051건으로 68.9%, 신용카드 위·변조는 224건으로 32.5% 증가하였다[1]. 경찰통계에서도 나타나듯이 분실 또는 도난카드사용 범죄나 탈세를 위한 카드가맹점 명의대여 등의 비교적 단순한 카드관련 범죄보다는 고도의 기술과 전문성을 요하는 범죄가 증가하고 있다. 특히 주목할 만한 것은 이러한 범죄의 대부분이 유출된 개인의 신용정보를 불법이용한 사기범죄라는 것이다. 최근까지도 훔친 신용카드매출전표(Sales Slip)의 신용카드정보를 이용하여 온라인상에서 물건을 구입한 후 이를 다시 되파는 등의 수법으로 거액을 챙긴 사건이 빈번히 발생하곤 하였다[2]. 이러한 유형의 범죄가 가능하였던 것은 신용카드 전자결제 시스템을 이용하는 경우에 실물 카드를 보유하고 있지 않더라도 신용카드번호와 유효기간 등의 신용카드정보만 알고 있으면 구매가 가능하다는것 때문이다. 이러한 도용피해를 막기 위해 신용카드번호와 유효기간 이외에 신용카드비밀번호와 주민등록번호를 추가로 입력하도록 하고 있었으나, 이러한 정보 역시도 쉽게 알아낼

1) 사이버경찰청(http://www.police.go.kr), 2004. 경찰백서.
2) 연합뉴스. 2002년 7월 25일자 사회면 '훔친 카드전표 이용 인터넷 사기' 기사 참조.

수 있는 경우가 많아 여전히 신용정보의 도용으로 인한 범죄는 꾸준히 증가하였다. 이러한 온라인상에서의 신용정보도용으로 인한 피해를 줄이려는 업체와 관련기관의 노력으로 현재에는 신용카드 전자결제시 금융기관의 전자인증서를 통한 인증시스템의 도입으로 같은 유형의 사기범죄는 발생하지 않는 듯 했다. 그러나 지금까지도 완전한 신용카드 전자결제 시스템을 구축해 놓고 있지 않은 일부 국내 쇼핑몰의 경우에는 이러한 확인조차 거치지 않고 있어서 여전히 피해발생의 소지가 다분하다고 할 수 있다. 이에 대한 법제도적·기술적 대처방안에 관한 연구는 아직 미미한 것으로 보인다. 특히 개인신용정보이용 신용카드범죄는 비교적 신종 범죄에 속한다고 할 수 있어 사실상 이에 대한 연구는 거의 드문 편이라 할 수 있다. 이에 이 연구는 인터넷 사이트에서의 신용카드 전자결제 시스템을 이용한 개인신용정보이용 신용카드범죄에 대하여 그 대처방안을 제시하는 것을 목적으로 한다.

2. 연구의 범위 및 방법

개인신용정보이용 신용카드범죄는 현재 상당히 심각한 실정이다. 최근 각 카드사에 접수되는 전체 민원의 상당수가 이러한 유형에 속하는 것으로 파악되고 있다. 대검찰청에서는 신용카드의 부정발급·불법사용·위조 및 변조, 다른 신용카드가맹점 명의사용, 그리고 신용카드정보 무단사용을 신용저해 5대 사범으로 지목해 이를 집중 단속하도록 전국 검찰에 지시한 바 있다[3]. 또한 경찰청은 현재 신용카드 범죄에 신속하게 대처하기 위해 금융감독원과 관할 경찰서간 공조망 구축을 추진하고 있다[4]. 그러나 검·경과 금융감독원 그리고 여러 관련기관의 신용카드관련 범죄의 척결과 방지를 위한 노력에도 불구하고 더욱 더 지능적인 파생범죄들이 발생하고 있다. 그리고 이러한 범죄에 이용하

3) 매일경제. 2002년 10월 10일자 경제면 '신용카드사범 특별단속' 기사 참조.
4) 공조망이 구축되면 현재 '피해자 신고→금감원→경찰청→지방경찰청→관할경찰서'인 신고체계가 '피해자 신고→금감원→관할경찰서'로 단축돼 피해자 신고에서 수사착수까지 2주일 정도 걸리던 시간이 대폭 줄어 발빠른 수사가 이뤄질 것으로 경찰은 기대하고 있다.

기 위한 신용카드정보를 대량으로 빼내거나 매매하는 행위, 심지어 신용카드 정보 전문 매매상까지 기승을 부리고 있는 실정이다. 따라서 이 연구에서는 기존의 신용카드범죄에 대한 논의와 더불어 좀 더 심도있고 근원적인 해결책을 강구하고자 한다. 특히 개인신용정보의 불법사용과 불법유출로 야기되는 파생범죄들의 위험성을 제시하고 기술적 부분의 한계를 지적함으로써 정보화 사회에서의 건전한 신용문화를 설계하고자 하는데까지 연구의 범위를 설정하였다.

이 연구의 방법은 개인신용정보 유출사례들과 불법사용 범죄들에 대한 자료를 발췌하기 위해 관련기사들에 대한 인터넷검색을 통해 각종 매체의 보도자료들을 확보하였고, 신뢰성있는 통계를 제시하기 위해서 경찰백서와 경찰통계연보를 활용하였다. 또한 연구의 특성상 기술적 부분의 한계를 극복하기 위해 정보통신관련 전문가와의 심층면접을 통해 내용을 보완하였다.

Ⅱ. 개인신용정보이용 신용카드범죄에 관한 이론적 고찰

1. 신용카드의 의의 및 거래구조

1) 신용카드의 의의

인류의 문명이 발달하기 이전에 상호간의 거래를 위한 지불수단은 잉여물품의 물물교환이었다. 이 후 인구의 증가와 교환경제사회로의 발전으로 물품의 교환과 유통을 원활하게 하기 위한 일반적 교환수단 내지 일반적 유통수단으로 만들어진 것이 화폐이며, 이는 동전이나 지폐의 형태로 제2세대의 지불 수단으로 널리 통용되고 있다. 현대사회로 들어서게 되면서 플라스틱의 혁명으로 불리는 신용카드는 화폐를 주조하고, 유통하고, 폐기하는 등의 화폐를 통용시키기 위해 또 다른 비용이 발생하게 되는 비효율적인 유통구조에 변화를 가

져왔고, 신용화폐(신용카드, 수표, 어음, 전자화폐 등)의 보편화를 통해서 경제 흐름의 투명화 및 상호간의 보다 객관적인 시각을 가지는 데 기여하였다. 하지만 이러한 신용카드에 대한 현대 자본주의 경제사회에서의 평가는 지폐나 동전 소지로 인한 불편함을 해소할 수 있는 편리한 지불수단이 될 수 있는 반면에, 성숙한 윤리와 책임감이 정착되지 않은 상태에서 신용사회로의 전환은 자칫 "도덕적 해이"로 이어질 수 있는 양면성을 지니고 있다고 할 수 있다.

신용카드의 개념은, 해당 신용카드 회사에서 신용카드 소지자가 구매하는 물품에 대하여 지불 보증을 서주고, 구매금액을 카드회사가 대신 지불하여 약정된 기간마다 지불된 금액을 신용카드 사용자와 정산해나가는 일종의 신용보증 수단이라 할 수 있다. 즉 신용카드는 구매자, 판매자, 지불자 간에 3자 계약에 의해 신용거래를 가능하게 하는 제3세대 지불 수단이다.

일반적으로 크레디트 카드(credit card)를 신용카드로 부르는데, 그 개념은 나라에 따라 조금씩 다르지만 이론적으로 보면 신용카드란 “신용카드회원이 대금을 즉시 지불하지 않고 지정된 신용카드가맹점으로부터 물품이나 용역등을 신용공여기간(usance) 동안 제공 받을 수 있음은 물론 신용카드회사나 제3자로부터 신용을 제공받을 수 있도록 신용카드 발행회사가 발급한 증표”를 의미한다(한상문, 1992:4). 즉 신용카드란 “신용을 매개체로 하여 신용카드회원의 가입신청에 따라 신용카드회사가 신용카드를 발행하고, 신용카드회원은 그 발급받은 신용카드를 이용하여 현금을 지급함이 없이 계속하여 반복적으로 신용카드가맹점에서 물품을 구입하거나 용역을 제공받을 수도 있음을 증명하는 지불수단”이라고 할 수 있다(최응렬, 1999:157).

〈표 2-1〉 신용카드의 유형

구분 기준	유 형
거래당사자 수	양당사자카드, 삼당사자카드, 다당사자카드
카드의 용법(이용목적)	물품판매용카드, 금전대부용카드, 기타서비스(숙박, 운송) 제공용카드
카드대금의 지불방식	일시불카드, 분할지급식카드
카드의 사용가능지역	국내카드, 국제카드
카드발행회사	은행계카드, 전업계카드, 백화점계카드
카드대금의 결제방식	신용카드, 직불카드, 선불카드

2) 신용카드의 거래구조

신용카드[5]에 의한 거래는 원칙적으로 신용카드회사, 신용카드가맹점, 신용카드회원의 3당사자간에 신용카드를 매개로 하여 행하여지는 거래로서 신용카드회원이 신용카드를 제시하여 신용카드가맹점으로부터 신용구매를 하면 그 대금을 신용카드회사가 신용카드회원 대신 신용카드가맹점에 지급한 후 신용카드회원으로부터 그 대금을 지급받는 것을 주요 골간으로 한다. 3당사자카드를 중심으로 신용카드의 거래구조를 살펴보면, 신용카드회사는 신용카드 발급신청서를 제출받아 이를 회원규약에 의거 심사하여 신용카드를 발급한다. 신용카드가맹점은 고객이 제시한 신용카드에 대하여 신용카드회사의 거래승인을 얻은 후 매출전표(sale slip)를 작성함으로써 상품매매거래가 이루어진다. 그리고 신용카드회사는 상품이나 용역을 제공한 신용카드가맹점으로부터 제출받은 매출전표의 이상유무를 심사하여 적합하면 매출액으로부터 일정한 비율의 수수료를 공제한 후 신용카드대금을 신용카드가맹점에 선지급하고, 약정한 결제일자에 신용카드회원에게 신용카드대금을 청구하여 회수함으로써 하나의 거래가 종결된다(최응렬, 1999:158).

5) 최초의 신용카드는 1953년 미국에서 발행된 다이너스카드(Diners card)이며, 우리나라에서는 1969년 신세계백화점이 신용카드를 발급하였으나 소수의 이용회원만이 사용하여 오다가 1980년 비씨카드와 국민카드가 보급되면서 신용카드 사용이 본격화되었다. 현재 국내에서 사용되고 있는 신용카드의 종류로는 각 은행마다 상품으로 판매하고 있는 은행계열카드와 전문계열카드 (LG, 삼성, 다이너스, 동양카드 등)가 있고, 해외발행카드(VISA, MASTER, American Express, Diners, JCB 등), 그리고 현금서비스가 제공되지 않는 단순 물품구매만을 위한 제한적인 용도로 사용되고 있는 백화점계열의 신용카드을 합쳐서 약 50여개의 신용카드가 있다.

2. 개인신용정보이용 신용카드범죄의 의의

개인신용정보이용 신용카드범죄란 부정한 방법으로 알아낸 타인의 신용카드 정보(신용카드번호, 유효기간, 비밀번호 등)를 이용하여 신용카드거래를 하는 행위를 말한다. 이 때 신용카드거래에는 주로 인터넷 쇼핑몰 등에서의 신용카드 전자결제 시스템을 이용한 구매 행위가 해당되게 되나 TV홈쇼핑 등에서의 텔레마케터를 통한 구매 행위도 그에 포함될 수 있다. 물건 등의 주문시 전화를 통해 텔레마케터에게 신용카드정보를 알려줌으로써 결제가 가능하기 때문이다.

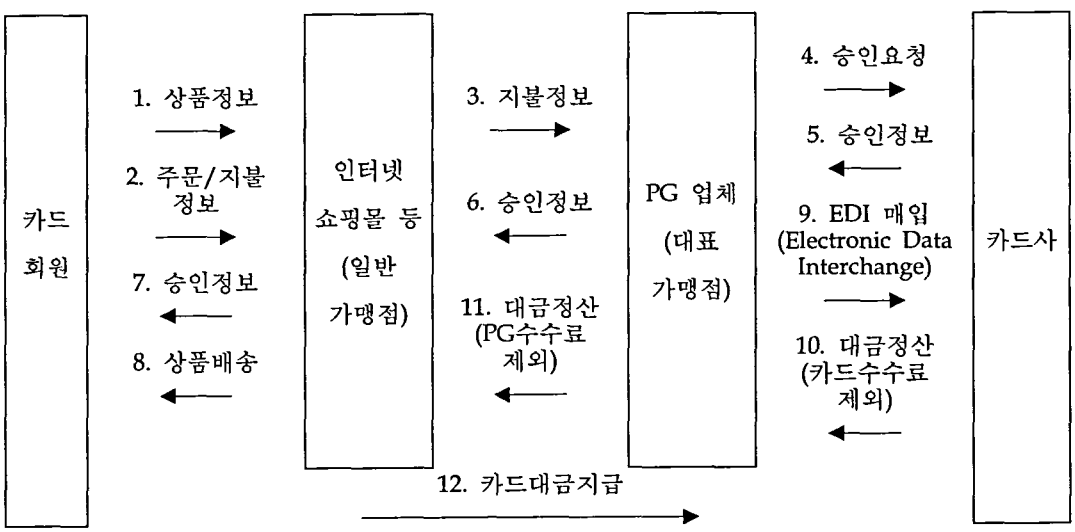
여신전문금융업법 제70조 제1항 제6호에서는 사위(詐僞) 그 밖의 부정한 방법으로 알아낸 타인의 신용카드정보를 이용하여 신용카드에 의한 거래를 하는 행위에 대한 처벌규정을 두고 있는데, 이 조항은 개인신용정보이용 신용카드범죄를 현행법적으로 가장 잘 정의하고 있는 내용이라 생각된다. 한편 이러한 행위를 위장(僞裝)이라고도 한다. 개방 네트워크 상에서 악의를 가진 제3자가 본인으로 가장하여 부정거래를 하는 것을 뜻한다(增田晋 ·飯田耕一朗 ·內山隆太郎, 1998:115-118).

3. 신용카드 전자결제 시스템의 의의

신용카드 전자결제란 신용카드회원이 인터넷과 같은 정보통신망을 통하여 물건을 구입하거나 용역의 제공을 받고 신용카드가맹점에 자신의 신용카드정보를 전송하여 결제하는 방법을 말한다(정진명, 2001:4-5). 이 때 이러한 신용카드 전자결제를 위해 구축된 시스템을 신용카드 전자결제 시스템이라 한다. 신용카드 전자결제 시스템은 주로 인터넷 쇼핑몰에서의 물건 구매나 유료 컨텐츠(성인정보, 영화, 게임 등) 제공 사이트에서의 서비스 구매에 이용된다. 인터넷 쇼핑몰 등을 운영하기 위해서는 구매가 발생할 때에 소비자가 대금을 신용카드를 통하여 인터넷상에서 쉽게 결제할 수 있는 방법이 제공되어야 하는

데, 이 때 사용되는 것이 바로 신용카드 전자결제 시스템이다. 즉 구매자가 상품이나 용역에 대한 대금을 지불하기 위해서는 보통 현금지급, 계좌이체, 신용카드결제(카드단말기 등을 통한 직접적인 대면 결제) 등의 방법을 통하여야 하나, 신용카드 전자결제 시스템을 이용하는 경우에는 인터넷상에서 몇 가지 신용카드정보를 입력하는 것만으로 즉시 결제가 가능한 것이다. 신용카드 전자결제 이외의 비대면 결제방식에는 인터넷 뱅킹 등을 이용한 계좌이체, 전자화폐사용 등의 방법이 있으나, 신용카드 사용이 대중화된 현재에는 그 어느 것도 이것보다 편리하지는 못하다. 그래서 현재 대부분의 국내 인터넷 쇼핑몰과 유료 사이트들은 신용카드 전자결제 시스템을 필수적으로 갖춰 놓고 있다.

<그림 2-1> 일반적인 신용카드 전자결제의 거래구조



자료: 코인츠 · 이니시스(2001:39 재구성).

위 <그림 2-1>은 일반적인 신용카드 전자결제의 거래구조로서 PG 업체가 결제처리와 결제까지 대행하는 구조(대표가맹점 서비스, 제3자 처리방식)를 알기 쉽게 그림으로 나타낸 것이다.

신용카드 전자결제 시스템을 인터넷 쇼핑몰 등에 구축하기 위해서는 신용카드 전자결제 프로그램을 설치하는 등의 기술적 조치가 필요하다. 이 때에도 역시 신용카드정보 등의 보안을 위한 암호화 과정은 필수이다. 그러나 인터넷 쇼핑몰 등 운영업체에서는 자체적으로 이러한 기술을 가지고 있지 않은 경우가 대부분이므로 전자상거래 솔루션을 제공하는 전문업체와 일정한 계약을 체결해야 한다. 그러한 전문업체를 보통 PG(Payment Gateway) 업체라고 부른다. 여신전문금융업법 제2조 제5호에서는 신용카드업자와의 계약에 따라 신용카드회원 등에게 물품의 판매 또는 용역의 제공 등을 하는 자를 위하여 신용카드 등에 의한 거래를 대행하는 자, 즉 결제대행업체에 대해 규정하고 있는데 이는 곧 PG 업체를 말하며 PG 업체는 신용카드가맹점으로 간주된다.

이러한 PG 업체는 신용카드 전자결제 시스템을 인터넷 쇼핑몰 등에 설치해 주어 이를 시스템적으로 대행하는 등의 업무 이외에 쇼핑몰 업자 등과 신용카드사와의 가맹점 계약도 대행한다.

즉 PG 업체의 서비스는 보통 ① 결제처리만 대행하는 서비스(자체가맹점 서비스) ② 결제처리와 결제까지 대행하는 서비스(대표가맹점 서비스)로 나뉘어진다(코인츠·이니시스, 2001: 49).

대표가맹점 서비스의 경우, 인터넷 쇼핑몰 등 운영업체는 신용카드사와 개별적으로 가맹점 계약을 맺을 필요가 없다. 그러므로 운영업체들은 PG 업체와의 한 번의 계약만으로 신용카드 전자결제 시스템과 신용카드사와의 가맹점 계약이 모두 갖춰지게 되어 신용카드 전자결제를 위한 모든 준비가 간단히 끝나게 되므로 매우 편리하다고 할 수 있다. 그래서 실제 거의 대부분의 운영업체들은 이러한 대표가맹점 서비스를 이용하고 있다. 이 경우 운영업체는 일반가맹점, PG 업체는 대표가맹점이 되는 관계가 성립하게 된다. 그리고 인터넷 쇼핑몰 등 운영업체(일반가맹점)는 PG 업체(대표가맹점)에 신용카드수수료와 결제대행 서비스에 대한 수수료를 합산한 금액(매출액의 약 5%)을 지불하게 된다.

신용카드 전자결제는 신용카드회원이 자신의 카드번호, 유효기간 등의 신용카드정보를 인터넷상에서 입력함으로써 이루어진다. 즉 신용카드회원이 신용카드정보를 가맹점(일반가맹점, 대표가맹점)에 전송하면 가맹점은 이를 다시

카드사에 전송하여 즉시 전자적인 거래승인을 얻는 방법으로 결제가 이루어지는 것이다. 결제가 이루어지면 가맹점(일반가맹점)은 즉시 상품을 배송하여야 한다. 이후에 가맹점(대표가맹점)은 신용카드회원으로부터 자신에게 전송된 신용카드정보 등을 매출전표에 기록·작성하여 이것을 카드사에 제시함으로써(매입) 대금을 정산하게 된다. 현재 PG 업체들은 이러한 매입 역시도 전자적 문서교환방식인 EDI(Electronic Data Interchange)를 이용하고 있다.

Ⅲ. 개인신용정보이용 신용카드범죄의 유형과 수법

1. 신용카드매출전표를 이용한 범죄

다음은 신용카드정보 부정취득의 방법을 기준으로 신용카드 전자결제 시스템을 이용한 개인신용정보이용 신용카드범죄의 실제 사례를 유형별로 나누어 본 것이다.

1) 버려진 매출전표를 주워 모은 경우

신용카드로 결제하고 난 뒤 버려진 매출전표들을 주워 모아 거기에 찍혀 있는 카드정보를 이용해 인터넷으로 공연티켓을 예매한 후 이를 현금으로 환불받는 수법으로 2백여만원을 챙긴 사례를 들 수 있다. 범인은 처음에 대형 음식점 앞 쓰레기통에서 남이 버린 신용카드매출전표를 주운 뒤 인터넷 티켓예매사이트에서 영화표 4장을 예매하고 이를 극장에 가서 취소하는 수법으로 3만원을 환불받았다. 그 후 범인은 70여 차례에 걸쳐 이와 같은 수법으로 수백만원을 편취하였다[6].

6) 오마이뉴스. 2002년 7월 5일자 사회면 '신용카드전표, 함부로 버리면 낭패' 기사 참조.

2) 매출전표를 훔친 경우

훔친 신용카드매출전표의 신용정보를 이용, 인터넷에서 물건을 사고 되팔아 거액을 챙긴 사례를 들 수 있다. 이것은 앞서 서두에서 잠시 언급한 사례이나 이를 좀더 자세하게 소개하면 다음과 같다. 명문 이공대 중퇴생 등인 범인들은 유흥비와 생활비 등으로 사용한 3,000여만원의 신용카드 연체대금으로 고심하던 중 신용카드번호와 유효기한만 알면 도박사이트나 인터넷 경매사이트에서 구매가 가능하다는 점을 이용하여 범행을 계획하였다. 그들은 식당에서 카드매출전표를 훔치거나 번화가를 돌아다니며 휴지통을 뒤지는 등의 방법으로 모두 2,400여장의 카드 매출전표를 확보했다. 그리고 이들은 확보한 매출전표에 찍혀 있는 신용카드번호와 유효기간 등의 신용카드정보를 이용, 인터넷 쇼핑몰을 돌아다니며 노트북, LCD 모니터, DVD 등 주로 고가의 물건들을 구입한 뒤 이를 경매사이트를 통해 되파는 방법으로 1억1,500만원을 벌어들였다. 또 도박사이트에서 동료에게 고의로 져주는 수법으로 1,500여만원의 신용카드 대금을 현금화하기도 했다[7].

또 길가에 주차된 차의 문을 열고 들어가 안에 있던 매출전표와 차량등록증 등을 훔쳐 이를 통해 주민등록번호, 카드번호, 카드유효기간 등을 알아낸 후 이를 이용해 인터넷 쇼핑몰에서 물건을 구입하는 수법으로 모두 3명에게서 1천5백여만원을 챙긴 사례도 있다[8].

2. 개인신용정보 역이용 범죄

개인의 신용정보를 이용한 불법행위들은 내국인을 포함하여 세계 각국에서

---

7) 국민일보. 2002년 7월 25일자 사회면 '신용카드전표주의! 휴지통 뒤져 카드번호 알아낸 후 수억 챙긴 일당 구속' 기사 참조.

8) 중앙일보. 2003년 5월 2일자 사회·경제면 '카드번호 알아내 인터넷 결제 피해 속출' 기사 참조. 같은 유형으로 차량 안에 있던 신용카드매출전표를 훔쳐 거기에 찍혀 있는 신용카드번호 등으로 유료 성인사이트에 가입해 8차례에 걸쳐 성인영화를 시청, 피해자에게 40여만원의 재산피해를 입힌 사례도 있다(굿데이. 2002년 12월 6일자 사회면 '타인 카드번호로 성인인터넷 영화 공짜 시청' 기사 참조).

우리나라를 표적으로 사기행각을 서슴치 않고 있는 실정이다. 이제는 국외에서 개인신용정보를 도용하여 신용카드를 위조하고 역으로 국내에 입국하여 마구잡이로 고가의 물건을 사들여 되파는 수법으로 범죄가 자행되고 있다. 비교적 내국인들이 관광을 많이 가는 동남아시아의 경우에는 현지에서 신용카드를 사용한 한국인들의 신용카드 정보를 빼내 신용카드를 위조하고 행동책들을 국내에 밀입국시켜 위조카드를 사용하여 카드깡을 하거나 고가의 물품을 구매하고 있다. 범행 대상도 국내 면세점에서 대형 할인매장으로 확대되고 범행 수법 또한 교묘해지고 있는 실정이다. 하지만 국내의 신용카드 사용자에 대한 신원이나 위조카드여부 확인이 매우 허술해 이들의 범죄에 대해 사실상 무방비로 노출돼 있다고 할 수 있다[9]. 최근 동남아, 중국, 일본, 미국 등 해외 각국의 범죄 조직과 결탁한 카드위조단이 국내 은행 발행 카드를 카드 리더기(card-reader · 복제기) 등으로 위조하고, 국내에 들여와 거액의 물품을 구입하는 조직적인 범행이 카드범죄의 주류를 이루고 있다. 이 사건의 경우 주유소나 유흥업소 등 신용카드 가맹점의 조회용 단말기에 특수장치를 부착하여, 신용카드의 마그네틱에 기록된 자기(磁氣)정보를 복사하듯 읽어 들이는 '스키밍(Skimming)' 수법으로 이용자의 개인정보를 훔쳤다. 이렇게 입수된 개인정보는 홍콩의 비밀 아지트를 거쳐 팩스로 일본에 보내졌고 일본에서는 카드위조 작업을 맡은 홍콩계 중국인들에게 1인당 2만엔 정도에 팔았다. 한편 자료를 입수한 위조 조직은 우선 아무것도 입력돼 있지 않은 '공카드'를 만드는 또 다른 조직에 한 장당 1만엔을 주고 회원번호와 유효기간 등을 새기는 작업을 맡겼다. 이러한 '공카드'가 완성되면 카드 뒷면의 마그네틱 테이프에 입수된 개인정보를 입력하여, 완벽한 위조카드를 만들어 냈다. 이렇게 만들어진 위조카드는 값비싼 상품을 마구 사들이는 전문조직에 한 장당 5만엔에서 8만엔에 팔리거나 위조조직이 직접 고가상품을 사들여 현금화하는 데 이용하였다[10].

9) 부산일보. 2004년 6월 26일자 사회면 '국제 신용카드 위조범죄 한국인 관관객이 표적' 기사참조.
10) 이는 2년전 일본에서 적발된 삼합회의 신용카드 위조 조직의 수법과 유사하다.

3. 신용대출을 가장한 사기범죄

신용도가 비교적 낮거나 연체정보로 인해 대출이 어려운 사람들을 대상으로 은행 예금 및 부금 가입을 통한 신용도 향상이 필요하다고 요구하며 접근하여, 인터넷 뱅킹에 가입시킨 뒤 관련 정보를 빼내고 예금을 부당 해지·인출하는 사례가 빈번히 발생하고 있다.

이들은 휴대전화가입자에게 무작위로 전화를 걸어 수천만원대 신용대출이 가능하다며 신용카드 비밀번호 등을 알아낸 뒤 카드깡 수법으로 거액을 편취하는 수법을 사용하고 있다.

사례: 모 텔레마케팅사 대표인 유씨와 속칭 '카드깡' 업체 H유통 등의 대표인 전씨는 각각 대상자 모집과 카드깡 업무를 맡기로 공모한 뒤 2003년 12월부터 2004년 4월 9일까지 유씨가 고용한 텔레마케터 10여명을 통해 전국의 휴대전화가입자 수만명에게 무작위로 전화를 걸었다. 이들은 "2,000만원까지 신용대출이 가능한데 신용불량 여부를 확인해야 하니 신용카드 번호와 비밀번호를 알려달라"고 한 뒤, 정모(43·여)씨 등 870여명의 카드로 전씨의 카드깡 업체를 통해 인터넷 쇼핑몰에서 물건을 산 것처럼 위장해 1인당 63만원씩 모두 5억 3,000여만원을 가로챘다. 이들은 또 신모(45)씨 등 113명에게는 가입비라며 63만원씩을 현금으로 입금받아 모두 4,500여만원을 가로챈 혐의도 받고 있다[11].

4. 허위 인터넷쇼핑몰을 이용한 사기범죄

최근 허위 인터넷쇼핑몰을 이용한 사기사건이 사회적 이슈가 되면서 많은 피해를 양산하고 있다. 수 많은 쇼핑몰들 중에서 비교적 저렴하게 물건을 구입하려는 서민들의 심리를 이용하여 대금만을 챙기고 쇼핑몰사이트를 폐쇄한 뒤 잠적해버리는 수법으로 사기행각이 이루어지고 있다. 실제 소비자보호단체

11) 한국일보. 2004년 5월 20일자 사회면 "신용대출함정" 기사참조.

나 기관에 접수되는 피해 사례를 보면, 고가의 상품이나 유명 브랜드의 상품을 싸게 판매한다는 광고성 e-mail로 고객을 유인한 뒤 현금으로만 결제를 받고 물품을 배송하지 않는 수법이다. 이는 2002년 많은 논란과 피해를 발생시킨 인터넷 전자상거래 업체 '하프플라자(www.halfplaza.com)' 온라인사건과 유사한 수법이다[12].

인터넷을 통한 온라인 거래는 상품을 파는 사람과 사는 사람이 대면하지 않고, 대금 결제 후 상품을 배송받는 '선지불 후배송'이 관행이어서 뜻하지 않게 사기를 당할 수 있다. 실제 대금을 송금했는데도 상품을 받지 못하거나 엉터리 제품을 받는 경우, 그리고 환불과 교환을 요구해도 이런저런 핑계로 미루다 결국 해당 사이트가 폐쇄돼 피해를 보는 경우가 해마다 늘고 있다. 이런 사기성 온라인 거래 피해는 당사자인 판매자에게 (또는 쇼핑몰과 연대해) 그 책임을 지우는 것이 당연하지만, 판매자가 사기성 부도를 내거나 잠적한 경우엔 보상을 받기가 쉽지 않다. 특히 온라인송금 같은 현금결제의 경우는 현행 법 테두리 안에서도 보상이 어렵다[13]. 그러므로 이러한 인터넷을 통한 온라인거래 사고 예방을 위해서는 인터넷 사이트가 '매매보호제도'를 운영하고 있는지부터 확인하는 것이 중요할 것이다.

사례: 허위 인터넷 쇼핑몰을 개설하여 회원들이 자신의 쇼핑몰에서 물건 구입시 입력한 카드정보를 빼내 이를 이용한 사례도 있다. 범인은 인터넷 쇼핑몰이 사업자등록 등을 하지 않아도 인터넷 홈페이지만 만들 줄 알면 누구나 만들 수 있다는 허점을 이용하여 사기 쇼핑몰을 개설한 후 회원들이 물건 구매시 입력한 신용카드정보를 이용하여 다른 쇼핑몰에서 1,000여만원 상당의 물건을 구입하고는 쇼핑몰을 폐쇄한 뒤 잠적하였다[14].

---

12) '경매+복권' 형식과 '시중의 절반 값'이라는 비정상적 영업으로 9만 명이 넘는 소비자에게 310억 원의 큰 피해를 준 '하프플라자(halfplaza.com)' 사건 같은 온라인 사기 사건이 있었다. 한국소비자보호원에 따르면 하프플라자는 주로 컴퓨터, 가전제품, 잡화 등을 판매하는 인터넷쇼핑몰로서 '제품을 반값에 판매한다'는 방법으로 회원을 모집하고 판매해 왔으나 2002년 11월 이후 '소비자가 대금을 지급한 후에도 제품 미배달', '장기간 제품배달 지연', '해약 후 제품 대금 미환불' 및 특히 '사업자 연락불통' 등의 피해상담이 소비자보호원에 집중적으로 접수됐다(동아일보 2005년 1월 27일자 '온라인사기거래 예방장치마련을' 이종인/여론마당, 기사참조).

13) 동아일보. 2003년 8월 26일자 경제면 '인터넷쇼핑몰 사기 단속시급' 기사참조.

5. 신용카드발급 무능력자를 이용한 사기범죄

사회적 보호대상자들인 노숙자들이나 지체장애인들을 대상으로 사기행각을 일삼는 파렴치한들이 역대합실이나 노숙자쉼터 그리고 기타 보호시설을 찾아다니며, 공공근로자를 선발하고 있으니 주민등록증을 맡기면 미리 돈을 준다고 속여, 정신지체장애인들과 노숙자 등 신용카드 발급 능력이 없는 타인의 개인 정보를 싼값에 사거나 속여 빼내는 수법으로 신용카드를 발급받거나 허위로 대출서류를 작성해 대출을 받는 사기유형들도 기승을 부리고 있다. 또한 이와 비슷한 유형의 수법으로는 '좋은 일자리를 제공한다'는 명목으로 노숙자들을 유인하고 말소된 주민등록증을 새로 만들어 은행통장을 개설하고 사업자등록증 등도 발급받아 이들의 명의로 유흥업소를 차려 매출전표를 허위작성하여 거액을 편취하는 등의 수법으로 명의도용 사기범죄들이 빈번히 발생하고 있다.

사례: 2004년 6월8일 노숙자와 지체장애아등을 속여 만든 신용카드를 이용해 대출과 카드깡을 한 혐의(영리약취유인 등)로 박모(52.노점상)씨가 구속됐다. 범인 박씨는 2000년 12월 초순경 경기도 송탄시에서 노숙생활을 하는 신모(50)씨에게 접근, '돈을 벌게 해주겠다'며 안산으로 데려온 뒤 신씨 명의로 신용카드를 만들어 대출과 카드깡을 하는 방법으로 3천만원을 편취한 혐의다[15].

6. 개인신용정보 중개상을 통한 불법거래

개인의 신용정보, 특히 신용카드의 정보유출은 심각한 재산상 피해와 더불어 사기피해의 이해관계자들의 법정다툼을 유발할 수 있다. 즉 신용카드회사와 카드가맹점 그리고 카드사용자 간의 피해보상 및 책임의 소재가 불분명하

14) 한국일보. 2002년 8월 21일자 사회면 '인터넷 쇼핑몰 사기 극성' 기사 참조.
15) 동아일보. 2004년 6월 8일자 사회면 '노숙자 속여 만든 신용카드로 대출' 기사참조.

여 오랜기간 법정다툼으로 전개될 우려가 많은 범죄이다. 이러한 사회의 공익적 피해를 양산시키는 개인신용정보 유출행위는 '익명의 바다' 내지는 '정보의 바다'라는 온라인상에서 그 범위가 짐작할 수 없을 정도로 넘쳐나고 있고, 그 해악성 또한 가공할 만하다. 또한 최근에는 온라인에서의 개인신용정보 유출행위가 주춤하는 사이 오프라인을 통한 개인신용정보 불법거래 행위가 만연하고 있다. 예전에는 신용카드발급자들이 회원들을 모집하여 신용정보를 작성하고 신용카드를 발급하는 과정에서 취득한 타인의 신용정보를 관련 업체들에 돈을 받고 거래하는 경우가 종종 발생했지만, 현재에는 각 신용카드사에서도 이러한 병폐들을 근절하고자 회원모집행위를 중단하고 있다. 그리고 신용카드 발급과정에서도 직접 비밀번호를 기록하지 않고 신용카드 수령 후 온라인 상에서 인증절차를 거쳐 회원본인이 직접 입력하도록 하고 있다. 이러한 절차상의 개선으로 카드발급과정에서의 신용정보 유출행위들은 많이 감소하였다. 그런데 최근에는 국가의 행정전산망을 취급하는 자와 개인의 신용정보를 관리하고 있는 이들이 불법적으로 개인의 신용정보를 개인신용정보 중개상에게 팔아넘기는 범죄행위들이 발생하고 있다.

사례 ①: 상근 예비역 김씨는 지난 9월부터 자신이 근무하는 읍사무소 PC를 이용하여 무단으로 국가행정전산망에 접속, 호적등본을 출력해 팩스로 송부하는 등의 수법으로 165회 가량에 걸쳐 건당 3만원씩 모두 500만원 가량을 받고 불법으로 개인정보중개업자인 박씨에게 개인정보를 제공한 혐의를 받고 있다. 김씨는 읍사무소 직원이 ID와 비밀번호로 접속해 놓은 국가행정전산망에 들어가 예비군 훈련 통지서 주소 조회 등을 한다며 무단으로 개인정보를 빼낸 것으로 드러나 국가행정전산망 관리에 문제점을 드러냈다. 한편 법무사 사무소 직원 정씨와 은행채권추심팀 직원 한씨 등은 이들이 불법으로 빼낸 정보를 이용해 법무사 사무소 운영과 채권추심 등 개인적인 영업에 사용해 왔다[16].

16) 부산일보. 2004년 11월 25일자 사회면 '개인신용정보관리에 구멍' 기사참조.

사례 ②: 이동통신사 직원 등이 5백여만명의 고객정보를 유출하다 경찰에 붙잡힌 데 이어 8백여만명의 개인정보가 신용카드사 경품 대행업자와 온라인 게임 사이트 운영자 등을 통해 새나간 사건이 검찰에 적발됐다[17].

사례 ③: 컴퓨터와 인터넷을 이용한 범죄를 수사하는 부서에 근무하는 검찰 직원이 업무상 취득한 2만6,679건의 신용카드 개인정보를 돈을 받고 유출한 사실이 드러났다. 이른바 '카드깡' 등 신용카드 관련 범죄수사 과정에서 수집한 신용카드 정보를 인터넷을 통해 유출하고 돈을 받은 혐의로 컴퓨터수사부 산하 인터넷범죄수사센터 일용직 직원 이모씨(28)를 2003년 11월 17일 구속했다.

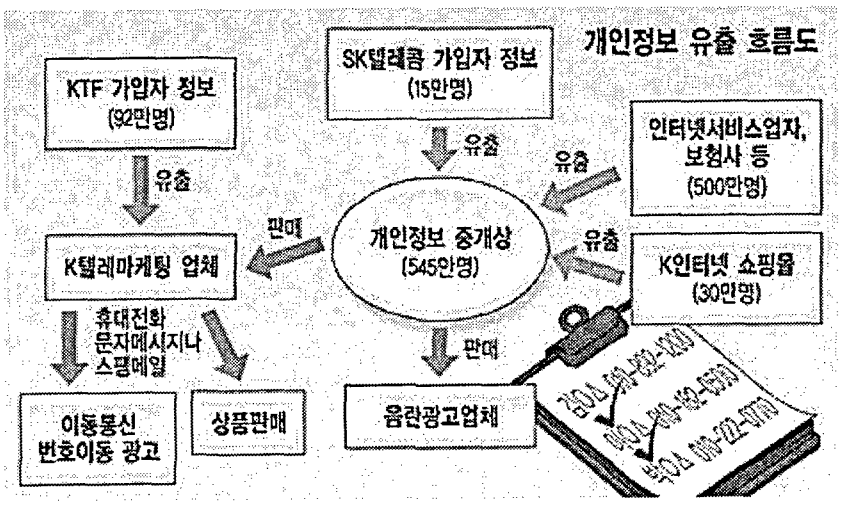
이씨는 2002년 8월부터 2003년 10월까지 업무상 수집한 2만6,679건의 신용카드 정보를 권모씨(25) 등 3명에게 e-mail로 넘겨주고 300여만원을 받은 혐의이다. 이씨는 이 가운데 116건은 이름과 주민등록번호, 신용카드번호, 유효기간은 물론 4자리의 비밀번호까지 알아내 유출했으며, 이 중 5, 6건은 실제 범죄에 이용됐다고 검찰은 전했다. 이씨는 신용카드 기본 정보에 나와 있는 비밀번호 앞 2자리와 카드 소유자의 생년월일이나 전화번호, 주민등록번호 등과 일치하는지를 확인한 뒤 일치할 경우 인터넷 신용카드 조회서비스를 이용, 최종 확인하는 방법으로 비밀번호를 알아냈다고 한다[18].

사례 ④: 2004년 10월 우리나라 인구의 8분의 1에 해당하는 637만명의 개인정보가 이동통신사 직원에 의해 유출되는 사건이 발생하였다.

---

17) 한국경제. 2004년 11월 8일자 사회면 '이동통신회원 정보 유출' 기사참조.
18) 동아일보, 2003년 11월 17일자 사회면 '검찰직원이 신용카드정보 빼내' 기사참조.

〈그림 3-1〉 개인신용정보 유출 흐름도



자료: http//www.kmib.co.kr/html/kmview/2004/1014/091958035911131200.html

서울경찰청 사이버범죄수사대는 14일 고객정보를 몰래 빼내 텔레마케팅업체에 팔아 넘긴 혐의(업무상 배임)로 KTF 수도권지역 대리점 담당 과장 김모(33)씨와 개인정보를 구입해 상품판매광고 등에 이용한 혐의(정보통신망이용촉진및정보보호등에관한법률위반)로 신모(26), 김모(31)씨를 구속했다. 김씨 등 7명은 지난 7월 주민등록번호와 휴대전화번호 등 자신이 관리하고 있던 고객 92만명의 개인정보를 텔레마케팅업체 K사에 1억3000만원을 받고 팔아 넘긴 혐의를 받고 있다. K사는 입수한 개인정보를 이용해 무차별적으로 휴대전화를 걸어 상품판매 등을 광고했다. 경찰은 또 인터넷을 통해 수집한 개인정보를 스팸메일과 휴대전화 문자 발송업자에게 판매한 혐의(신용정보의이용및보호에관한법률위반)로 중개업자 강모(29)씨 등 12명을 불구속 입건했다. 강씨 등 8명은 인터넷 개인정보 중개사이트에서 545만여명의 개인정보를 사들여 스팸메일과 문자메시지 등을 무작위로 보내 2억3000만원의 부당이득을 챙긴 혐의를 받고 있다[19].

19) 국민일보. 2004년 10월 14일자 사회면 '637만명 개인정보 유출됐다' 기사참조.

사례 ⑤: 신용카드사 직원과 카드정보 중개상을 통하여 입수한 약 600명분의 신용카드정보와 인적사항을 이용하여 인터넷 쇼핑몰에서 물품구매를 가장한 카드깡을 통해 1억원 상당을 가로챈 사례도 있다[20].

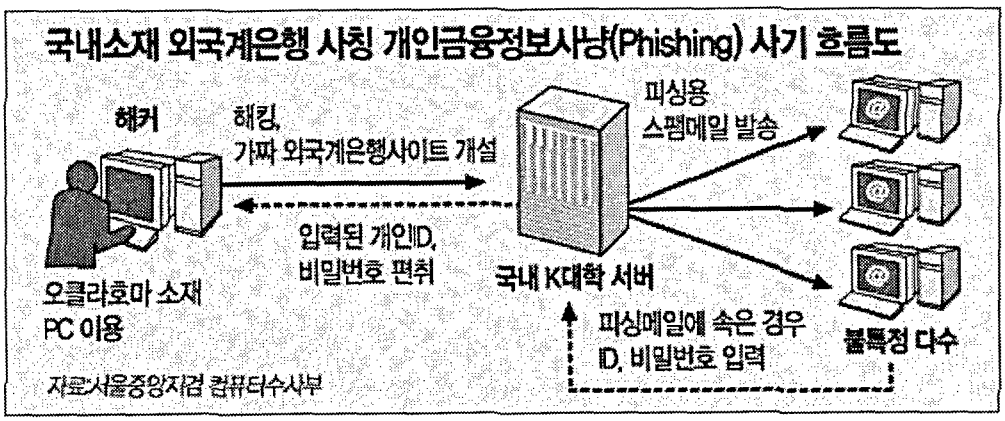
7. 개인금융정보 해킹을 통한 범죄

최근에 국내에서도 메일 발송을 통해 개인정보를 빼내가는 피싱(Phishing)에 대한 주의보가 내려져 네티즌들의 각별한 주의가 요구된다. 이미 미국, 영국 등에서는 피싱(Phishing) 사기가 이미 심각한 사회문제가 되고 있다. 지난 2003년부터 그 문제점이 제기되어 오던 피싱이 올들어 급속하게 증가하고 있어 조만간 국내에서도 상당수의 피해가 발생될 것으로 예상된다. 피싱은 개인 정보(Private Data)와 낚시(Fishing)의 합성어로, 범죄 용의자가 유명 회사의 홈페이지를 위조한 뒤 인터넷 이용자들에게 e-mail을 보내 위조된 홈페이지에 계좌번호나 주민등록번호 등의 개인정보를 보내도록 유인하는 신종 사기행위이다. 피싱사기는 인터넷 이용자들이 위조된 홈페이지에 개인정보를 보내면 개인계좌에서 돈이 빠져나가거나 개인정보가 범죄에 악용될 수 있어 대책마련이 시급한 현실이다.

---

20) 한국일보. 2003년 5월 3일자 사회면 '신용정보매매 인터넷서 극성' 기사 참조.

〈그림 3-2〉 개인금융정보사냥(phishing) 사기 흐름도



자료: http://www.donga.com/fbin/output?search=1&n=200410270295

실제로 2004년 10월 10일 신원 미상의 범인이 미국 오클라호마 소재 가정집 PC를 이용해 국내 K대학의 서버를 해킹한 뒤 H은행의 홈페이지로 가장한 개인정보사냥용 화면(피싱화면)을 설치한 것으로 드러나 국내도 더 이상 피싱사기의 안전지대가 아님이 밝혀졌다. 〈그림 3-2〉 에서처럼 공인인증서가 있어야 인터넷뱅킹이 가능한 국내 은행과 달리 H은행은 ID와 비밀번호만으로도 인터넷뱅킹이 가능하기 때문에 피싱사기의 대상이 된 것으로 보인다.

범인은 H은행 홈페이지로 가장한 피싱화면으로 곧바로 이동할 수 있도록 만든 스팸메일을 불특정 다수에게 대량 발송해 수신자들의 H은행 인터넷뱅킹 ID와 패스워드 등 개인정보 획득을 시도하였다[21]. 이러한 피싱사기의 접근유형들은 주로 유명 은행이나 카드사 등을 사칭하며, 계좌번호·카드번호·비밀번호 등의 확인 또는 갱신을 유도한다. 그리고 피해자가 확인 또는 갱신을 하지 않을 경우에는 거래가 중지된다는 등의 협박성 문구를 사용하여 정보 입력을 강제한다.

21) 피싱(Phishing): 개인정보(Private Data)와 낚시(Fishing)를 합성한 조어(造語)이다. 불특정 다수에게 이벤트 당첨이나 개인정보 확인 요청 등의 내용을 담은 거짓 e-mail을 보내는 수법으로, 수신자가 피싱화면으로 접속을 하게 되면 개인정보를 빼내 마케팅에 이용하거나 금융범죄에 악용하는 행위를 일컫는다(동아일보. 2004년 10월 27일자 경제면 '개인금융정보사냥(피싱) 주의보' 기사참조).

또 이들은 비교적 정교한 피싱화면으로 피해자들을 교란시키는데, 유명업체 마크, 로고 등을 이용하여 마치 해당 은행이나 카드회사에서 보낸 정상적인 메일로 보이게끔 가장하는 수법을 사용한다. 또 다른 유형은 인터넷포털사이트나 쇼핑몰 등을 사칭하여 경품당첨안내 또는 이벤트 참가 등을 유도하며 주민등록번호, 휴대전화번호 등의 개인정보를 입력하도록 유도하는 것이다. 일반인들이 이러한 피싱메일의 진위를 가려내기는 쉽지 않다. 가장 쉽게 진위 여부를 확인할 수 있는 방법은 이메일이 웹사이트 링크를 포함할 경우 그 URL을 체크하는 것이다. 이 때 잘못 쓰인 철자나 문법을 찾아보는 것이 한 가지 방법이다. 원래 글자와 비슷한 문자를 대신 써서 URL을 속이는 경우도 있다[22].

이러한 신종 수법에 의한 피해를 최소화하기 위해서는 사용자들의 각별한 주의와 함께 관련기관의 모니터요원들이 피싱에 대한 상시 모니터링을 실시하여야 한다. 또한 한국정보보호진흥원에 온라인 피싱사기 신고창구를 개설해 금융기관, 인터넷 쇼핑몰, 포털사이트 등과 연계해야 한다. 그리고 피해발생시에는 발송지 주소를 추적해 검·경에 신속히 수사를 의뢰하고 인터넷서비스제공사업자(ISP) 등에 해당 메일의 수신 차단조치도 요청하여야 할 것이다.

8. 기타 다른 수법을 이용한 범죄사례

1) 해킹을 통한 범죄

인터넷 쇼핑몰에 대한 해킹을 통해 회원 전원의 신용카드정보를 알아낸 뒤 이를 이용해 온라인 게임사이트 등을 돌며 사이버머니를 구입해 이를 되파는 방법으로 6,800여만원을 챙긴 사례도 있다. 해당 인터넷 쇼핑몰의 경우 공인된

22) 예를 들면 yahoo.com의 경우 yaho0.com으로 속일 수도 있다. 1 대신에 I, zero 대신에 O를 사용하기도 한다. URL이 길수록 주소를 속이기 쉽기 때문에 사이트 주소가 긴 것도 한번쯤 의심할 필요가 있다. 특히 사이트 주소에 흔히 '골뱅이'라고 부르는 @표시가 있다면 주의해야 한다. 대부분의 브라우저는 @표시 바로 앞의 모든 철자들을 무시한다. http://www.respectedcompany.com@thisisascam.com과 같은 주소는 Respected Company의 사이트처럼 보이지만 실제로는 thisisascam.com 을 방문하게 될 가능성이 크다(연합뉴스. 2004년 10월 19일자 사회면 '피싱 메일 식별 및 대응요령' 기사참조).

지불중개업체를 이용하지 않고 회사 내 서버에 직접 회원들의 카드번호와 비밀번호를 저장해 놓아 해킹을 당한 것으로 알려졌다[23].

2) 신용카드번호생성프로그램을 이용한 경우

신용카드번호생성프로그램을 이용해 만든 다른 사람의 신용카드번호로 인터넷 쇼핑몰에서 물품을 구입한 사례도 있다. 범인은 일부 인터넷 쇼핑몰의 경우 신용카드번호와 유효기간만 맞으면 물품을 구입할 수 있는 점을 이용해 다른 사람의 신용카드번호로 물품을 구입하였다. 범인은 인터넷에서 다운받은 신용카드번호생성프로그램을 이용해 신용카드번호 4개를 만든 후 인터넷 쇼핑몰에서 47차례에 걸쳐 1,200여만원 상당의 물품을 구입하였다. 범인은 먼저 주민등록번호생성프로그램으로 가짜 주민등록번호를 만들어 인터넷 쇼핑몰에 회원으로 가입한 뒤 다시 신용카드번호생성프로그램으로 신용카드번호를 만드는 수법을 사용하였다[24].

3) 신용카드 사진을 이용한 경우

신문에 자료사진으로 실린 타인의 신용카드사진을 보고 카드번호와 유효기간 등을 알아내 인터넷 쇼핑몰에서 물품을 대량 구입한 사례도 있다. 범인은 일간지 경제면 기사에 자료사진으로 실린 8개의 신용카드 중 2개의 카드번호와 유효기간을 알아낸 뒤, 인터넷 쇼핑몰에 친구의 아이디와 비밀번호로 접속하여 그래픽카드 등 컴퓨터 부품 300여만원 상당을 구입하는 등 22차례에 걸쳐 모두 1,100여만원 상당의 물품을 구입하였다. 그는 이것을 다시 경매사이트 등을 통해 되팔아 현금화하였다[25].

---

23) 동아일보. 2003년 4월 22일자 사회면 '인터넷몰 회원 6,500명 카드정보 해킹' 기사 참조.
24) 동아일보. 2001년 10월 29일자 사회면 '신용카드번호 다운받아 물품구입 대학생 적발' 기사 참조.
25) 국민일보. 2001년 8월 23일자 사회면 '신문에 난 카드사진번호이용 인터넷서 물품구입후 되팔아' 기사 참조.

Ⅳ. 개인신용정보이용 신용카드범죄에 대한 형사적 규제

1. 여신전문금융업법(제70조 제1항 제6호)

개인신용정보이용 신용카드범죄에 대한 형사적 규제에 있어서 현행법상 형사처벌 규정은 다음과 같다. 먼저 여신전문금융업법 제70조 제1항 제6호를 들 수 있는데, 여기서는 사위(詐僞) 그 밖의 부정한 방법으로 알아낸 타인의 신용카드정보를 보유하거나 이를 이용하여 신용카드에 의한 거래를 한 자를 7년 이하의 징역 또는 5천만원 이하의 벌금형에 처하고 있다. 즉 ① 부정한 방법으로 알아낸 타인의 신용카드정보를 보유하는 행위 ② 이러한 정보를 이용하여 신용카드 거래를 하는 행위의 두 가지 유형을 처벌하고 있는 것이다. 물론 두 가지 행위를 모두 한 경우, 즉 부정한 방법으로 타인의 신용카드정보를 알아내 이를 이용하여 신용카드 거래를 한 경우도 이에 해당된다.

사위 그 밖의 부정한 방법의 유형에는 제한이 없다. 사위란 거짓을 꾸며 남을 속이는 것을 말하며, 이것은 부정한 방법의 한 유형에 포함될 뿐이다. 신용카드정보란 카드번호, 유효기간, 비밀번호 등 해당 신용카드와 관련된 정보를 말한다. 신용카드에 의한 거래에는 주로 인터넷상에서의 신용카드 전자결제를 이용한 구매 행위가 해당되게 된다. 실물 카드 없이도 신용카드정보만 알고 있으면 결제가 가능하기 때문이다.

이 때 징역형과 벌금형은 이를 병과할 수 있다(동법 제70조 제7항). 법인의 대표자, 법인 또는 개인의 대리인·사용인 기타 종업원이 그 법인 또는 개인의 업무에 관하여 이러한 행위를 한 때에는 그 행위자를 벌하는 외에 그 법인 또는 개인에 대하여도 동 벌금형을 과한다(동법 제71조)[26].

---

26) 이를 양벌(兩罰) 규정이라 한다.

2. 컴퓨터등사용사기죄(형법 제347조의2)

다음으로는 컴퓨터등사용사기죄(형법 제347조의2)를 들 수 있는데, 여기서는 컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력·변경하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 한 자를 10년 이하의 징역 또는 2천만원 이하의 벌금형에 처하고 있다.

컴퓨터 등 정보처리장치란 자동적으로 계산이나 데이터의 처리를 할 수 있는 전자장치로서 사무처리에 사용하는 정보처리장치를 말한다. 입법취지에 비추어 재산의 득실, 변경에 관한 전자기록 등을 사용하여 정보를 처리하는 장치에 국한된다. 사무용 컴퓨터, 개인용 컴퓨터(PC) 등이 주로 해당되며 은행의 현금자동입출금기 등도 여기에 포함된다(임웅, 2002:343).

이 때 부정한 방법으로 취득한 타인의 진정한 신용카드정보를 컴퓨터 등을 통하여 신용카드 전자결제 등에 이용해 물건을 구매하는 등의 행위는 권한 없이 정보를 입력하여 정보처리를 하게 함으로써 재산상의 이익을 취득하는 행위에 해당되게 된다.

3. 정보통신망이용촉진및정보보호등에관한법률

'정보통신망이용촉진및정보보호등에관한법률'은 1999년의 '정보통신망이용촉진등에관한법률'[27]의 명칭을 변경한 법률로서 동법 제9장 제61조에서 제66조까지에서 벌칙규정을 두고 있다.

1) 업무상 비밀침해죄(제62조 제1호 내지 제3호, 제63조 제2호)

제62조 제1호 내지 제3호는 인터넷정보통신서비스제공업자, 제63조 제2호는

27) 동법은 정보통신망을 통하여 수집·처리·보관·유통되는 개인정보의 오·남용에 대비하여 개인정보에 대한 보호규정을 신설하고, 수신자의 의사에 반하여 광고성 정보를 전송하는 행위를 금지하는 규정을 두었다.

분쟁조정위원회의 분쟁조정 업무, 정보보호관리체계 인증 업무, 특정한 정보보호시스템의 평가 업무에 종사하거나 종사하였던 자의 개인정보에 대한 범죄에 대해 각각 5년 이하의 징역 또는 5천만원 이하의 벌금, 3년 이하의 징역 또는 3천만원 이하의 벌금을 규정하고 있다. 그러나 이는 일정한 업무에 종사하거나 종사하였던 자들이 주체가 되는 신분범의 성격을 띠고 있는 범죄로서 오프라인에서도 이루어질 수 있는 범죄이고 반드시 인터넷을 통하여 행해지는 것은 아니다.

2) 정보훼손 및 비밀침해죄(제62조 제6호)

본죄는 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설함으로써 성립하는 범죄이다. 형법 제316조 제2항의 비밀침해죄의 객체가 전자기록 등 특수매체기록이어서 전송중인 데이터는 객체가 될 수 없는데, 본죄는 전송중인 데이터도 비밀침해의 객체로 하여 범죄규정을 확장한 것이다. 또한 내용을 알아내지 않고 정보를 훼손하거나 침해하는 행위는 형법상 비밀침해죄에 해당하지 않는데, 이를 범죄로 규정한 것이다.

4. 신용정보의이용및보호에관한법률

신용정보의이용및보호에관한법률은 제32조에 벌칙규정을 두고 해당법규 위반자를 처벌하고 있다. 제32조[벌칙] ②에서는 제27조(업무목적외 누설금지등)을 위반한 자는 3년이하의 징역 또는 3천만원이하의 벌금에 처한다고 규정하고 있다.

1) 신용정보업자등과 제16조 제2항의 규정에 의하여 신용정보의 처리를 위탁받은 자의 임원 및 직원이거나 이었던 자(이하 "신용정보업관련자"라 한다)는 업무상 알게 된 타인의 신용정보 및 사생활등 개인적 비밀을 업무목적 외로 누설 또는 이용하여서는 아니된다.

2) 다음 각호의 ①에 해당하는 경우에는 제1항의 규정에 의한 업무목적 외 누설 또는 이용으로 보지 아니한다. 이 경우 신용정보제공·이용자간 또는 신용정보제공·이용자와 신용정보업자간에 제공된 신용정보의 보안관리대책을 포함한 계약을 체결하여야 한다.

① 신용정보제공·이용자가 다른 신용정보제공·이용자의 업무에 활용하도록 하기 위하여 자기의 업무와 관련하여 얻어지거나 만들어낸 타인의 신용정보를 제공하는 경우

② 신용정보제공·이용자가 신용정보업자의 수집에 응하여 자기의 업무와 관련하여 얻어지거나 만들어낸 타인의 신용정보를 제공하는 경우

3) 신용정보업관련자로부터 신용정보를 제공받은 자는 타인에게 그 신용정보를 제공하여서는 아니된다. 다만, 이 법 또는 다른 법률의 규정에 의하여 제공이 허용되는 경우에는 그러하지 아니하다. 그리고 권한없이 신용정보전산시스템(공동전산망을 포함한다)의 정보를 변경·삭제 기타 이용불능하게 하거나 권한없이 신용정보를 검색·복제 기타의 방법으로 이용한 자를 처벌하는 규정을 두고 있다.

5. 관련법규의 적용 및 비교

신용카드 전자결제 시스템을 이용한 개인신용정보이용 신용카드범죄에 대하여는 그 적용을 놓고 특별법인 여신전문금융업법(제70조 제1항 제6호)과 일반법인 형법(제347조의2)이 경합하게 되는데, '특별법은 일반법에 우선한다(lex specialis derogat legi generali)'라는 원칙에 의하여 여신전문금융업법(제70조 제1항 제6호)이 우선적으로 적용되게 된다. 따라서 개인신용정보이용 신용카드범죄는 거의 대부분 여신전문금융업법(제70조 제1항 제6호) 위반죄에 해당되게 된다고 할 수 있다.

그러나 여신전문금융업법(제70조 제1항 제6호)이 적용될 수 없는 경우에는 사

안에 따라 컴퓨터등사용사기죄(형법 제347조의2)가 보충적으로 적용되게 된다.

여신전문금융업법(제70조 제1항 제6호) 위반죄와 컴퓨터등사용사기죄(형법 제347조의2)의 법정형을 비교해 보았을 때, 징역형은 각각 7년 이하와 10년 이하로 후자가 더 높으나 벌금형의 경우에는 각각 5천만원 이하와 2천만원 이하로 전자가 2배 이상 더 높은 것을 알 수 있다. 실제 판결에서는 징역형보다 벌금형의 선고가 더 많은 점을 감안한다면 사실상 여신전문금융업법(제70조 제1항 제6호) 위반죄가 법정형이 더 높은 셈이다. 또한 여신전문금융업법(제70조 제1항 제6호) 위반의 경우에는 앞서 기술한 바와 같이 징역형과 벌금형을 병과할 수 있고 양벌규정까지 존재하고 있으므로 더욱 더 그러하다고 할 수 있을 것이다.

Ⅳ. 개인신용정보이용 신용카드범죄에 대한 효율적 대처방안

1. 신용카드정보 유출의 방지

1) 신용카드사용자의 사용의식 전환

사실 타인의 신용카드정보를 알아내는 것은 그다지 어려운 일이 아니다. 가장 쉬운 방법은 앞서 든 사례에서 본 것과 같이 타인의 신용카드매출전표를 이용하는 것이다. 신용카드매출전표에는 신용카드번호, 유효기간, 이름 등이 모두 찍혀 나오기 때문에 그것을 입수하기만 하면 매우 손쉽게 신용카드정보를 취득할 수 있는 것이다. 따라서 신용카드회원 각자가 매출전표의 관리에 각별한 주의를 기울이는 등의 신용카드에 대한 사용의식의 전환이 매우 중요하다. 즉 카드번호와 유효기간, 비밀번호, 주민등록번호 등의 정보가 유출되면 곧바로 자신에게 큰 피해가 돌아올 수 있다는 사실을 깨닫고 항상 정보유출에 주의하는 자세가 필요한 것이다. 특히 신용카드결제 후 받은 매출전표를 아무

렇게나 버리는 경우가 많은데, 매출전표를 폐기할 때에는 남이 알아볼 수 없도록 반드시 찢거나 잘라서 버리는 등의 습관을 들이는 것이 중요할 것이다. 위의 사례에서 보듯 신용카드정보는 버려지거나 분실·도난된 매출전표로 인해 유출되는 경우가 대부분이기 때문이다. 또한 피싱사기의 경우에는 사용자가 자신도 모르는 사이에, 자신의 정보를 가상의 금융기관으로 전송되는 형태이므로, 사용자의 주의가 많이 요구되는 것이다.

이에 대한 해결방법은 수 많은 매체를 통한 홍보가 이루어져야 하며, 각 금융기관이나 대형 온라인 쇼핑몰 등에서는 각 사이트를 통하여 공식적인 공지가 없는 한 개인정보를 요구하지 않지만 사용자의 부주의로 인한 문제가 있을 때는 마땅한 해결책이 없다. 그러므로 온라인쇼핑 부문에 있어서는 사용자가 물건을 받기전에는 결제가 이루어지지 않는, 즉 제3자가 입금하는 방식[28]이 전면 확대되어야 한다.

2) 신용카드매출전표의 인쇄내용 개선

현재 은행현금카드를 이용해 현금자동입출금기에서 현금을 입금 또는 출금한 경우에는 그 명세서에 찍혀나오는 계좌번호 등을 타인이 알아보는 것을 방지하기 위해 일부 숫자를 보이지 않게 아스트라표시(*) 등으로 처리하고 있다. 그러므로 이것과 마찬가지로 신용카드매출전표의 경우에도 카드번호나 유효기간의 숫자들 중 일부를 이러한 표시 등으로 보이지 않게 처리하는 방안을 검토해 볼만하다고 생각된다.

이러한 방안은 이미 일부 카드사 등을 중심으로 시행 단계에 들어가 있는데, 매출전표에서 유효기간이 기록되는 곳을 특수코팅 처리하여 숫자가 찍히지 않도록 하거나 롤 전표(일반 팩스용지에 인쇄되는 전표)의 카드번호와 유효기간 일부를 아스트라표시(*)로 기재되도록 하고 있다[29].

---

28) 예를 들면, 금융기관과 연계된 옥션의 '에스크로제'의 경우는 현재 경매관련 사이트에서 많이 사용되고 있다.

29) 머니투데이. 2003년 3월 6일자 증권면 '카드 부정사용 원천 차단 - 카드업계' 기사 참조.

3) PG 업체 등을 통한 카드정보 암호화의 법제화

현재 국내 인터넷 쇼핑몰의 대부분은 PG 업체를 통한 신용카드 전자결제가 일반화되어 있으나 아직도 소형 인터넷 쇼핑몰 중에는 공인된 지불중개업체를 이용한 신용카드 전자결제 시스템을 갖추어 놓고 있지 않는 곳이 상당수 있는 것으로 보인다[30]. 따라서 신용카드정보의 암호화가 제대로 이루어져 있지 않아 늘 해킹과 정보유출의 위험에 노출되어 있다고 할 것이다. 그러므로 신용카드 전자결제 시스템 구축시에는 반드시 공인된 PG 업체나 암호화 프로그램을 이용하도록 법제화하여 신용카드정보의 암호화를 법적으로 명확히 강제할 필요가 있을 것으로 생각된다. 현재 전자거래소비자보호지침(공정거래위원회고시) 제7조 제3항에서는 사업자는 전자거래의 안전성 확보를 위하여 보안시스템 구비 등 필요한 조치를 취하여야 함을 규정하고 있다.

2. 비밀번호 입력에 대한 보완

신용카드 전자결제 시스템을 이용한 구매는 카드번호, 유효기간 등의 간단한 신용카드정보 입력만으로 가능하다. 그래서 현재 국내 인터넷 쇼핑몰과 유료 컨텐츠(성인정보, 영화, 게임 등) 제공 사이트들의 거의 대부분은 타인의 신용카드정보를 이용한 도용을 막기 위해서 카드번호와 유효기간 이외에 비밀번호와 주민등록번호 등을 추가로 입력하도록 하고 있다[31]. 이 때 주민등록번호 등의 개인정보는 쉽게 취득할 수 있는 경우가 많으므로 결국 도용을 위해

30) 비대면성을 특징으로 하는 온라인 상에서의 안전한 결제를 위하여 키보드 입력정보 암호화 프로그램을 설치해야 한다. 이 때 여러번의 카드정보 입력시에 발생할 수 있는 문제를 해결하기 위하여 한번 카드정보를 등록해두면 그 뒤로 카드정보를 입력할 필요가 없도록 하는 프로그램도 설치하는 경우가 많다. 대표적인 것이 VISA의 안심결제(삼성, 엘지, 현대카드 등)와 은행계 카드와 BC카드 계열의 ISP이다. 이 프로그램들은 한번 카드 정보를 카드사의 웹사이트에 등록해 두면, 그 뒤로 카드의 번호와 비밀번호, 유효기간의 입력을 하지 않아도 된다.

31) 정보입력시 아예 주민등록번호를 입력하지 않게 하는 방안도 강구되어야 한다. 인터넷서점 http://www.amazon.com 에서는 서적구매시 주민등록번호를 입력하지 않고, 카드정보만으로 인증절차를 거치면 서적을 구매할 수 있도록 하여 절차를 단순화하였다. 복잡한 절차는 그 만큼의 정보유출가능성을 가지고 있고, 불법이용가능성 또한 확대될 수 있으므로 간략한 입력절차를 통한 견고한 인증시스템의 개발이 필요하다.

서는 비밀번호를 알아내는 것이 가장 핵심적인 사항이 될 것이다.

통상 주민등록번호는 13자리 중 뒤 7자리, 비밀번호는 4자리 중 앞 2자리의 입력을 요구하고 있다. 그러나 비밀번호 입력의 경우 상당한 문제점을 지니고 있는 것으로 보인다. 즉 4자리 중 2자리만 입력하도록 함으로써 지속적인 입력[32]을 통해 그것을 맞힐 수가 있는 것이다. 일부 쇼핑몰의 경우 비밀번호 입력을 3회 이내로 제한하고 있어 연속으로 3회 이상 비밀번호가 틀릴 경우 카드사용이 중지되기도 하지만 대부분의 쇼핑몰에서는 비밀번호 입력 오류시 다시 주문화면으로 돌아가 작성하기만 하면 되도록 하고 있다. 그러므로 비밀번호 입력에 대한 보완이 시급하다 할 것이다. 이에는 여러 가지 방안이 있을 수 있겠으나 4자리 모두 입력하도록 하고 연속 3회 이상 입력 오류시에는 카드사용이 중지되도록 하는 방안이 가장 좋을 것으로 생각된다. 이런 경우에는 입력을 통해 우연히 비밀번호를 맞힐 확률이 3/10000, 즉 0.03%로서 사실상 비밀번호를 맞힐 가능성이 거의 존재하지 않는다고 볼 수 있다. 또한 비밀번호의 자릿수를 6자리나 8자리 등으로 좀더 늘리는 등의 방안도 고려해봄직하며, 이에 대한 PG 업체와 카드사 등의 프로그램 개선의 연구가 필요할 것이다.

3. 키보드 프로텍션(해킹방지) 시스템의 보급

암호화가 이루어지지 않은 온라인 상에서의 키보드 입력정보는 인터넷의 특성상 보안을 전혀 보장할 수가 없으며, 약간의 해킹 지식만으로도 그 정보를 모두 볼 수 있다. 예를 들면, 어떤 목적으로든 간에 네트워크 데이터를 감시하는 프로그램을 설치해 두면, 보안되지 않은 정보는 그대로 노출된다. 이를 위하여 도입된 것이 키보드 프로텍션 시스템이며 BC카드사 등에서 사용하고 있다. 다만 이 때 팝업창으로 설치여부를 묻게 되는데, 대형기관의 경우에는 그 안전성이 보장된다고 볼 수 있겠으나, 인지도가 거의 없는 쇼핑몰의 경우에는 개인정보 유출의 가능성이 있다는 것이다.

32) 00, 01, 02, 03, ... 96, 97, 98, 99의 순서 등으로 입력해보면 될 것이다. 이 경우 모두 100개의 숫자 밖에 되지 않으므로 비교적 쉽게 맞힐 수 있을 것으로 보인다.

또한 웬만한 사이트에 접속시(특히, 성인물 사이트)에 본인인증을 위한 정보를 입력하라고 요구하는 경우가 많은데 이 경우 주민등록번호와 성명으로 인증하기 때문에 노출의 위험이 당연히 존재한다. 경우에 따라서는 신용카드 정보와 유효기간을 입력하라고 요구하는 경우가 있는데, 예전에도 나타난 문제지만 신용카드 번호와 유효기간을 알면 카드사용자의 의사와는 상관없이 결제가 이루어진다. 이 때 카드를 해지하지 않는 한 결제를 막을 수가 없다. 또한 대부분 외국에서 영업하는 경우가 대부분이므로, 그 사이트의 운영자를 국내법으로 처벌할 수는 없다. 범죄인인도협정이 맺어져 있는 경우라도 마찬가지일 것이다. 그러므로 키보드 해킹에 의한 피해를 최소화하고 개인신용정보의 유출을 막기 위해서는 키보드 프로텍션 시스템을 신용카드결제시스템을 사용하는 모든 부문에 확대하여 관련업체와 인증기관들이 이러한 보안서비스를 제공해야 할 것이다.

4. 결제내역 즉시통보의무의 법제화

고객의 신용카드 전자결제시 카드사가 그 결제 내역을 휴대폰문자메시지(SMS), e-mail 등을 통해 즉시 사용자에게 통보하는 것을 법률적으로 의무화하여 규정하는 방안이 필요하다. 이렇게 할 경우 본인이 결제하지 않은 내역이 통보되면 조기에 자신의 카드도용여부를 알 수 있게 되어 피해를 최소화할 수 있게 될 것이다. 현재 일부 카드사에서는 이와 같은 결제내역 즉시통보 서비스(SMS, e-mail 등 이용)를 실시하고는 있으나 월 일정액의 요금을 지불하는 유료 서비스 형태로 운영되고 있는 실정이어서 사실상 그리 큰 효과는 없다고 볼 수 있다.

전자상거래등에서의소비자보호에관한법률 제8조 제3항에서는 전자상거래사업자와 전자결제업자 등은 전자적 대금지급이 이루어진 경우 전자문서의 송신 등(전화·모사전송·이동전화단말기 등의 이용)의 방법에 따라 소비자에게 그 사실을 통지하여야 함을 규정하고 있으나 카드사에 대해서는 이러한 의무를

부과하고 있지 않다. 실제적으로 전자상거래사업자나 전자결제업자의 소비자에 대한 결제 사실 통지는 신용카드정보 부정이용범죄의 방지에 별 도움이 되지 못한다. 이 경우 소비자는 곧 도용자이기 때문에 도용자의 e-mail 주소나 휴대폰 번호로 통지가 될 뿐이기 때문이다. 그러므로 카드사가 해당 카드회원의 휴대폰 번호나 e-mail 주소로 결제 내역을 통지하는 방안만이 그 실효성을 거둘 수 있는 것이다.

5. 다양한 본인 인증 방법 개발

1) 전자인증서를 통한 인증

앞서 살펴본 것처럼 신용카드 전자결제시 카드번호와 유효기간 이외에 비밀번호와 주민등록번호 등을 추가로 입력하도록 하는 것도 현재로서는 그리 효과적인 대책이라고는 할 수 없다. 그러므로 이러한 허점을 보완하기 위해서는 인터넷 뱅킹, 사이버 증권거래, 전자정부 서비스 이용 등에서 본인 인증을 위해 사용되고 있는 공인인증서(Certificate)를 인터넷 쇼핑몰 등에서의 신용카드 전자결제에도 전면적으로 도입하여야 한다. 전자서명법 제18조의2에서는 공인인증서는 다른 법률에서 그것을 이용하여 본인임을 확인하는 것을 제한 또는 배제하고 있지 아니한 경우를 제외하고는 그것에 의하여 본인임을 확인할 수 있음을 규정하고 있다.

이렇게 할 경우 개인은 금융결제원[33] 등 공인인증기관(Certification Authority)[34]

33) 금융결제원(www.kftc.or.kr)은 은행공동업무 수행을 위해 1986년에 설립된 비영리 사단법인으로, 현재 국내 20여개 이상의 금융기관이 사원·준사원 은행으로 구성되어 전국 모든 은행을 하나로 연결하는 금융공동망을 구축·운영하고 있다. 주요 업무는 어음교환소 설치·운영, 지로제도 운영, 금융공동망 구축·운영, VAN 사업, 인터넷 지로서비스, 전자서명 공인인증업무, PG 업무, 전자화폐 공동업무, 주택청약 공동업무 등이다. 'Yessign'이라는 공인인증서를 발급하고 있다.

34) 공인인증기관의 지정은 정보통신부장관이 행하며, 국가기관·지방자치단체 또는 법인에 한하여 지정받을 수 있다. 공인인증기관으로 지정받고자 하는 자는 대통령령(전자서명법시행령)이 정하는 기술능력·재정능력·시설 및 장비 기타 필요한 사항을 갖추어야 한다(전자서명법 제4조). 2004년 현재 우리나라 공인인증기관은 전자서명인증관리센터(http://www.rootca.or.kr). 한국정보인증(주)(http://www.signgate.com). 한국증권전산(http://www.signkorea.com). 금융결제원(http://www.yessign.or.kr). 한국전산원공인인증센터(http://www.sign.nca.or.kr). 한국전자인증(주)(http://www.crosscert.com). 한국무역정보통신(http://www.tradesign.net) 7개 업체가 지정되어 있다.

의 공인인증서를 자신의 컴퓨터의 하드디스크에 저장하여야만 신용카드 전자결제가 가능해진다. 이를 교부 받기 위해서는 은행 등에서 신원 확인을 통하여 교부신청을 한 후 인터넷으로 인증서를 자신의 컴퓨터에 다운 받아야 한다. 결국 자신의 인증서를 설치한 컴퓨터에서 접속비밀번호 등을 입력하여 본인 인증 절차를 거쳐야만 신용카드 전자결제가 가능하기 때문에 카드번호의 인증만으로 되어 있는 현행 인증체계보다는 도용으로부터 훨씬 안전하다 할 수 있으므로 신용카드정보 부정이용범죄를 막는 데에는 매우 효과적일 수 있는 대책이라 생각된다. 현재 금융결제원 등 7개 공인인증기관은 전자서명 상호연동 협약을 체결하여 하나의 공인인증서만 발급 받으면 모든 전자거래를 이용할 수 있게 하고 있다[35].

그러나 이러한 방안은 이용절차의 번거로움 등으로 인해 쇼핑몰 등을 이용하는 고객이 줄어들 우려도 있는 것으로 보인다.

① 본인이 은행 등에 직접 가서 신원 확인을 받아 인증서 신청을 해야 한다는 점.

② 전자인증서를 다운 받은 컴퓨터에서만 결제가 가능하다는 점.

③ 소액결제의 경우에는 적용되지 않고 있지만, 소액까지 적용하게 되면 사용자가 불편할 것이라는 점.

④ 전자결제시 본인 인증을 위하여 접속비밀번호 등의 또 다른 입력 절차를 거쳐야 한다는 점 등은 사용자에게 상당히 번거롭고 귀찮은 절차일 수 있는 것이다. 그리고 이로 인한 쇼핑몰 등의 매출감소는 PG 업체에도 타격을 가져올 수 있다. 하지만 보안 문제 등으로 신용카드 전자결제를 기피하던 쇼핑몰 이용고객들이 안심하고 신용카드를 사용할 수 있게 되므로 오히려 장기적으로는 매출이 늘어날 것이라는 반대 의견도 있다[36].

---

35) 디지털타임스. 2003년 1월 28일자 정보통신면 '공인인증기관간 전자서명 상호연동 실시' 기사 참조.
36) 디지털타임스. 2002년 12월 10일자 정보통신면 '온라인쇼핑몰 공인인증서 도입, PG업계 이해득실 이견' 기사 참조.

현재 이 방안은 이미 금융감독원[37]에서 의무화할 방침이어서 앞으로 그 귀추가 주목된다[38].

2) 생체인식 기술을 이용한 인증

그 외 생체인식(Biometrics) 기술을 도입하는 방안을 생각해볼 수 있다(최석범, 2000: 198). 생체인식이란 개인의 독특한 생체정보를 추출하여 정보화시키는 인증방식을 말한다. 지문, 목소리, 눈동자 등 사람마다 다른 특징을 인식시켜 이것을 비밀번호로 활용하는 것이다. 즉 인간의 신체적 · 행동적 특징을 자동화된 장치로 측정하여 개인식별의 수단으로 활용하는 모든 기술방식을 가리킨다. 전자인증서를 통한 인증도 누군가 전자인증서의 접속비밀번호를 알아내고 사용자의 컴퓨터에 접근하여 전자인증서 파일을 다운 받아가게 되면 도용에 속수무책일 수밖에 없다는 점을 감안한다면 본인이 아니고서는 절대적으로 인증이 될 수 없는 이러한 방안도 도입해 볼만하다고 생각된다.

생체인식은 타인과 구별되는 개인의 신체적 특성을 이용하는 만큼 획득이 용이하고 편리하며 망각, 분실, 도난, 복제의 위험이 적어 정보보안시장의 총아로 부상하고 있다. 생체인식기술은 지문, 얼굴, 음성, 손, 서명, 홍채, 망막, 정맥 등은 물론 유전자까지도 분석해 인식할 수 있는 단계까지 와 있는데 이를 이용한 응용분야로는 컴퓨터, 물리적 접근제어, 금융, 의료, 통신, 이주 · 이민, 복지 등 매우 다양하다. 초기에는 물리적인 접근 제어에서부터 시작하였으나 점

37) 금융감독원(www.fss.or.kr)은 금융감독위원회의 지시를 받아 금융기관에 대한 검사·감독업무 등을 수행하게 하기 위하여 설립된 무자본특수법인이다(금융감독기구의설치등에관한법률 제24조). 금융감독위원회(www.fsc.go.kr)는 금융감독업무를 수행하게 하기 위하여 국무총리 소속하에 설치된 기관으로서 그 권한에 속하는 사무를 독립적으로 수행한다(금융감독기구의설치등에관한법률 제3조). 위원장, 부위원장 각 1인을 비롯한 9인의 위원(재정경제부차관, 한국은행부총재, 예금보험공사사장 등 포함)으로 구성된다(금융감독기구의설치등에관한법률 제4조 제1항). 금융감독위원회는 ① 금융기관에 대한 감독과 관련된 규정의 제정 및 개정 ② 금융기관의 설립, 합병, 전환, 영업양수·양도 등의 인·허가 ③ 금융기관의 경영과 관련된 인·허가 ④ 금융기관에 대한 검사·제재와 관련된 주요사항 ⑤ 증권·선물시장의 관리·감독 및 감시 등과 관련된 주요사항 등을 심의·의결한다(금융감독기구의설치등에관한법률 제17조).

38) 한국경제신문. 2003년 1월 21일자 산업/기업면 '공인인증서 사용 의무화, 전자상거래 신용카드 결제시' 기사 참조.

차 전자상거래 및 네트워크, 컴퓨터보안 등으로 옮겨가고 있는 추세이다[39].

생체인식 중 가장 먼저 자동화된 기술은 지문이다. 피부의 표피 밑층인 진피에서 만들어진 지문은 진피 부분이 손상되지 않는 한 평생 변하지 않는 특성을 갖기 때문에 지문인식(finger scan)은 개개인을 인식하는 방법으로 오래 전부터 보편적으로 사용되었다. 지문인식 시스템의 원리는 지문의 골이나 곡점 등 지문이미지의 특징점을 파악하여 저장된 원본데이터와 일치하는지를 비교하는 것이다[40]. 지문을 이용한 인증은 여러 부문에서 이미 실용화 단계에 와 있다. 이것은 보안성을 중시하는 곳에서의 입·퇴장 관리나 중요한 컴퓨터 시스템의 접속허가여부 확인에 이용되고 있다. 주택의 현관문에는 지문인식 전자도어록이 보급되어 있으며 중요 공공기관 등에서는 PC에 지문인식 마우스와 지문인증 보안소프트웨어를 설치하여 중요 문서에 접근할 수 있는 권한자에 대한 인증에 사용하고 있다[41].

지문을 이용한 인증을 신용카드 전자결제에 도입할 경우에는 지문인식 마우스 등을 이용하여 사용자의 지문을 공인인증기관 등에 미리 등록해 놓은 다음 별도의 공인인증서를 통하지 않고도 마우스에 지문을 대는 것만으로 결제가 가능하도록 하는 방법이 좋을 것으로 생각된다. 현재 일부 카드사에서는 결제시 신용카드 없이 고객의 지문만으로 결제처리가 가능한 지문인식결제서비스를 시험적으로 도입하고 있다. 이것은 회원이 매장 내에 마련된 지문등록 데스크를 방문하여 지문등록기를 통해 신용카드정보 및 주민등록번호 등과 함께 자신의 지문을 등록시키면 물품구입시 별도의 신용카드 제시 없이도 결제가 가능한 서비스이다[42].

한편 성문(聲紋)을 이용하여 인증하는 방법, 사인(Sign)을 화상 데이터로 처리하여 확인하는 방법도 생각해볼 수 있다(이노우에 요시유키, 2000: 207-209). 이 역시 방법은 지문을 이용하는 경우와 동일하다.

궁극적으로 가장 좋은 본인인증 방법은 생체인식이 되겠으나, 전자결제의

---

39) 디지털타임스. 2002년 10월 9일자 정보통신면 '생체인식(Biometric)' 기사 참조.
40) 네이버백과사전, 검색어 '생체인식'(http://100.naver.com/search.naver?adflag=1&cid=AD1043311951379&query=&where=100&command=show&mode=m&id=752966&sec=1).
41) inews24. 2003년 3월 14일자 정보통신면 '니트젠, 관세청에 지문인증 로그인 프로그램 공급' 기사 참조.
42) edaily. 2003년 5월 1일자 경제면 'LG카드, 지문만으로 신용결제한다' 기사 참조.

특성상 인식오류가 일어나게 되면 대단히 큰 문제가 발생할 수 있으므로 아직까지 제한적으로 혹은 시범적으로만 사용된다. 이는 성능 자체가 아직 100%의 신뢰도를 가지지 못하기 때문이다. 영화 "마이너리티 리포트"에 나오는 것처럼 사람의 눈(홍채, 혹은 각막)을 보고 즉시 누구인지 확인하는 기술은 아직 기술적으로 불가능하지만, 네트워크의 속도와 컴퓨터의 성능이 그 시기를 앞당길 수는 있을 것이다.

6. 신용카드사용국가의 제한

내국인들이 자주 출국을 하는 널리 알려진 관광지나 나라를 제외하고는 아직까지 후진성을 면치 못하고 있는 나라에서의 신용카드 사용은 위험함 그 자체이다. 만약의 경우 결제에 문제가 생겨도 일단 귀국한 후에는 복잡한 절차에 따라 그 승인을 취소하여야 하는데, 이는 까다로울 뿐더러 다시 출국해야 한다는 것이다. 그리고 그 나라에 다시 가더라도 결제취소가 보장이 안된다는 것을 널리 알려야 할 필요가 있다. 이를 위해서 심한 경우 카드사들은 특정 나라에서는 아예 그 카드로 결제 자체가 이루어지지 않도록 하고 있다. 예를 들면, 세계 어디서나 사용가능한 Diners Club 카드는 방글라데시에서는 사용이 불가능하다. 이처럼 사고발생의 위험성을 기준으로 각 국가의 신용등급을 평가하여 제한적으로 신용카드사용제한 국가를 규정하여 두는 것도 개인신용정보 불법사용으로 인한 피해를 예방하는데 기여를 할 것으로 생각된다.

7. 불법복제장치 판매상에 대한 처벌

신용카드 불법복제를 위해서는 우선 신용카드 판독기(reader)와 입력기(writer)가 필요하다. 판독기는 신용카드의 자기 띠에 저장된 정보를 읽어들이고, 입력기는 읽어들인 정보를 새로운 신용카드에 저장하는 장치다. 하지만 이러한 위·변조를 위한 카드 복제장치가 청계천이나 용산 전자상가 등에서 2백

만원 미만의 가격에 공공연히 거래되고 있지만, 이를 막을 법적 규제 장치가 없어 사실상 신용카드 불법복제는 단속사각지대에 놓여 있다고 할 수 있다. 따라서 불법복제행위를 처벌하기에 앞서 복제장치를 금제품으로 규정하여 허가받지 아니하고 소지하거나 판매하는 자에 대하여 강력한 처벌을 하는 방안이 좀더 근원적인 예방책으로 작용할 것이다.

Ⅵ. 결 론

우리나라는 이제 총 인구의 약 60%에 달하는 2,600만명 이상이 인터넷을 이용하고 있고 초고속인터넷 가입자 수는 이미 1,000만명을 돌파하여 초고속인터넷 부문에서는 그 규모를 짐작할 수 없을 정도이다[43]. 그리고 2002년 6월을 기준으로 현재 우리나라의 총 카드발급매수는 약 1억500만매에 달하고 있으며 총 가맹점수는 약 1,500만개, 이용금액은 연간 약 400-500조원에 이른다[44]. 2002년 한 해 동안 인터넷 쇼핑몰 전체 거래규모는 약 6조300억원이며 2002년 말을 기준으로 인터넷 쇼핑몰 사업체는 약 2,900개로 집계되었다[45].

이러한 급속한 성장과 함께 인터넷 쇼핑몰 등을 이용한 전자상거래는 이미 우리 일상 깊숙이 자리잡은 상태이며[46] 신용카드 전자결제는 이러한 전자상거래에서 없어서는 안될 결제수단이 되었다. 인터넷 쇼핑몰 등에서의 비대면 결제에 있어 신용카드 전자결제는 그 어떤 결제수단보다 간편하고 편리하다고 할 수 있다. 그러나 신용카드정보의 유출, 전자결제시 본인 인증 방법상의 허점 등이 신용카드정보를 이용한 카드도용의 문제를 가져오고 있는 것이다. 이

43) 정보통신부, 주요 현안 업무 보고(2003. 3. 28).

44) 한국여신금융협회, 신용카드업계현황(http://www.knfa.or.kr/menu03_information/sub_list.php?select_no=1).

45) 서울경제신문 2003년 6월 15일자 IT면 '사이버몰 눈부신 성장세, 거래규모 6조 넘어' 기사 참조.

46) 마케팅 여론조사기관 TNS가 세계 37개국의 인터넷 이용률과 인터넷 쇼핑현황에 대해 조사한 결과에 따르면, 한국은 인터넷 쇼핑몰 이용률 면에서 영국, 프랑스를 제치고 미국에 이어 2위인 것으로 나타났다. 이 조사에 따르면 우리나라 인터넷 이용자 중 31%가 인터넷을 통해 제품을 구매하고 있는 것으로 집계됐다(inews24 2002년 6월 24일자 IT면 '한국, 인터넷쇼핑몰 선진국' 기사 참조).

에 관하여 정부와 관련기관이 해야 할 것은 법에 관한 개정인데, 아직 온라인 상거래에 대해서는 그 관련규정들이 모호한 것은 물론이고 아직 규제 법규 자체가 없는 것도 있어서 대책마련이 무엇보다 시급하다.

개인신용정보이용 신용카드범죄에 대한 대책으로서는 먼저 신용카드정보의 유출을 방지하는 것이 매우 중요하다 할 수 있다. 이를 위해서는 카드 사용자의 사용의식 전환이 가장 바람직하다고 할 수 있는데, 카드번호·유효기간·비밀번호·주민등록번호 등의 정보 유출에 항상 주의하고 신용카드결제 후 받은 매출전표는 남이 알아볼 수 없도록 반드시 찢거나 잘라서 버리는 등의 습관을 들이는 것이 중요할 것이다. 그 외 신용카드 전자결제 시스템 구축시 반드시 공인된 PG 업체 등을 통해 카드정보를 암호화하도록 법제화하는 방안도 매우 중요하다고 생각된다. 그리고 전자결제시의 비밀번호 입력에 대한 보완이 현재 상당히 시급한 것으로 생각된다. 또한 카드사가 그 결제 내역을 휴대폰문자메시지(SMS), e-mail 등을 통해 즉시 카드회원에게 통보하는 것을 법률적으로 의무화하는 방안도 매우 효율적인 대책이라 할 수 있을 것이다.

이러한 방안들이 효율적인 성공을 거두지 못할 경우 그 차선책으로 공인인증기관의 전자인증서를 통한 인증, 더 나아가 지문·성문·사인 등을 이용한 생체인식 기술을 통한 인증 등의 기술적 대책을 도입할 필요성이 있을 것으로 생각된다. 결국 개인신용정보이용 신용카드범죄에 대한 대처를 위해서는 카드사용자, 카드사, PG 업체, 정부 기관, 공인인증기관 등의 종합적인 협력과 노력이 필요할 것이다. 앞으로의 연구에서는 홈쇼핑 등 텔레마케터를 통한 구매, 그리고 외국 인터넷 쇼핑몰을 통한 구매 등에서의 신용카드정보 도용방지책에 대한 연구가 필요할 것으로 생각된다. 전화 등을 통해 신용카드번호와 유효기간 등을 불러주는 방법으로 결제되고 있는 텔레마케터 구매에서는 또 다른 문제가 제기되기 때문이다. 또한 우리나라의 법제도가 미치지 않아 주민등록번호와 비밀번호 입력 등의 절차마저도 거치지 않고 있는 외국 인터넷 쇼핑몰에서의 신용카드 전자결제에서는 더 복잡한 문제가 제기될 것이다. 그리고 앞서 든 방안들 이외의 비대면적 본인 인증 방법에 대한 다각적인 연구도 필요할 것으로 보인다.

참 고 문 헌

경찰청(2003). 『경찰백서』. 서울: 경찰청.

박상기(1999). 『형사정책』. 서울: 한국형사정책연구원.

사법연수원(1999). 『신종범죄론』. 사법연수원 강의교재.

임웅(2002). 『형법각론』. 서울: 법문사.

이재상(2002). 『형법각론』. 서울: 박영사.

이노우에 요시유키[박명섭, 조종주, 한낙현 역](2000). 『전자결제 시스템의 구조』. 서울: 부키.

정보통신부(2003. 3. 28). 주요 현안 업무 보고.

정진명(2001). 『인터넷상 신용카드사용의 법적 문제』. 인터넷법률 6. 법무부: 4-5.

최석범(2000). "전자결제상의 위험유형과 대응방안에 관한 연구". 『경영대학원논총』, 제16호, 영남대학교 경영대학원.

최응렬(1994). "신용카드범죄에 관한 고찰". 한국형사정책연구원. 『형사정책연구소식』, 21:35-45.

최응렬(1999). "신용카드위조범죄와 그 대책에 관한 연구". 『한국공안행정학회보』, 8:157-158.

코인츠·이니시스(2001). "컨텐츠 유료화 및 전자상거래 발전을 위한 전자결제솔루션". 상공회의소. 실무세미나 자료집: 39.

한상문(1992). 『신용카드법입문』. 서울: 정법사.

增田 晋·飯田耕一朗·內山隆太郎(1998). 『電子マネーの實務』. 新日本法規.

국민일보(2001). '신문에 난 카드사진번호이용 인터넷서 물품구입후 되팔아'.8.23.

국민일보(2002). '신용카드전표주의! 휴지통 뒤져 카드번호 알아낸 후 수억 챙긴 일당 구속'.7.25.

굿데이(2002). '타인 카드번호로 성인인터넷 영화 공짜 시청'. 12.6.

동아일보(2001). '신용카드번호 다운받아 물품구입 대학생 적발'. 10.29.

동아일보(2003). '인터넷몰 회원 6500명 카드정보 해킹'. 4.22.

디지털타임스(2002). '생체인식(Biometric)'. 10.9.

디지털타임스(2002). '온라인쇼핑몰 공인인증서 도입, PG업계 이해득실 이견'.12.10.

디지털타임스(2003). '공인인증기관간 전자서명 상호연동 실시'. 1.28.

매일경제(2002). '신용카드사범 특별단속'. 10.10.

머니투데이(2003). 증권면 '카드부정사용 원천차단 - 카드업계'. 3.6.

서울경제신문(2003). '사이버몰 눈부신 성장세, 거래규모 6조 넘어'. 6.15.
연합뉴스(2002). '훔친 카드전표 이용 인터넷 사기'. 7.25.
오마이뉴스(2002). '신용카드전표, 함부로 버리면 낭패'. 7.5.
중앙일보(2003). '카드번호 알아내 인터넷 결제 피해 속출'. 5.2.
한국경제신문(2003). '공인인증서 사용 의무화, 전자상거래 신용카드 결제시'. 1.21.
한국일보(2002). '인터넷 쇼핑몰 사기 극성'. 8.21.
한국일보(2003). '신용정보매매 인터넷서 극성'. 5.3.
edaily(2003). 'LG카드, 지문만으로 신용결제한다'. 5.1.
inews24(2002). '한국, 인터넷쇼핑몰 선진국'. 6.24.
inews24(2003). '니트젠, 관세청에 지문인증 로그인 프로그램 공급'. 3.14.

http://100.naver.com/search.naver?adflag=1&cid=AD1043311951379&query=&where=100&command=show&mode=m&id=752966&sec=1
http://www.knfa.or.kr/menu03_information/sub_list.php?select_no=1

ABSTRACT

A Countermeasures on Credit Card Crime Using Personal Credit Information

Kim, Jong Soo

Recently, because credit card crime using a personal credit information is increasing, professionalizing, and spreading the area, the loss occurring from credit card crime is enormous and is difficult to arrest and punish the criminals.

At past, crime from forging and counterfeiting the credit card was originated by minority criminals, but at present, the types and appearance of credit card crime is very different to contrasting past crime.

The numbers of people using credit card in the middle of 1990's was increasing and a barometer of living conditions was evaluated by the number having credit card, therefore this bad phenomenon occurring from credit card crime was affected by abnormal consumption patterns.

There is no need emphasizing the importance of personal credit card in this credit society. so, because credit card crime using personal credit card information has a bad effect, and brings the economic loss and harms to individuals, credit card company, and members joining credit card.

Credit card crime using personal credit card information means the conduct using another people's credit card information(card number, expiring duration, secret number) that detected by unlawful means.

And crime using dishonest means from another people's credit information is called a crime profiting money-making and a crime lending an illegal advance by making false documents.

A findings on countermeasures of this study are as follows:

Firstly, Diverting user's mind, improving the art of printing, and legitimating password from payment gateway was suggested.

Secondly, Complementing input of password, disseminating the system of key-board protection, and promoting legitimations of immediate notification

duty was suggested.

Thirdly, Certificating the electronic certificates as a personal certificates, assuring the recognition by sense organ of organism, and lessening the ratio of crime occurrence, and restricting the ratio of the credit card crime was suggested.

【Key Words: credit card crime, personal credit information, electronic certificates】