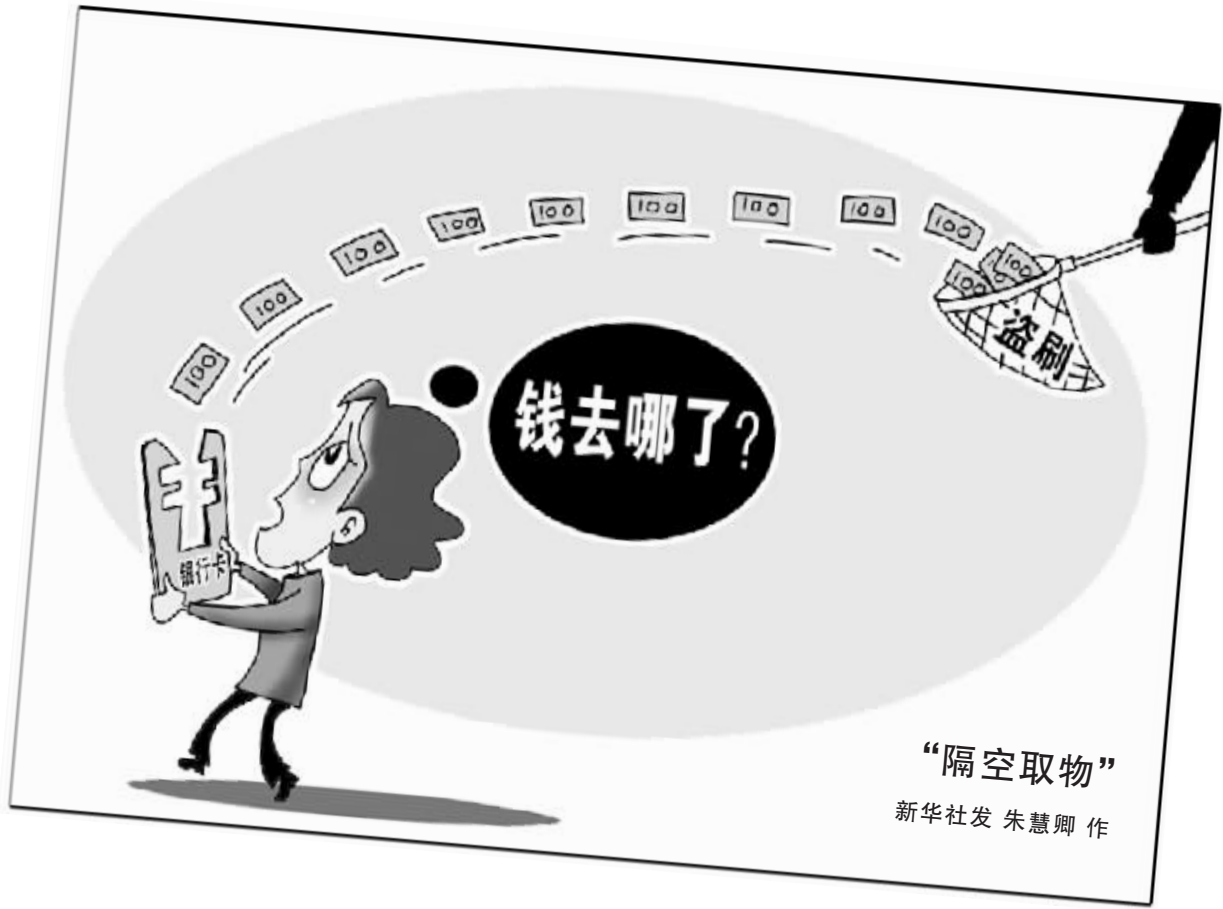


# 卡在身边 钱却没了 谁该负责

## ——一个银行卡盗刷事件的样本调查



### 卡未离身 U 盾在家 钱莫名支付网游公司

5 月 11 日,邵女士陆续接到工行客服 95588 发来的短信,提示她的一张工行储蓄卡通过网银支出 5000 元到 10000 元不等的金额。就在地拨打 95588 冻结账户的三分钟内,共被莫名其妙“支出”3 万元。

开卡行工商银行北京沙窝路支行查询明细后告诉邵女士,3 万元是通过福建福州一家支行支付给了“福建网龙计算机网络有限公司”。

“我很少使用工行网银,和这家网络公司也没有交集,为什么我人在北京、卡不离身、U 盾在家,钱却从福建支付给了一家公司?”邵女士大为吃惊。

在工行填写了“客户银行卡疑似被盗刷情况登记表”的几天后,沙窝路支行反馈给邵女士初步调查结论:钱是通过无卡支付方式支付给网龙公司。福州当地支行与网龙公司交涉过,但网龙公司表示这笔钱是网络游戏玩家用于购买游戏道具“魔石”的,不可能赔付。

“我没有开通无卡支付,银行是怎么不经核实就将钱支付给这家公司的?”邵女士心存疑问。

工行负责外部欺诈风险的工作人员告诉记者,无卡支付类似于快捷支付,在一定限额内无需 U 盾即可实现转账,目前不少银行和第三方支付均有类似业务,有时储户将银行卡绑定第三方支付即被视作开通了无卡支付。

记者了解到,工行快捷支付还需要输入手机发送的动态密码,邵女士并未开通该业务。那么,会不会有人通过第三方支付进行了网上支付操作?

工行沙窝路支行行长刘涛表示,是否通过第三方支付途径,在其网点信息看不到,需要邵女士去和第三方支付机构了解情况。

邵女士表示,她曾使用第三方支付在网上消费过,但是否由于第三方支付的原因,她也无从追问。

### 公司拒赔 银行推诿 损失谁来买单

邵女士的钱怎么离奇转到“网龙公司”的?银行业内部人士认为,邵女士很可能遭遇了网络盗刷,她的银行卡信息或第三方支付账户信息可能此前已被不法分子,通过钓鱼网站或木马病毒获取。而通过游戏网站消费,正是犯罪分子销赃的惯用手法。

2013 年,曾有不少消费者在网购时资金被意外转入上海巨人网络科技有限公司的玩家账号,套取现金,数额从几百元至数十万不等。2014 年 10 月底,合肥公安机关发现巢湖市居民陶某某通过钓鱼网站和手机木马,成功盗取网银资金后,购买游戏充值卡等物品后低价销赃,非法获利。

“我不玩网络游戏,网龙公司是怎么审核交易的,难道什么钱都来者不拒?”邵女士说。

记者从网龙公司官网了解到,魔石充值可通过工行银行卡直购,U 盾客户不受额度限制;也可通过支付宝快捷支付,额度是每张卡每天 500 元。在没有使用 U 盾、额度有限的情况下,邵女

士的 3 万元是如何支付购买魔石的,成为待解之谜。

网龙公司客服以“不能泄露客户账户信息”为由,拒绝向记者和邵女士提供账户详情,并表示目前该公司玩家的账号通过手机号码、QQ 账号、邮箱等方式注册,并不都是实名认证,一些玩家道具和装备的线下交易无法追踪溯源。

北京市兰台律师事务所张合军认为,尽管一些不法分子利用游戏充值、话费充值等方式销赃,但并不能直接推定网游公司、通信运营商等企业负有法律责任,因为这些企业不具备有效辨别购买商品的资金是否是赃款的专业能力。

“尽管如此,一些游戏网站容易成为销赃平台,暴露了此类网站为求简便快捷地实现买卖交易,对用户交易审核不严,对账户疏于管理。”中国人民大学财政金融学院副院长赵锡军表示,另外,银行在追求支付创新的同时,也存在对账户安全监管不到位的问题。

### 受害人难追偿 谁来负责

“银行只口头通报我调查结论,说书面调查结果只提供给警方,但事发到现在 20 多天过去了,警方并没有告诉我案件的丝毫进展。”邵女士去报案的派出所咨询,得知目前类似的网络盗窃案件已积压了很多,警方让她回家等着等消息。

工行沙窝路支行行长刘涛表示,截至目前还没有警方来他们网点调查和了解相关情况。

“网龙公司不给查,北京的工行建议我起诉福建分行,警方说要忙比我盗刷金额更大的案件,我真不知道还能通过什么途径解决。”邵女士说。

中央财经大学法学院教授郭华表示,类似的网络诈骗、盗刷事件,在犯罪分子最终落网前,电子商务网站、第三方支付机构、银行等事件的关联方很难为受害人负责。而迫于警力有限,诈骗、盗刷金额不是特大的案件进展相对缓慢。“互联网催生了不少新兴犯罪手法,尤其是金融领域的案件跨机构、跨地域,而且民事、

刑事交叉,涉案财产处理难度大、时间长,很多受害人的赔付最后就不了了之了。”

张合军建议,储户可以尝试与银行协商解决,毕竟储户和银行存在合同关系,至于各方应承担责任多少可以协商确定。

目前此案还在进一步调查中。但警方和专家提醒消费者,要加强安全意识,妥善保管好自己的账户信息和密码。“储户也应绷紧维护自身资金安全的弦,尤其是在网上交易时,要认真检查电子商务网站的域名是否正确,不轻易点击陌生人发来的链接或来自电子商务网站外的链接。”赵锡军说。

日前,银监会出台 20 条监管细则,加强银行业金融机构内控管理,防范外部欺诈和内部舞弊引发的案件。其中,要求银行特别关注互联网环境下新兴业务应用、交易系统存在的客户信息泄露隐患,确保对可能产生信息泄露的环节有足够的监测和管控能力。

(据新华社电)