银行卡中储存着不少的财产信息，稍有不慎便会被他人窃取，发生银行卡盗刷案件。看着钱款从银行眼皮底下溜走，很多受害人认为银行难辞其咎。

那么，银行卡盗刷事件的责任该如何认定呢？哪些情况是银行之过，哪些情况要自己承担？我们通过4个不同类型的案例，来看看法院如何解答。

案例1：近距离异地被划款

市民张女士家住在上海市嘉定区安亭镇。2016年10月的一天，张女士突然一下子收到了6条短信，上面显示张女士的中国银行借记卡在1019号ATM机上先后发生了支取和转账3笔交易，金额共计2.6万余元，交易地点是在家附近的昆山花桥市。张女士当时身在嘉定，且并未去过花桥，她马上意识到自己的银行卡是被盗刷了，当即打电话与中国银行的客服进行了联系，并将涉案的借记卡挂失后去安亭派出所报了案。

经公安机关调查，这3笔交易的操作人并非张女士，并且所使用的银行卡也并非张女士的涉案银行卡。与此同时，张女士也向上海嘉定法院提起了诉讼，要求被告中国银行赔偿其被盗刷银行卡造成的损失。

法庭辩论中，被告银行表示，涉案借记卡交易发生地点在中国银行昆山花桥支行，而张女士在安亭，距离不过才半小时车程。被告有理由相信，张女士可在涉案交易点自行进行交易后再返回，所以不能证明交易时银行卡不在张女士身上，也不能证明涉案交易是伪卡盗刷所致，因此请求法院驳回张女士诉请。

法院审理后认为，张女士在被告处设立个人银行结算账户，被告向原告张女士发放借记卡，双方形成储蓄合同关系，双方均应依法履行各自义务。原告张女士作为被告借记卡持卡人，在其得知所持借记卡发生非正常交易后，立即与中国银行客服联系，挂失涉案借记卡，并向公安机关报案。

作为储户，张女士已尽到了其基本的注意义务。并且，上海市公安局嘉定分局已将涉案的交易作为诈骗案处理，可以说明涉案交易不是张女士本人操作。而关于被告银行所提出的涉案地点距离较近的问题，法院认为，根据张女士及银行工作人员的陈述，可以判断张女士与他人串通欺诈银行的可能性较小。此外，涉案金额仅2.6万元，这样的风险报酬似乎并不值得去冒险。

因此，法院认定涉案交易行为系伪卡交易。被告作为借记卡的发卡行及相关技术、设备、操作平台的提供者，在其与储户的关系中明显占据优势地位，其应承担伪卡的识别义务。被告银行在没有证据证明原告存在违约或违法犯罪情形的前提下，理当先行向储户承担因银行安全系统漏洞及技术风险所造成的储户资金损失。即使《

个人账户开户及综合服务协议书》约定以原告资金凭证和密码所进行的一切交易均视为原告（意愿）亲自办理，但该条款适用前提必须是当事人持真实的借记卡进行交易，持伪卡交易的不应适用该条款。

综上，被告作为发卡行，对持伪造借记卡交易的案外人支付了原告账户内的资金，未尽到对储户银行卡内资金安全的保障义务，应承担违约责任。张女士要求被告支付存款损失，合理合法，法院予以支持。

案例2：点错网址泄露密码

2010年，市民林先生在工商银行开通了一张银行储蓄卡，并在同日开通了电子银行。2015年，林先生为了更加方便自己生意上的往来，向工商银行申请了开通工商银行的电子密码器。按照办理流程，他在《申请凭证》上签字确认已阅知并同意遵守凭证背面的《客户须知》，同时还在《工银电子密码器领用须知》上签字确认已阅读和知悉上述内容，并自愿遵守和承担相应责任。

2016年的一天，林先生收到了一条发送者为“95588”的短信息，内容为“尊敬的工行用户：您的电子密码器将于次日已失效，请速登入www.ixdva.com升级激活，给您带来不便请谅解！工商银行”。

收到短信后，林先生当晚就用家中的电脑登录了短信中的网址，但是数次登录后，网页却一直显示网址无效。林先生觉得奇怪，他再次打开那条短信，直接在手机上点击了短信中提供的网址。这一次，林先生顺利打开了网页，和平常使用的工行网页看起来并无二致，林先生放心地按照网页上的要求输入了账号及密码。不料，稍后林先生又陆续收到了工商银行发来的两条短信，这次竟然是通知他的银行卡在办汇款，前后共汇走了24万余元。

林先生发觉事情不对劲，立即拨打了工商银行的客服电话，听了林先生的讲述后，客服人员告知林先生，他应该是收到了诈骗短信，并对林先生的银行卡进行了冻结，让林先生第二天去工行网点拉出详单报案。

因为不小心点击了错误的网址，林先生一下子就损失了24万余元，他认为银行作为网银交易服务的提供者，应该保证交易安全，且网银交易存在安全风险，造成的损失不应让储户承担。为此，林先生向法院提起了诉讼，要求被告工商银行赔偿自己存款资金被盗造成的损失24万余元，并支付自资金被盗之日起至今的利息损失（按同期银行贷款基准利率计算）。

法院审理后认为，原告林先生在被告工商银行处办理领取银行卡、开通网上银行，并申领了介质密码器，应对电子银行相关介质和密码负有妥善保管责任。工商银行

的真正官网在《工银电子密码器领用须知》《中国工商银行电子银行个人客户服务协议》中都有明确记载。而且，林先生开通网上银行后自己实际操作过网上银行的转账业务，因此他对于工商银行的官网网址是明知的。林先生在收到短信后，本应注意到信息上所显示的链接与实际官网不一致，但林先生却忽视并点击了该链接，同时将自己的密码账号输入，从而将自己重要的资金信息泄露，导致涉案银行卡两笔款项通过工银电子密码器被转出。

而被告方面，工商银行在《工银电子密码器领用须知》《客服服务协议》中已经提醒原告林先生须保管电子密码器的开机密码、不得将工银电子密码器上生成的动态口令泄露给他人，特别提示原告在网页上输入电子密码器上生成的数字，要特别注意网站的域名是否是工行官网，如果不是千万不要输入，因此被告已经尽到安全告知义务。

因此，法院判定驳回林先生的全部诉请。本案涉案两笔款项的转出，是由于原告林先生自身过错所致，被告并不存在过错。

案件3：人卡分离被盗划

市民曾先生在上海和连云港两地做五金机电生意，平时要时常奔波于上海和连云港，因此大部分的钱款及银行卡都不会随身携带，而是经常放在家中，由家人保管。但就是这样的做法，最终造成了曾先生16万余元的损失。

2017年4月份，曾先生打算刷卡购物，但是结账时却突然发现自己卡内余额不足了，曾先生大吃一惊，明明这张银行卡里应该有10多万元，怎么会连几千元的余额都没有了呢？

4天后，曾先生联系了银行客服，反映了自己的情况，确定银行卡被盗刷，过了两天曾先生又去派出所报了案，并向法庭提起了诉讼，要求银行赔偿自己16万余元的经济损失及相应利息。

卡内钱款不翼而飞，曾先生认为这是银行没有识别伪卡所致的盗刷，而银行方却坚持认为是曾先生用卡不当，没有保存好银行卡而被盗刷，双方争执不下。

法庭审理后查明，原告曾先生虽然声称银行卡被盗刷时自己人在上海并未与卡分离，但是却始终无法提供相应的证据予以证明。况且曾先生由于其工作原因，经常人卡分离，在系争交易发生后，曾先生非但未及时向发卡行客服反映被盗刷情况，反而间隔4天后才致电客服，且在6天后才选择报案，此举更加无法证明曾先生在涉案交易发生时本人及真卡所在的位置。

同时，法院也注意到，系争交易发生的时间亦属正常交易时间，结合曾先生平时存在人卡分离的情况，综合考量，不能断定系争交易持卡人所使用的卡片为伪卡。

在此案中，系争储蓄卡须凭密码交易，原告曾先生在法庭审理时也未能提供证据证实被告银行存在泄露曾先生储蓄卡密码等信息的违约行为。

综上，根据谁主张谁举证的原则，曾先生理应提供证据证明银行存在无法辨识伪卡或泄露信息的违约行为，但原告曾先生提供的证据并不足以证实，因此对于曾先生要求被告银行赔偿经济损失的主张，法院不予支持。

案件4：轻信他人被盗刷

市民王先生此前接到一通电话，对方自称银行工作人员，为拓展业务，可为林先生免费办一张高额度的信用卡，但前提是王先生需办理一张该银行的储蓄卡，并存入15万元，同时要将银行签约手机号码留成该工作人员的号码。

对此，该工作人员解释，是为了能够第一时间得知是否已存入钱款，方便尽快为王先生办理信用卡。

面对“免费”办理高额度信用卡的诱惑，王先生心动了。当天他就去银行办理了一张储蓄卡，并开通了网上银行的业务，按照之前电话中“工作人员”的要求，将银行签约手机号码留为了电话中“工作人员”所提供的手机号，当天也开通了手机银行及超级网银等业务。随后，王先生还按照电话中“工作人员”的指示，办理了两笔汇入和汇出业务。

王先生也担心遇到诈骗，并未在当天接着存入相应的钱款，而是隔了几天后，又去了一次银行。这一次，王先生将原来预留的手机号码改成了自己的手机号，同时还修改了交易密码，自认为已经万事大吉的王先生这才放心地向银行卡内存入了近10万元人民币。

可是，令王先生没想到的是，自己的重要个人信息其实早在最初按照电话中“工作人员”的指示办理时就已经泄露了，10万元刚刚存入不久，就在王先生一无所知的情况下，银行账户很快被人分两次转空了，且收款人就是最初电话中“工作人员”让王先生转账的名字。

高额度的信用卡没等到，自己反而还损失了近10万元，由于有了最初办卡时“自愿”向对方转账的记录，王先生甚至都没有办法解释这次的转账是被诈骗了。愤怒不已的王先生将办卡银行告上了法庭，认为是银行未能为自己提供安全可靠的交易环境，请求法院判令银行赔偿其损失。

法院经审理后认为，原告王先生在被告银行处设立个人结算账户，双方形成储蓄合同关系，则双方均应依法履行各自义务。此案中所涉及近10万元的两笔款项的支付，系被告银行在接收到王先生授权的银行总行的付款指令后，按照协议约定，从王先生指定的涉案储蓄卡向王先生指定的账户划款，且支付的金额未超过协议约定的单笔金额的上限。因此，被告银行的操作未存在违约或有过错的行为，且原告王先生亦无证据证明其存在近10万元经济损失的证明，因此王先生要求被告银行承担赔偿责任无事实和法律依据，法院不予支持。

在庭审中，法官注意到，王先生在最初办理银行卡时抱有非正常目的，由于听信他人诱惑，且风险意识淡漠，自身保护意识不强，最终导致自己的钱款被骗。被告银行在原告王先生办理涉案储蓄卡及修改储蓄卡相关信息的过程中，已通过书面的客户风险提示向王先生作了提醒，明确要求原告保证“本人提供的个人信息及联系方式确为本人真实信息”，并将银行客户有可能遭遇诈骗的情形一一罗列，其中就有王先生所述的情形。

然而，王先生明知此要求，还将他人手机号码预留给银行作为接收短信通知和动态密码的联系电话，从而泄露了涉案储蓄卡的相关信息，导致自己近10万元的钱款被盗划。因此，法庭判定王先生的损失与被告银行无涉，驳回了王先生的全部诉请。

理财金手指：被盗刷后如何增加获赔胜算

从4个案例看来，被盗刷后要让银行作出赔偿并不容易，客户的主张要有足够的证据支持。万一遇到被盗刷的情况，我们应该如何做到及时止损，增大赔付几率呢？法院建议，在发现银行卡有不正常的金额变动时，要立即致电发卡行客服说明情况，也要将银行卡及卡号拍照存档，并及时去派出所报案。另外，可以带好银行卡去最近的ATM机操作一次，以证明被盗刷时并非本人消费，也并未因自身疏漏而导致人卡分离。

上海市嘉定区人民法院商事审判庭审判长王筑慧表示，客户开卡，在银行设立了个人结算账户，银行向客户发放储蓄卡，双方就形成了储蓄合同关系，都应该依法履行各自的义务。作为银行一方，要最大程度地保障客户的财产安全，及时提醒客户安全交易须知，正确地识别伪卡交易。

而作为客户一方，也应该提高自己的财产安全意识，例如，在使用银行卡进行交易时注意掩盖防止密码泄露，保留好带有重要个人信息的购物票据等。尤为重要的是，要防止电话及短信恶意诈骗，对不明网站要提高警惕，不可随意点击，更不能轻易输入自己的重要个人信息。

本文源自理财周刊

更多精彩资讯，请来金融界网站(www.jrj.com.cn)