珠海的李某2014年11月发生了这样一件事，他的银行卡和网银认证K宝(类似U盘，也称USB-KEY)均未丢失，账户资金却被操作41次，以快捷支付方式转走12万元。近期李某起诉珠海某银行要求全额赔偿，珠海市香洲区法院判决银行承担20%责任，一审后双方均未上诉。

【案件回顾】41笔款被转走储户却无法收到短信

2014年9月，李某在涉案银行申领一张银行卡，并开通了短信提醒等业务。2014年11月14日21时41分，李某在自动柜员机上取现200元，指定手机收到了短信提醒。然而，从当天21时54分开始至16日的16时04分的3天里，李某的银行账户款项却频频发生变动，分别以网上银行、手机客户端、电话银行等快捷支付方式共支出了41笔款项，支出金额合计122964.78元。后来发现账户异常的李某立即挂失该银行卡，并到派出所向警方报案，该案警方至今尚未侦破。

在这一案件中，李某表示，涉案的41笔资金交易，其手机没有收到银行发送的短信交易提醒。然而银行提供了41笔款项的支出时系统短信记录，全部短信记录显示“短消息转发成功”。

【解析】不同于以往的“伪卡”交易

经过仔细分析双方提供的证据，法官发现本案中的41笔交易是通过电话银行、手机银行、网上银行的快捷支付方式进行，因此该案件不同于以往制造“伪卡”后到ATM机上取款的盗窃案件。本案中使用的交易方式不需要通过银行储蓄卡为介质，也不需要网银交易K保进行认证，在操作中只需通过电话银行、网上银行等电子银行渠道输入银行账号、密码即可产生付款行为，即便有些付款需要验证码，验证码也是发送至指定的手机上。

【审判结果】涉案资金确系被盗，双方均有过错

接到报案后珠海警方调取了银行交易流水，发现涉案41笔支出大部分属于密集重复操作，均是通过网银转账、电子收款机等快捷支付方式转走，其中2014年11月14日11时13分以李某手机号码注册了“掌钱”账号，并且在14日、16日从李某的银行账户向上述“掌钱”账号充值7笔，共计35000元，然后分别转账至李某不认识的余某和袁某农的账号，李某未向该两人汇款，也未在掌钱注册过账号。警方判断符合盗刷的基本特征，法院认定涉案资金确系被他人盗取。

之所以被盗刷，法院认为资金被盗主要是由于李某手机信息、银行账户和密码的泄

漏所造成。李某设置的账户密码由其个人掌握控制，不为银行所知，他人通过窃取密码而盗取款项说明了原告对银行卡密码保管不当，发生账户和密码泄露最终导致损失，李某使用电子银行时没有做到足够警惕和注意，对账户资金被盗负主要责任。

另外，法院认为银行作为金融机构，需增强金融服务的安全性，提高银行系统软件的技术水平，承担相应安全保障责任。银行在为储户提供电话银行、网上银行、手机银行等电子银行服务时，也应提供相应配套措施用以检测用户交易环境是否安全，以免储户账号信息泄露。

最终，法院根据双方过错的比例，酌定银行承担20%赔偿责任。

【相关知识】“伪卡”交易多是银行担责

通常情况下，“伪卡”交易多是银行担责。由于银行未能采取措施有效识别伪卡，导致卡内资金被盗刷，故而承担责任。

??????

??????????“?”??????100%????????????????????

??????????

??5????????