



# 银行卡被盗刷 打官司却败诉

律师建议: 与银行签约时, 最好明确持卡交易中使用签名认证

□李鹏飞 辛 爽

卡在身上存, 钱从网上飞。银行卡被盗刷, 储户资金受到威胁。储户报警后, 公安机关按刑事案件立案, 由于网络犯罪作案者踪影难觅, 破案难度很大。储户起诉至法院后, 要求银行的赔偿有的被支持, 有的被驳回。今天选择一个储户被法院驳回诉讼请求的案例, 给开通网上银行的读者一点启示。

## 案情

王女士于2013年2月份, 在某银行办理了结算通卡一张, 2014年7月30日上午, 王女士发现自己的该银行卡内余额减少, 立即去银行营业厅询问。得知自己账户于2014年7月28日, 分四次被网上支付消费共15780元, 但网上支付U盾在王女士手上, 并未使用, 且其开通了短信提醒功能, 亦未收到相关消费短信提醒。后王女士到公安局报案, 经初步查明, 其账户被不法分子通过网上支付进行了盗刷。王女士认为, 该银行作为商业银行, 应当保护储户的财产权益不被侵害, 因其未尽到保障交易安全的监管义务, 导致自己财产损失, 应当承担赔偿责任, 遂起诉至法院。

## 分歧

王女士的代理律师认为, 之所以要求银行赔偿储户的全部经济损失, 理由是: 其一, 王女士在某银行办理了银行卡并储蓄了现金, 双方即建立了储蓄合同关系, 被告作为商业银行, 应保护储户的财产权益不被侵害, 负有保障交易安全的监管义务。其二, 银行账户支付功能仅需输入手机验证码即可完成支付的方式, 安全设施存在严重漏洞, 在银行无证据证明因储户个人原因导致银行卡被盗刷的情况下, 银行应承担全部责任。其三, 王女士将款存入银行, 手中持有的银行卡只是一张便携式债权电磁形式之记录, 与之等额的钱款则是存在银行并由银行占有银行应将卡内减少的钱款予以赔偿。

针对原告王女士及代理人的诉求, 被告银行也陈述了自己不予赔偿的理由和实施。

第一, 银行尽到了合同义务。账号支付的具体流程为客户按照程序填写账号、手机号后, 点击发送验证码的指令, 然后由手机号码接收验证码, 输入验证码后即可实现网络支付。本案中, 原告所称的4笔交易, 如原告所说, 均系账号支付, 在整个账号支付过程中, 银行按规定向原告发送了短信, 系统对原告的交易如实记录, 依法履行



了合同义务。

第二, 如上所述, 原告王女士进行的4笔交易中, 最关键在于客户自己的手机SIM卡及相关交易动态口令、手机验证码等身份认证要素, 原告应对此要素的保管和使用负责, 由此产生的交易后果, 应由原告自己承担。

第三, 账号支付可分为信息发送和信息接收两个阶段, 如前所述, 银行在信息发送阶段履行了合同的义务, 银行的系统显示发送信息正常, 而原告王女士没有收到被告的信息, 问题出在信息的接收介质, 即原告的手机及SIM卡。而这个过程的问题, 应由原告负责。

第四, 原告方认为, 银行从“在银行无证据证明储户遗失银行卡及泄露密码的情况下, 出现银行卡被盗情况, 说明银行安全措施存在问题”的角度来论证账号支付类交易中银行的过错, 不符合逻辑。

## 判决

法院经审理认为, 原告王女士提交的诉讼证据, 并不足以证明被告某银行未完全履行合同义务, 也不足以证明银行对保证原告卡内存款的安全有漏洞及在交易中有过错。而被告银行方提出的相反主张, 且提交的相关诉讼证据足以证明其履行了银行职责, 故法院对原告的主张不予支持。依照规定, 判决驳回原告王女士的诉讼请求。

## 释法

王女士提供的证据不足以证明银行存在交易安全漏洞以及在支付过程中存在过错。本案中, 原告王女士在被告银行办理了银行卡, 即建立了储蓄存款合同关系。原告开通并使用账号支付交易工具, 则原、被告又建立了委托代理合同关

系。如原告王女士所述, 其与银行方所签订的网上银行协议, 符合法律规定依法成立。王女士办理了银行卡并储蓄了现金, 双方即建立了储蓄合同关系。王女士将款存入银行, 银行应负有保障交易安全的监管义务。王女士为此提交了公安局对原告银行卡被在网上消费, 以信用卡诈骗罪予以立案的材料。从该证据的内容来看, 并不能说明王女士的银行卡如何被网上消费的具体事实, 也没有对该行为定性。王女士提交的其他证据, 并不足以证明银行未完全履行合同义务, 也不足以证明银行对保证王女士卡内存款的安全有漏洞及在交易中有过错。

银行提出的证据足以证明其在支付过程中没有违约和过错。在开户资料中, 银行已对王女士进行了相关的风险提示。据银行提交的银行系统交易流水显示, 2014年7月28日王女士的账号通过网银动态口令、手机验证码交易了4笔消费业务, 一切都按照双方合同约定正常进行。原告王女士无证据证明银行在网上银行操作系统存在问题。相关手机短信因王女士的手机接收系统“卡壳”未收到, 恰恰说明其接收媒介出现问题, 银行电子服务系统接收到交易验证码当然视为本人同意的划拨转账。

警惕网银风险签名认证可减少储户责任。据专家介绍, 银行卡信息泄露通常有以下渠道: 持卡人将交易凭条随手丢弃; 网上交易时, 赠他人免费WiFi使用; 网上交易时不小心进入“钓鱼”网站; 将银行卡给朋友应急使用等。发生银行卡被盗刷后, 持卡人想举证银行有过错, 往往很难, 这种情况下起诉银行有违约责任, 也可能吃力不讨好。律师建议, 市民与银行签订服务协议时, 最好明确持卡交易中使用签名认证, 而不使用密码认证, 这样, 银行卡被盗刷后, 将会加大银行承担责任的概率。

原告王女士虽败诉, 这场诉讼的社会意义远远超过了法律意义。银行卡作为自然人和单位的“钱袋子”, 其支付手段和储藏功能在经济生活中发挥着十分重要的作用, 网上支付给传统的结算手段带来一场深刻的革命, 然而在享受高效便捷的同时, 也给人们的资金安全带来了巨大的风险。要堵塞电子交易漏洞和搞好网银风险防范, 这里面有银行的责任, 也有储户的责任, 同时还需要利用科技发明提高金融电子服务手段的安全保密系数, 依靠科技升级更新“扎紧篱笆”。

市公安局干河陈分局

## 开展防电信诈骗宣传

本报讯(见习记者 李文婧) 3月29日下午, 市公安局干河陈分局组织民警走进辖区街道、居民小区、河堤游园等场所开展防电信诈骗宣传。民警们通过讲述生动案例、散发宣传单等形式向群众讲解什么是电信诈骗、电信诈骗的形式以及如何防范电信诈骗。

据悉, 本次干河陈分局开展的防电信诈骗宣传是市公安局打击多发性侵财犯罪“春雷行动”的一部分。负责组织这次活动的民警沈毅恒对记者说: “随着网络、电信等通信技术的广泛应用, 很多不法分子采取打电话、发短信、网上购物等方式, 经常进行各类诈骗犯罪活动, 给人民群众造成很大的经济损失, 我们这次宣传的目的就是要帮助群众识别什

么是电信诈骗, 提高群众的防范意识, 从根本上遏制电信诈骗案件的发生。”

民警提示

市民日常打电话和银行转账、汇款要做到“四个不要”、“一个只要”: 不要轻易泄露个人信息和银行账户资料、密码等信息; 不要轻信来历不明的电话和信息; 不要轻易给陌生人转账、汇款; 不要按照别人的提示在ATM机上操作银行卡。只要是涉及钱和账的事, 一定要谨慎, 必要时要向公安机关报案、咨询。

银行员工、保安人员在为群众办理异地汇款等业务时, 应及时对群众进行善意提醒, 遏制电信诈骗案件的发生, 发现问题及时向公安机关报告。

召陵区司法局

## 整治“四风”突出问题

近期, 召陵区司法局结合我市四项突出问题专项治理工作自查情况的开展, 查纠该局“四风”突出问题。

该局紧盯重要节点和关键少数, 采取明察暗访、随机抽

查、跟踪督查等方式, 加大检查力度, 重点检查干部到岗及上班期间是否存在看电影、玩游戏、逛淘宝以及公款旅游、公款大吃大喝、超标准接待等情况。

吕盘根

郾城区司法局

## 组织开展网上祭英烈活动

4月1日上午, 郾城区司法局组织人员开展“我们的节日·清明——网上祭英烈”活动。

活动中, 大家都积极参加中国文明网平台开展的“网上祭先烈”活动, 通过写下寄语、网上祭奠英烈、网上献花、缅怀先辈, 铭记革命先烈

的光荣事迹, 抒发自己对革命烈士的真挚情感。通过活动, 进一步引导机关干部职工继承弘扬革命先烈优秀品质, 振奋民族精神, 凝聚中国力量, 使广大司法行政干部职工以身正纪, 转变作风, 努力创新, 促进司法行政工作更好地开展。

王 欢

## 民警助走失老人“回家”

日前, 市公安局阴阳赵分局民警王平定、潘宏伟走访到省道241程庄村公路边的商店时, 看见两位年轻人站在一辆面包车旁边, 一脸焦急与无奈, 于是民警上前询问情况。原来两人把车停在路边休息时, 一位老人趁机坐上了车, 老人不说自己叫啥, 也不知道家是哪里的, 不管怎么劝说, 就是不下车。面对民警的提问, 老人答非所问, 只说自己

要回家, 但说不出具体信息。

经过一番劝说, 老人终于同意从车上下下来跟随民警去派出所。到派出所后, 民警耐心与老人沟通, 老人终于想起自己姓名, 并说自己住在阴阳赵镇水坑赵村。民警立即联系该村村干部。经了解, 原来老人患有精神病, 是该村“五保”户, 现在阴阳赵镇敬老院生活。民警随即又联系敬老院, 并驱车将老人送回。

刘晓杰

