

万事达卡批量境外盗刷调查

钱退回来了,但恐慌还没有散去。

近日,万事达信用卡遭批量境外盗刷事件持续发酵,多名持卡人在国内、妥善保管实体卡片,且未操作任何境外交易的情况下,却遭遇境外地区陌生扣款,有持卡人遭盗刷金额超过万元。

北京商报记者进一步多方采访发现,大量持卡人有着高度重合的遭遇:实体卡长期闲置、仅绑定在Apple Pay中,甚至从未线下刷卡。

多位持卡人反馈,盗刷资金全部追回,用户无实际资金损失,但在业内看来,这也暴露了跨境支付链路中被忽视的风控盲区。不同于传统信息泄露式盗刷,本次事件直指发卡行Token场景校验缺位、交易路由配置疏漏及卡组织风控预警不足的系统性风控短板。

业内认为,后续,银行、卡组织、钱包三方需建立联合风控,持卡人也要提前做好防护。

如何防范信用卡被境外盗刷:

普通用户关掉境外无卡支付开关,从源头堵死境外线上盗刷通道

卡组织要压实自身风控责任,对集中式、批量试探类的异常交易行为做到更早识别拦截

银行应在准入层硬性拦截异常请求

多名持卡人遭遇“离奇”扣款:资金已全额退回

9月28日下午1点30分至2点,历经境外信用卡盗刷风波后,陈杨(化名)账户内的两笔遭盗刷资金全额退回,这场离奇的经历依旧让他心有余悸。

“被盗刷的第一时间,我脑子是懵的”,9月26日上午9点30分,陈杨正居家休息,手机接连弹出两条来自中国银行的交易提醒短信,Apple Pay钱包同步推送境外消费记录。突如其来的通知,让他瞬间绷紧神经,发生扣款的,是一张锁在家中抽屉、从未实际消费过万事达信用卡。两笔交易商户名称均以星号隐去,交易地点指向巴西,被盗刷金额合计11404.68巴西雷亚尔,折合人民币约1.48万元。

这张卡是陈杨去年9月申请办理的,授信额度约7万元人民币。当初办卡的初衷,一是看中了卡片的外观,二是准备未来赴欧洲出行使用。卡片到手之后,实体卡始终留在家中,从未外带。陈杨回忆称,“当时我仅将卡片绑定至手

机Apple Pay钱包,但自始至终没有通过Apple Pay完成任何一笔支付”。

事发时,他本人身处国内,手机就在手中,并未收到任何支付验证。发现异常后,陈杨曾尝试通过手机银行App锁卡止损,并拨打信用卡贵宾客服热线。

“最让人不安的是,我全程没有收到银行任何风控预警、交易核实或临时冻结提示。”陈杨回忆,由于信用卡交易存在结算窗口期,资金并不会像储蓄卡那样实时划转,银行也依托这一机制,通过卡组织渠道发起止付操作,最终完成了盗刷资金的追回。

陈杨告诉北京商报记者,他所在的持卡人交流群中,从9月28日至9月29日,已有不少持卡人反馈,被盗刷的资金已经完成退回。

另一名持卡人李凯(化名)也向北京商报记者还原了相似的经历。半年前,他特意办理了这张中国银行信用卡,以备后续境外消费使

用。为了不浪费卡片,李凯平日偶尔会用到这张卡,但卡片大部分时间都处于闲置状态,几乎没有大额消费、境外消费记录。异常情况同样发生在9月26日,李凯突然收到了中国银行的交易短信提醒,发现卡片出现了3笔陌生的境外盗刷交易,3笔款项折合人民币总金额近8000元。事发的同一时间段,李凯本人身处国内,实体信用卡也一直由他妥善保管、随身携带,卡片从未离身,不存在遗失、转借他人的情况。

“银行告诉我已查明是盗刷,欠款不用我归还,但并未说明此次被盗刷的原因”,李凯说道。

另外,北京商报记者从中国银行信用卡客服人员处了解到,目前该行已采取相应的风控措施,中国银行信用卡客服人员表示,此次盗刷事件不会造成客户的额外资金损失,请等待银行后续联系。

虚拟令牌反成盗刷突破口:有银行启动内部排查

资金虽然失而复得,但整个事件暴露的风控漏洞,并未随着退款而消失。

从被盗刷的情形来看,多名持卡人的遭遇呈现高度相似性:卡片绑定过Apple Pay,所持实体卡大多很少使用甚至从未线下刷卡。

被盗刷卡片多数为绑定Apple Pay的万事达卡,多位持卡人猜测,这场盗刷事件的核心突破口,正是Apple Pay绑定银行卡后生成的Token卡号,也就是支付令牌。

李凯告诉北京商报记者,“Apple方面也曾回复过我,设备卡号本身不属于保密信息。我的Apple Pay账户里并没有出现被盗刷的3

笔订单,也就是说,是盗刷团伙获取了信用卡相关信息后,将卡片绑定到其自己的Apple Pay中发起支付”。他认为,前几个月Apple曾推广Apple Pay与万事达卡的绑定活动,不少用户在同一时间段把信用卡绑定到Apple Pay,卡片有效期也集中在同一区间。盗刷分子或许是借此掌握了这批卡片的有效期,再通过不断试猜设备卡号,绕过CVV验证完成盗刷支付。

一位银行信用卡中心人士介绍,用户将信用卡绑定Apple Pay时,手机不会直接留存、使用用户的真实银行卡号,系统会自动为

每张绑定的卡片生成一个专属的虚拟替代卡号,这个专属虚拟卡号就是支付令牌(Token)。

但此次盗刷事件,核心问题出在虚拟令牌和风控体系的漏洞上。上述信用卡中心人士猜测,此次盗刷事件中,黑客有可能模拟了专属的虚拟替代卡号生成顺序,然后批量刷卡进行了远程盗刷。

针对批量盗刷存在的风险,已有银行启动内部排查。某银行信用卡中心相关人士表示,该行暂未出现盗刷案例,虽监测到几次盗刷尝试,但均未通过交易检验。

校验去哪了:一场技术理想与实际配置的落差

值得警惕的是,这并非万事达首次陷入盗刷风波。

早在去年9月,就有浦发银行发行的万事达卡出现过高度相似的批量异常交易。仅隔一年时间,再次出现批量盗刷,均指向了提供服务的万事达卡,在业内看来,这也暴露出万事达在跨境风险联防上存在短板。

南开大学金融学教授田利辉指出,持卡人的技术判断与已知信息高度吻合。

与以往盗刷相比,田利辉认为,此次呈现三个新特征:攻击对象从实体卡信息转向设备Token,攻击路径绕过了Apple Pay的人脸核验,攻击方式从单点泄露变为批量试探号段。

“这已不是传统意义上的卡片被盗,而是支付技术落地环节的配置缺陷被规模化利用。”田利辉进一步称,万事网联作为清算机构,对号段异常交易的监测和预警负有管理责任。连续两年出现批量盗刷,说明这不是偶发漏洞,而是部分发卡行在Token场景校验上的系统性配置缺失。发卡行是第一道

闸门,万事网联是监测层,两者责任不能互相替代。

更深层的矛盾,还有来自安全承诺和现实落地之间巨大的执行鸿沟。

“最核心的原因是Token的安全承诺与发卡行实际配置能力之间存在落差。”田利辉解释,Token化本应用设备账号替代真实卡号并严格限定交易场景,但设备卡号顺序发放、可被批量试探;场景校验又缺乏统一强制标准;更危险的是,一旦持卡人和机构因“Token即安全”而放松警惕,其他防线也会随之松动。连续两年同类事件说明,攻击者已形成稳定利用模式,而产品设计上的号段规律和落地配置的参差不齐,为这种攻击提供了可复制的条件。

“不少受害者只是把卡绑了Apple Pay,实体卡没丢、自己也没出境,照样在拉美线上商户被盗刷。所以从这个角度来看,这件事不能怪Apple Pay本身,它的令牌技术本身是安全的,问题可能主要出在万事达跨境清算链路

上面。”博通咨询首席分析师王蓬博则说道。

王蓬博进一步称,作为卡组织,万事达对全球下游境外商户的风控约束力度不足,部分海外线上商户可以绕过二次校验,黑产有可能是钻了这个空子批量做交易。同时卡组织层面对于同一段号段集中出现大量试探交易,事前预警拦截做得也不够,非要等到大批用户已经被盗刷之后才后知后觉暴露风险,暴露出它在跨境风险联防上存在明显短板,风险压力很大一部分转嫁到发卡银行和普通持卡人身上。

招联金融首席研究员董希淼则提醒,与传统盗刷相比,此类风险攻击面从卡号信息扩展至设备与数字凭证链路,交易常呈跨境、分散特征,参与方更多,责任认定更复杂。Apple Pay以设备账户信息替代实体卡号,并配合动态安全机制,可降低卡号直接泄露风险;但Token并非绝对安全,尤其是如果注册环节风险监控不足,单一机构难以识别跨行业的团伙欺诈。

业内建议厘清权责:三方需建立联合风控

业内认为,要堵住这类新型欺诈,不能只靠某一家,而是需要重新厘清钱包、卡组织、发卡行三方的安全边界,并拿出可落地的整改路径。

田利辉指出,“万事达应全面审计已发行设备卡号段,修复配置缺陷,并将号段生成从顺序发放改为随机化。银行、卡组织、钱包三方需建立联合风控:钱包写入不可篡改的场景标识,卡组织在清算层强制校验并实时告警,发卡行在准入层硬性拦截异常请求”。

王蓬博强调,卡组织不能只做一条“交易管道”,“后续卡组织必须压实自身风控责任,对集中式、批量试探类的异常交易行为做到更早识别拦截”。

董希淼则进一步指向制度层面,需要在注册环节强化风险评分,推动卡组织、支付平台与银行实现风险信息实时共享,并完善跨境交易争议与责任判定规则。跨境链条的特殊性正在于此:一笔

交易从手机钱包发出,经过清算网络、海外商户网关,再抵达国内发卡行后台,中间跨越不同国家的监管环境与数据规则;任何一环校验松口,都可能让整条防线出现缺口;而等到资金异常已经发生,损失往往先由持卡人直面,再由银行启动拒付流程进行回溯。

这也意味着,在系统性补丁全部落地之前,用户也需要建立属于自己的安全边界。

针对已经遭遇盗刷,或是希望提前做好防护的持卡人,董希淼建议,“持卡人若发现境外异常交易,应遵循‘止损—取证—申诉’顺序:立即通过客服或App冻结、挂失卡片;尽快在境内ATM查询、取现或POS消费并保留凭条,以证明卡未离身;随后向银行提出盗刷调查并向公安机关报案。应保存交易凭条、账单与提醒截图、客服沟通记录、报案回执及出入境或行程材料”。北京商报记者 刘四红 宋亦桐

