信用卡套现是指信用卡持卡人通过非正常手段，将信用额度内的资金以现金的形式套取出来，同时又不支付银行提现费用的行为。信用卡套现是违法行为，不仅会增加持卡人债务压力，加剧银行信贷坏账风险，而且容易导致信息泄露，进而衍生出各类欺诈风险，带来严重的经济损失，已成为威胁金融市场稳定的重要因素之一。本文以三起信用卡套现引发的欺诈案件为切入点，深入探析信用卡套现衍生的欺诈风险，并提出防控对策。

一、信用卡套现衍生的欺诈案件

当前，经济形势严峻，社会个体偿债压力急剧增大，不少持卡人伺机通过信用卡套现缓解资金压力。但是，信用卡套现极易导致账户信息泄露，经常被不法分子利用作案，从而造成银行及持卡人的重大经济损失。

1.案例一：“境外机”窃取信用卡信息伪卡案

（1）案情介绍

2017年10月下旬，多名持卡人向银行反馈本人在国内，信用卡携带在身边，却在泰国地区被盗刷的情况。调查员深入分析交易特征，调取消费凭证，判定该起案件为一起典型的跨国伪卡欺诈案。

（2）案件研判

伪卡欺诈是指犯罪分子通过改装POS或利用侧录器窃取信用卡磁条信息，然后将窃取的磁条信息写入白卡或作废的银行卡中，最后制作成假卡进行交易的欺诈手法。窃取信用卡磁条信息在伪卡欺诈犯罪链条中起着非常关键的作用。因此，及时侦测信息泄露源，对于防控潜在欺诈风险、对犯罪分子进行刑事打击至关重要。根据案件调查经验，涉案卡片均在泰国地区通过取现的形式被盗刷，作案手法相似，历史用卡的共性商户极有可能是信息泄露源。但该案受害客户遍布全国各地，历史消费无共性商户，那么到底是哪个环节泄露了磁条信息呢？

调查员深入研判案件特征，在错综复杂的交易线索中寻找共性，终于发现涉案卡片近半年内均在东南亚地区有刷卡交易，且交易有套现嫌疑。经多方核查，确认客户前期在东南亚地区的刷卡交易系持卡人为满足其套现、资金周转的需求，利用“境外机”伪造的境外交易。持卡人在“境外机”上刷卡时，信用卡磁条信息被侧录，信息通过服务器传输至境外，并在极短时间内被复制成伪卡在境外POS上刷卡，虽然是在国内刷卡交易但在银行显示为境外交易，由此误导银行认为持卡人在境外消费，达到提升信用额度的目的。基于“境外机”可存储磁条信息的运作原理，调查员大胆作出推断，“境外机”为该起跨国伪卡欺诈案的信息泄露源。广东省公安厅

在破获该案时，当场查获窃取银行卡磁条信息平台5个、存储磁条信息后台服务器5个、银行卡磁条信息侧录器5600多个、空白银行卡245张，证实了调查员的推断，涉案卡片均是在“境外机”上套现时被窃取磁条信息继而被盗刷。

2.案例二：某管家套现App境外网络盗刷案

（1）案情介绍

2019年上半年，境外某游戏网站的欺诈交易量大幅上升。调查员梳理案件时发现，该案具有短时间内高频案发、交易模式趋同且涉案卡号存在一定连续性等特征，调查员判定该案为一起典型的批量信息泄露后通过境外网络盗刷的案件。

（2）案件研判

境外网络盗刷是指信用卡持卡人前期交易的商户遭遇黑客攻击，或交易时被他人记录信用卡信息，继而通过境外网站被盗刷的作案模式。调查员对盗刷卡片的历史交易进行数据交叉关联，排查信息泄露源，发现涉案客户前期均在商旅类网站上有频繁交易，交易的频率、金额明显超出正常商旅需求，且与客户的工作性质不匹配。调查员针对异常交易展开深入调查，确认此类商旅类交易均非正常交易，客户是通过某管家套现App模拟正常消费，从而套取信用卡内资金。调查员实际操作验证后发现该App注册时用户需填写姓名、身份证号、手机号码、储蓄卡信息，注册完成后在交易环节输入卡号、有效期、CVV码等敏感信息即可进行套现。基于此，调查员大胆作出假设，该套现App为该起境外某游戏网站案的信息泄露源。最终，经警方侦查，确认该App存在非法截留客户信息以及被黑客攻击盗取账户信息的情况。

近年来，互联网套现App逐渐兴起并迅速发展，此类平台安全系数低，管理混乱，风险防御能力差，信息泄露事件频发，成为滋生互联网欺诈的“温床”。

3.案例三：江某电信网络诈骗案

（1）案情介绍

2019年11月12日，持卡人江某接到自称是银行客服的诈骗电话，电话中称客户江某涉嫌套现，根据监管机构的规定，要冻结江某的信用卡，若要解冻需进行信用卡信息核验。江某在当地经营一家建材店，店内资金紧张时会利用信用卡套取现金用于商铺资金周转，一旦信用卡被冻结，商铺经营的资金链可能断裂，赖以生存的生意将无法为继。因此，江某为了解冻信用卡，被假冒银行客服人员的诈骗分子套取信用卡信息，诈骗分子在套取到交易关键信息后迅速实施盗刷。

（2）案件研判

上述案件中，由于江某固定在某商户套现，该商户对江某的信息了如指掌，在利益驱动下将江某的信息出售给恶意第三方，恶意第三方在购买江某的详细资料后，针对江某的信贷需求状况，“量身定制”一套话术成功骗取江某的信任，并诱导江某泄露信用卡支付的关键信息，从而盗刷江某卡片，给江某造成重大财产损失。

近年来，电信诈骗案件持续高发，据统计，90%的电信诈骗案件是由于信息泄露所致，信息泄露已成为电信诈骗案犯罪的主要源头。犯罪分子实施诈骗前掌握受害人的姓名、职业、学历、爱好、婚姻状况等详细信息，从而实施精准诈骗，迷惑性极强，让人防不胜防。而客户在套现的过程极易泄露个人信息，将自己置于危险的境地，成为犯罪分子的目标。

部分持卡人认为套现可解自己资金需求的燃眉之急，银行亦可收取交易的手续费，双方均可获益，殊不知，不法分子却借机窃取信息，实施盗刷。上述案例一中，商户恶意通过“境外机”窃取持卡人账户信息实施盗刷，从中获取不当利益；案例二中，商户违规保留客户的账户信息，却因自身防御能力不足，遭遇黑客攻击，导致账户信息被不法分子获取；案例三中，套现商户更是直接参与买卖客户信息的违法活动，致使客户遭遇电信诈骗。由此可见，套现不仅虚构交易、扰乱银行的判断，且更容易导致信息泄露，使套现衍生的欺诈风险积聚，为银行的风险防控带来挑战。

二、防控对策

随着信用卡套现衍生的欺诈风险日益加剧，发卡行、收单机构、持卡人等交易参与主体应明确各自的责任与义务，从杜绝信用卡套现行为和防范套现衍生的欺诈风险两个方面着手，必要时借助法律武器对违法违规行为予以严惩，推动信用卡产业的健康发展。

1.发卡行加强风险管理

发卡行应完善信用卡发卡考核体系，审慎选择目标客户群体，从源头上强化信用卡套现风险管理。严格审核申请人单位信息，防止客户以虚假单位信息骗领信用卡。另外，银行应承担社会责任，建立对持卡人安全用卡警示教育的长效机制，让持卡人切实了解信用卡套现的危害。交通银行信用卡中心推出“防欺诈动漫秀”，在交通银行信用卡公众号、订阅号等渠道设置专栏，以漫画的形式生动揭示最新欺诈手法，引导持卡人合规用卡，重视个人信息安全，增强风险防范意识。

银行要充分发挥大数据等技术优势，研判套现衍生的欺诈案件的主要形式，针对异

常交易及时预警，建立全流程的风险策略管理体系。事前以防为主，审查持卡人消费行为是否涉嫌套现，一旦认定为套现交易，可根据套现程度采取交易限额、信用降额乃至停卡等管控措施；事中及时干预，根据各类套现手法与盗刷特征的关联性，布控相应的预警规则，对潜在欺诈交易及时拦截，将持卡人和银行的损失降到最低；事后密切追踪，全景还原案件发生过程，挖掘看似独立的案件之间的深层关系，集成关联信息，优化风险策略，提高同类事件的风险识别能力。通过搭建事前、事中、事后套现客户异常交易模型，全流程防控套现衍生的欺诈风险。

2.收单机构严格监控商户

收单机构应杜绝商户套现，严格审查特约商户的入网资质，了解商户入驻的真实意图，切断信用卡套现的渠道。全方位监控商户的资金状况，分析商户的交易数据，设置与商户经营状况相应的风险线，判断商户的经营活动是否涉及套现，必要时亲临现场核查交易的真实性。

收单机构作为交易工具的重要供给方，在严防信息泄露方面应承担更多的责任。一是敦促特约商户规范经营，重视持卡人账户信息管理，严禁违规存留账户信息；二是不断进行技术革新，重视反欺诈人才培养，提高抵御外部风险的能力；三是审查商户经营管理状况，建立风险监控模型，重点关注商户是否存在信息泄露的情况；四是警惕商户沦为不法分子违法所得的洗钱工具，严格审查商户入网资料，加强对交易真实性的验证。

3.持卡人增强安全意识

持卡人不能只顾及当下的资金窘况，更要了解套现的严重后果，自觉合规、合法用卡。随着社会诚信体系的健全，金融监管机构加强对持卡人信用状况的监督，必要时公布持卡人信用履行情况。个人征信对于人们日常生活起着重要的作用，对于申请信用卡、贷款有着重要的影响。持卡人应谨慎、合规使用信用卡，明确自己的权益和责任，珍惜个人信誉。

持卡人应增强信息安全意识，以免信息泄露导致信用卡被盗刷。接到陌生电话、短信、邮件时需提高警惕，核实对方的真实身份，以免财产受损。使用信用卡交易时，卡片不可脱离自己的视线范围，以免信息被他人恶意记录后售卖。另外，网上交易、办理业务时需在官方渠道操作，套现App属于违法交易工具，风险敞口大，信息泄露可能性高，持卡人应杜绝在此类App上填写个人信息。一旦出现信息泄露或信用卡被盗刷的情况，应马上致电银行说明情况，并对风险卡片管制，及时止损。

4.以法律震慑违法犯罪行为

《中华人民共和国刑法》和相关司法解释明确信用卡套现为犯罪行为，严格界定信用卡套现所涉及的罪名、构成要件及处罚标准。商户使用销售点终端机具（POS）等，以虚构交易、虚开价格、现金退货等方式向信用卡持卡人直接支付现金，情节严重的，以非法经营罪定罪处罚。持卡人需认识到套现是扰乱金融秩序的违法行为，以虚假交易套取资金的行为本身具有欺诈成分，有贷款诈骗嫌疑，套现后若未按期还款，或涉嫌信用卡诈骗罪。金融机构应当与司法机关密切合作，依据法律法规严厉打击信用卡套现行为，防止信用卡套现犯罪风险蔓延。

信息泄露已成为套现衍生的欺诈案件的重要源头，对于信息泄露方应依据法律予以严惩。发卡行、收单机构、持卡人应积极主动向司法部门报送信息泄露线索，积极配合公安机关调查、取证，根据《最高人民法院 最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》等相关法律的规定对违法犯罪行为进行严厉打击，震慑违法犯罪活动，铲除危害金融市场安全的社会毒瘤。

随着互联网经济的发展和科技的不断进步，信用卡套现方式不断翻新，特别是网络交易中客户信息在产业各方间流转，使信息泄露的可能性加大。在信用卡套现风险防控难度不断加大的背景下，产业各方应对风险防控的压力增大，因此，各方应协同配合，信息共享，不断优化风险策略，将套现衍生的欺诈风险降到最低，共同维护产业健康发展。