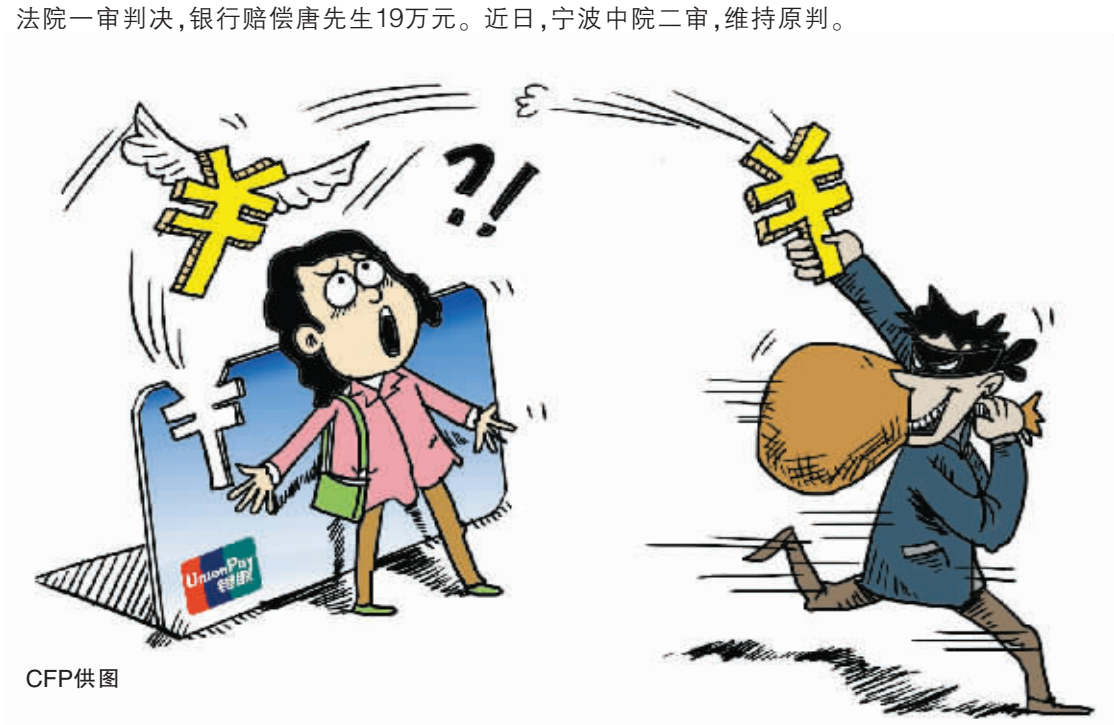
银行卡在身边却遭异地盗刷

事主立即做了三件事，最终挽回19万元损失

□记者 王思勤 通讯员 郑禾

银行借记卡在身边没动，却突然接到提醒短信，说卡内19万存款被转走，市民唐先生急坏了，立即找了银行并报警。在之后与银行交涉未果的情况下，唐先生将银行诉至法院，要求赔偿。镇海法院一审判决，银行赔偿唐先生19万元。近日，宁波中院二审，维持原判。



CFP供图

被盗刷后他立即做了三件事

2013年6月8日，唐先生在某银行办理了一张借记卡。他是开厂的，平时和客户都是通过微信支付货款。截至去年11月18日上午，这张绑定微信的借记卡内存款余额还有19万余元。

11月18日18时40分，唐先生手机突然收到一条转账提醒短信：您尾号为××××的银行卡，18日18时40分转账19万元……唐先生惊呆了，自己在家里吃饭，卡也在身边，怎么会出现这么大笔的银行转账？他意识到，应该是银行卡遭到了盗刷。

顾不上吃饭，他拉着老婆跑到最近的ATM机，让老婆赶紧在卡里存了100元，自己则在一旁给银行打电话挂失。银行客服说，卡里的19万元已被转出，只剩下58元。唐先生马上打电话报警，之后又赶紧跑到最近的派出所备了案。公安很快就查出，钱是在河北唐山在一种带有刷卡设备的固定电话机上刷走的。

由于与银行交涉未果，唐先生便以储蓄存款合同纠纷为由向镇海法院提起诉讼，要求银行赔偿存款损失19万元，并赔偿相应的存款利息损失。

事主认为银行未尽安全保障义务

在庭审过程中，唐先生认为，他与银行间存在储蓄存款合同关系，他将钱款放在银行处保管，银行有义务保护存款安全，银行未尽安全保障义务使得唐先生存款被盗，银行负有不可推卸的责任，依法应当承担赔偿责任。

银行方认为，唐先生在银行开卡，并设立密码，密码只有唐先生知道，银行已将包括密码保护在内的提醒及相关事项告知唐先生，尽到了注意义务。唐先生将借记卡与微信等第三方交易平台进行绑定，存在第三方泄露密码的可能。

此外，唐先生还可能存在密码使用不当或密码设置过于简单等问题。同时，在银行借记卡章程中约定“凡密码相符的借记卡交易均视为持卡人本人的合法交易”、“对于挂失生效前发生的资金损失发卡行不承担责任”等内容。总之，银行并不存在任何过错，故无须承担民事赔偿责任。

法院：银行未能有效识别伪卡应担责

法院审理认为，原告唐先生在被告银行办理了具有储蓄功能的借记卡，并存入存款，储蓄合同关系合法有效。唐先生的借记卡中19万元在河北唐山市转入案外人账户，转账在带有卡槽的固定电话机上进行刷卡并输入密码完成，而原告本人及其借记卡均位于浙江省宁波市，故可以认定涉讼的借记卡存在伪卡。

原告在发现借记卡被异地操作后，立即向公安机关报案，采取了补救措施，及时防止损失扩大，并无过错。而使用借记卡进行消费、支付、取现是银行广泛开展的业务，银行应保障其发放的借记卡具有可识别性和唯一性，并完善真假借记卡的识别技术，以防止非法分子通过伪卡侵权。本案中，被告银行作为发卡行，未能对伪卡有效识别导致盗刷，应对其服务瑕疵或履约瑕疵造成的储户损失承担赔偿责任。

此外，虽然银行借记卡章程约定“凡密码相符的借记卡交易均视为持卡人本人的合法交易”、“对于挂失生效前发生的资金损失发卡行不承担责任”，但这些条款系银行为重复使用而预先印制，系合同法意义上的格式条款，该条款免除了被告审核银行卡真伪的义务及相应的法律责任，不能当然被认定有效，故被告不能据此免除自己的责任。

最后，被告银行称原告唐先生将借记卡与第三方交易平台进行绑定，存在第三方泄露密码的可能，但并未提供证据证明确实是因为原告将借记卡与第三方交易平台进行绑定而造成密码泄露。至于银行称原告可能存在密码使用不当或密码设置过于简单等问题，由于也没有事实依据与法律依据，法院不予采纳。

综上，法院判决，银行赔偿唐先生19万元。

法官提醒

被盗刷后要赶紧做这三件事

银行卡遭到盗刷后，到底该怎么办？昨天，镇海法院的法官建议要尽快做三件事：

首先，通知银行并办理挂失。持卡人应立即拨打银行客服电话告知账户异常变动情况，办理挂失。

其次，拨打110报警。持卡人在通知银行后，应及时报警，告知盗刷金额、方式、时间、地点，以及交易另一方账户信息。

最后，立即去ATM机上操作。持卡人应迅速到附近的ATM机操作银行卡。此举的目的在于证明卡主和银行卡均不在盗刷现场，证明银行卡系被他人伪造并盗刷。在伪卡盗刷案件中，盗刷发生后及时通过ATM机进行真卡操作，是证明发生伪卡盗刷行为的有效方式之一。

通过QQ诈骗的最多

冒充“公检法”的老套骗局依然骗倒不少市民

□记者 马涛

昨天，我市警方对今年一季度通讯（网络）诈骗案件进行统计分析，利用数据直观呈现了当前我市网络诈骗犯罪形式和未来变化趋势。

据分析，以银行、航空、淘宝或QQ客服等为主的常规诈骗案件仍十分突出，QQ、微信、淘宝是网络诈骗的主要平台。其中，40岁以下中青年为主要受害者，冒充“公检法”和社保、消防军警等行骗的行为居高不下。

冒充“公检法”骗走市民60万元

今年4月18日，市民郭女士接到陌生电话，来电显示是上海。对方自称是宁波市医保局的工作人员，说她的医保卡涉嫌洗钱，被锁住不能用。一听这话，郭女士顿时慌了，解释自己最近没去过上海，也没有办理过任何社保业务。对方建议郭女士报警，并直接为她转到“上海闵行公安分局”。

一名“警官”证实，她的医保卡在上海骗保，有人利用她的身份证洗钱。“警官”提出，为了确保其资金安全，得尽快将钱转出去。根据他的指示，郭女士通过ATM机向对方账户里汇入55万元。

第二天，一个自称“检察院”的工作人员打来电话，说案子还在调查中，要求她将所有钱转到安全账户进行资金清查。

就这样，郭女士又汇走5万元。在朋友提醒后，当她再次拨打“医保局”、“公安局”等电话，才发现不是关机就是无法接通，这时她才明白过来。

据办案民警说，通过对涉案10万元以上的案件分析，冒充特定身份诈骗案件达67.16%。

其中，冒充公、检、法或社保局谎称被害人涉案的通讯诈骗案件19起占27.15%，杀伤力最大。

此外，冒充消防等军警以虚假购买军需品或虚设工程项目的方式，实施诈骗的案件共8起，占11.43%；另以网上投资理财等方式实施的诈骗案件12起占17.15%。

QQ、微信、淘宝成网络诈骗主要平台

陆先生年近60岁，是宁波一家知名企业的经理。今年1月18日，一个陌生号码加了他的微信，对方用的是老板的头像和名字，陆先生以为是老板本人。

“老板”开门见山地说，转了27万元到他的银行卡上，不过要24小时后才能到账，让他先另外掏钱转给一个客户。

微信中，老板还拍了张照片，是电脑转账记录。陆先生没有太多怀疑，因为对方说话的口气和老板很像，而且以前他也给老板办过同样的事。手头钱不多，他还找朋友借钱，当天陆续转过去7万。

不过，当天当他联系上老板时，对方说根本没有这回事。陆先生意识到上当，当晚就报了案。

第二天，他听说公司好几个同事都收到了老板通过微信要求转账的信息，所幸，同事们没有被骗。

民警分析，骗子可能是通过手机号搜索到陆先生的微信，而使用的银行转账截图，很可能是“PS”的。事实上，要识破这样的骗局很简单，只要打一个电话跟老板核实一下就清楚了。

梳理类似的网络诈骗，可以看出骗局主要依托QQ、微信、淘宝网等平台进行。

其中，通过QQ诈骗的有112起占60.2%，通过淘宝网诈骗的有29起占15.6%，通过微信诈骗的有43起占23.1%。