

无须偷窥密码即可复制盗刷

——你的银行卡还安全吗



偷窥密码已经过时了

在许多ATM提款机上,都能见到“输入密码时请注意遮盖”等安全提示。因为在传统的作案手段里,偷窥密码是比较常见的行为。

2014年,南京市就发生了这样一起案件:一名消费者在鼓楼区某酒店请客户吃完饭,女服务员主动接过卡到前台刷卡买单,结果不久后消费者发现卡被盗刷。其实,这是一个盗窃银行卡信息的团伙,他们派出一些年轻女子随身带着能复制银行卡信息的“猫仔机”,以服务员身份“潜伏”到一些大城市的酒店和娱乐场所。刷卡时她们用机器复制银行卡信息,并偷看客人输入的密码,然后把信息转给同伙复制。

浙江绍兴的卢女士也是在超市刷卡时被收银员复制了磁条,偷窥了密码,导致卡被盗刷。类似的案件还有很多。

在这些案件里,“偷窥密码”似乎成为一个要素。但事实上,随着技术的进步,你的银行卡密码就算不被别人看见,卡也照样能被复制和盗刷,而且无需“内奸”潜伏。

5月13日,昆明市公安局五华分局就公布了这样一起案件,这次犯罪分子的手段更为直接——改装刷卡机使其能够窃取银行卡的信息和密码,然后卖或租给商户。消费者到使用着改装刷卡机的商户刷卡时,银行卡信息就被窃取并复制。警方抓获的这个团伙,嫌疑人就有16名。他们非法窃取了1000多张银行卡的信息,盗刷了50余名受害人共计290万余元。由于涉及到云南、四川、河南、广东、上海、江苏等地,查实有一定困难,给消费者带来的实际损失可能还远远不止于此。

这个团伙在改装刷卡机时利用到了这些设备:刷卡机、破译芯片、电子按键软膜、手机通信发射器、内存卡。这些设备有的用于破解卡信息,有的用于记录密码,有的用于发射或存储信息。而团伙头目也很“高端”:计算机专业本科毕业生、一知名IT互联网公司在职员工。

“犯罪分子的手段越来越高明。上述方式科技含量更高、更隐蔽、侦破难度极大。”办理此案的王警官说。

银行卡信息破译:那都不是事儿

安全隐患、监管乏力……面对诸多问题,消费者在使用银行卡时陷入了两难境地。

除了盗刷,银行卡信息可被轻易破译也是一大问题。作为招商银行信用卡的用户,记者就曾经接到过诈骗电话,且能报出记者的姓名、单位、招行卡号,甚至曾在信用卡商城进行过消费等信息。上网搜索不难发现,有不少招商银行信用卡的客户都有类似遭遇,有的已经被骗,但致电招行后,仅能得到一个“我们已经了解到这一情况”的答复。

而一旦银行卡在使用的某个重要环节出现问题,被盗刷几乎成了必然。在昆明市发生的这起案件中,受害人正是利用了刷卡机的销售漏洞:我国刷卡机的指定一级代理商有160多家,下面

还有许多二级、三级代理商,加上生产厂家也不少,导致了市场较为混乱。犯罪嫌疑人于是利用这种乱象,将改装过的刷卡机通过经销商卖给商户。“这家经销商是挂靠在一家二级代理商下面的,以该代理商的名义与他人签合同。”王警官说,经销商对设备被改装过并不知情:“一般的刷卡机要三四千元,而他从犯罪嫌疑人那里买来的刷卡机只要1000多元,出于利益驱动他并没有对供货商进行相应的审查。”

“银行卡给人的感觉太不安全了,所以我基本不用银行卡。”30多岁的昆明市民王女士说,就连单位办理的工资卡,自己也取消了卡,只留下了存折。昆明市民俞女士则对刷卡机的销售方式存疑:“毕竟是跟银行卡相关的设备,竟然到处都能买卖。这样太不安全了。”

关键是损失该谁买单

遭遇了银行卡克隆盗刷的消费者,损失无疑是巨大的。如昆明这起案件,警方查到的盗刷金额有290多万元,但目前追回的只有20多万元。

对此,云南凌云律师事务所主任李春光认为,银行对储户的财产安全保障责任既是约定的义务也是法定的义务。银行卡可以被轻易破译,足以说明银行方面的保障义务履行不足乃至严重缺失。就此引发的财产损害后果,银行应向储户承担足额赔偿责任。如果寄希望于储户提升安全意识,以防范将银行卡类犯罪,既不可能也不现实。在一些案件中,储户根本无法防范信息被复制、发送和盗刷。因此,希望银行业在收费问题上已与国际惯例快速接轨的背景下,能让储户的权利和保障也尽早与国际接轨。

云南大学法学院副院长高巍分析,在实际操作中,用户如果对自己的卡和密码尽到了保护义务,有不少判例是判银行承担全部或部分民事赔偿责任的。

记者了解到的相关案例表明,前些年频频发生的银行拒赔现象正在改变,银行主动赔偿、经法院调解赔偿和判赔的案件越来越多。多方面的原因,使银行方面也在寻求更安全的银行卡,如在推行的磁条卡换成芯片卡就是举措之一。

“银行卡的保密性和不可复制性需要银行不断采取措施加强。毕竟新形势下,一些案件根本不是普通消费者能够防范的,除非他们彻底不用银行卡。”王警官说。

(据新华社电)