# 卡没离身,两储户92万存款丢了

## 事发青岛同一银行支行,出事的银行卡多是磁条卡

**35万元存款在睡梦中被人转走,如此大额的存款丢失,究竟是因为银行系统漏洞,还是储户大意泄露了密码?奇怪的是,这并不是个例,涉事银行的储户在半月内遭遇了两起存款丢失事件,总案值达到92万元。**

本报记者 姜宁

### 一觉醒来,35万元被人在两地转走

青岛市民臧先生说,4月1日下午,他的银行卡内收到了35万元的转账款,可第二天一早,他去银行取款时发现,原来钱早在凌晨1点多的时候,就被人在河南、广东两地转走了。慌了手脚的臧先生,急忙报了案,也联系了这家银行。

从臧先生提供的银行流水单据上,记者了解到,这35万元存款是被分为13笔取走的,其中有30.5万元是通过郑州市一家电器商行的POS机转账,另外4.5万元通过广州市白云区的银行ATM取走。“这张银行卡,我从来都是放在身上的,也从来没有对外人说起过卡号密码。”臧先生在联系了银行之后,银行方面很快便堵截了通过POS机转账的30.5万元。“剩余的4.5万元,最近我们会协助警方办案,争取早日给市民一个说法。”这家银行青岛市分行一位负责人说。

3月中旬,一市民的57万元存款也是在这家银行昌乐路支行“丢失”,4月初,臧先生的35万元存款又在这一银行网点遭遇了盗刷。半个月内,这家支行“丢了”92万元存款。

元旦之后,青岛市出现了多起市民存款被盗刷的案件,从伪基站发送诈骗短信,到连接WIFI导致个人信息泄露,再到银行卡片被“克隆”,犯罪分子的盗刷手段越来越多。“一般来讲,诈骗短信针对中小储户,一些大额储户的银行卡才可能被‘克隆’。”银行业内一位知情人士介绍,犯罪分子的手段让银行越来越感到防不胜防。

### 大多盗刷案都发生在晚上11点之后

据银行专业人士分析,臧先生的这张银行卡在事发前就已被犯罪分子克隆完毕,待这35万元转入后,身处广州和郑州的犯罪分子分头作案。“大多数盗刷案件都发生在晚上11点钟之后,因为这期间市民的防范意识最差,发生了存款盗刷,也很难及时补救。”银行知情人士介绍。

从银行转账流水中得知,30.5万元是通过商户POS机转账进行盗取。“因为ATM机每日的取款限额为2万元,所以臧先生的大部分存款是通过POS机转账的。”知情人士说,正是因为有银行每日取款限额的存在,才让臧先生避免了大部分存款的损失,因为在犯罪分子进行POS机转账之后,资金不会立刻打入目标账户中,从而给了银行方面足够多的时间来冻结臧先生的账户。此外,银行知情人士还介绍,臧先生此次遇到的是克隆卡盗刷的情况,而对一些通过支付宝支付等无卡盗刷案件,中间代理商都会有先行赔付措施。“我们遇到过的最大先行赔付案件是6万元,即市民遭遇盗刷之后,第三方代理先将钱赔给受害者。”

针对此事,该银行青岛分行的工作人员告诉记者,他们近日将会积极配合警方前往郑州和广州两地调查此事,为的就是尽快找回臧先生另外的4.5万元钱。“通过ATM取款后,就不太好找回了,除非是警方抓到犯罪嫌疑人,或者是银行承认自己存在过失,给客户以赔付。”银行知情人士说。

### 低成本作案,测录机仅售几百元

据记者从工农中建四大行了解到,大多银行卡盗刷案件出自磁条卡,因为磁条卡安全性能较低,从而给了犯罪分子可乘之机,要想真正防范风险,最好的方式便是将手中的磁条卡换成芯片卡。

李沧区书院路附近市民满先生在睡梦中接到银行的扣费通知,说他的银行卡在广东被刷走9000多块钱。据最后调查显示,满先生的银行卡遭遇了克隆,这种短小的测录机在网上的售价仅为几百元。“有很多犯罪分子到酒店、餐厅等公共场合‘卧底’,待市民刷卡时,趁其不备,测录了市民的磁条卡信息,然后克隆一张卡片进行盗刷,而芯片卡就不一样了,全国仅有银联总部等为数不多的几个地方能够破解芯片卡的安全防护装置,相比破解磁条卡来讲,难度太大。”一位银行工作人员说。

从今年4月1日开始,磁条卡正式退出银行舞台,市民到银行开办的所有银行卡都已是芯片卡,但这并不代表着所有的磁条卡都已被废弃不用。据了解,很多市民因为怕麻烦或者不愿意花钱换卡等因素,没有及时到银行更换磁条卡,从而给了犯罪分子以可乘之机。“现在大银行换芯片卡基本都不花钱了,办新卡可能会花10块钱,但是很多人还是不愿意来换卡,因为一些市民没有意识到磁条卡存在的安全漏洞。”银行工作人员说。

此外,市民在银行卡密码设置方面也不要太过简单,尤其不要使用身份证号、生日、手机号、邮箱密码等作为支付密码。这是因为,黑客想入侵储户银行账户,就会根据储户个人信息进行匹配,比如储户生日、手机号等,企图试出支付密码从而盗走存款。一旦储户设置这些信息作为密码,很有可能中了骗子的圈套导致存款“蒸发”。

银行卡遭盗刷后,臧先生从银行拿到的盗刷提现转账明细表。
本报记者 姜宁 摄

### 揭秘银行卡复制盗刷流水线


相关链接

### 扒一扒那些安全漏洞

据记者多方探听得知,现在银行系统内也有不少安全漏洞,这给了犯罪分子可乘之机,这些银行漏洞,有的已经被及时修正,还有一些仍没有得到修复。

●已修正

**四位密码也能取款**

虽然这一银行安全漏洞已经及时被终止,但是仍然让人后怕。据一银行工作人员介绍,在3年前,某国有大行的一部分银行卡的六位取款密码只要输入前四位,按回车键后就能从ATM正常取款。这是由于该操作系统内有一部分老旧银行卡,当时使用的是四位数密码,在系统密码升级至六位后,这些没有及时改密码的老卡密码只要键入四位,也能进入取款页面。不过,这一安全漏洞已经被银行及时堵住。

●仍存在

**没交易密码也能盗刷**

一般来讲,犯罪分子只有同时拥有了交易密码和登录密码之后,才能进行盗刷,但是稀奇的是,有的犯罪分子恰恰能通过银行的系统漏洞来作案。

据了解,前几日,一犯罪分子在盗取了市民的网银登录密码后,利用银行购买贵金属不需要输入登录密码的漏洞,将市民账上的资金都购买了黄金,这样一来,市民资金账上的钱为0,然后犯罪分子冒充银行工作人员,提示市民资金账户上出了问题,要求市民将钱转到骗子的“安全账户”,为了让市民相信自己的银行工作人员身份,骗子在打完电话后,快速将账上的黄金卖出,让市民相信自己有能力为账户上的钱“解冻”。

本报记者 姜宁

### 防盗刷要“磁”旧迎“芯”

有律师表示,原则上来说,如果银行的系统安全存在漏洞导致盗刷发生,银行需要承担相关责任;如果银行尽到了维护系统安全的责任,而是持卡人自身原因导致卡片信息泄露,相关责任由持卡人承担。具体到此次事件,还在进一步调查中,到底谁的责任还不好说。

银行卡频频被盗刷,一个共同的特点是使用了磁条卡。这与磁条卡本身的漏洞不无关系。据了解,银行卡磁条有三轨信息,只要将这三轨信息通过电脑软件写到空白卡上,很容易就能复制一张信息完全相同的卡。不法分子正是利用这一漏洞,将复制装置安装在ATM(自动取款机)或POS机上,获取持卡人的相关信息。

其实,早在2011年,人民银行就启动了银行卡芯片化进程,以逐步实现从磁条卡向金融IC卡过渡,旨在提高我国银行卡的整体风险防控能力,降低风险损失。金融IC卡又称芯片银行卡,采用中央处理器(CPU)芯片作为介质,它每刷一次,信息就变一次,因此很难被不法分子“克隆”,可以有效阻止伪卡欺诈行为的发生。 (宗禾)