支付机构八大风险案例

近年来，通过非银行支付机构办理支付业务的客户资金风险案件频发，暴露出部分支付机构一味追求支付便捷而忽视支付安全、支付系统存在严重漏洞、客户资金安全和信息安全难以得到有效保障等问题。

“据统计，2014 年至今，人民银行全系统金融消费权益保护部门受理的网络支付类投诉占互联网金融类投诉的 95.06%”，“2015 年 1 月，某支付机构泄露了上千万张银行卡信息，涉及全国 16 家银行，截至 7 月 31 日由于伪卡形成的损失已达 3900 多万元。”央行有关人士透露。

现将近年来部分支付机构风险事件案例汇总整理摘编如下：

1.利用黑客手段盗取支付宝客户资金系列案

2015 年 6 月，珠海市公安机关侦破一宗横跨广东、黑龙江、四川、上海和浙江 5 省(市)的特大利用黑客手段盗取支付宝资金系列案件，打掉一个非法买卖公民个人信息、制作扫描探测软件和实施网络套现的犯罪团伙，抓获关键犯罪嫌疑人 6 名，缴获作案计算机等工具一批。该案是比较常见的支付账户盗窃案件，犯罪嫌疑人通过网上购买他人提供的账号、密码信息，使用扫号软件批量测试是否与支付机构支付账号、密码一致，比对成功后实施盗窃。公安部门初步查明，犯罪嫌疑人涉嫌盗窃支付宝账户 117 个，涉案金额 7 万余元。此外，嫌疑人电脑硬盘中存储各类公民个人信息 40 多亿条，涉及支付宝、京东和 Paypal 等支付账户达 1000 多万个，初步估算账户涉及资金近 10 亿元。

2.内鬼泄密 20G 海量用户信息被盗卖

2013 年 11 月 27 日，某支付公司内部员工因伙同他人多次以批量出售的方式泄露用户信息被杭州当地警方逮捕。据该涉案嫌疑人交代，他曾经是该支付公司技术员工，利用工作之便在 2010 年分多次在公司后台下载公司用户资料，资料内容超 20G。随后伙同两名外部人员，以 500 元 3 万条的价格将用户信息多次出售予电商、数据等公司。用户资料包括公民真实姓名、手机、身份证号、电子邮箱、家庭住址、消费记录等。据其供述，仅最大买家服装类电商 V 公司就曾通过该团伙一次性购买用户资料 1000 万条。不过 V 公司一位副总裁表示并不清楚此事。支付公司方面则承认确有内部员工盗卖用户信息案，一名负责人称：“不得不承认，我们在管理上出了一些问题。”

3.支付公司未履行安全保障义务导致消费者购物款被盗转

2014 年 7 月，张先生在某购物网站和卖家协商购买价值 27500 元的照相机一台，双方约定分多笔交易付款。后根据支付机构网页提示登录到网上银行进行付款操作，收款方名称为：XX 支付科技有限公司。付款后该购物网站显示“等待买家付款中”，张先生到银行查询被告知钱款已经打到支付机构。后张先生发现

打入支付机构的钱款被转入另外一个工商银行账户，而此账号并非本次交易卖方的账户。按照支付机构交易规则，买方没有确认收货前，支付机构不能将货款转出。张先生诉至人民法院认为该购物网站和支付机构作为交易平台的提供方和第三方资金管理方，未尽到安全管理义务致使己方购物款被盗转，要求法院判决该购物网站和支付机构赔偿其相应损失。经法院查明，支付机构未将货款转入卖方而转入他人账户，未尽到安全注意义务，其经营的网络系统、服务器和程序安全性不足，或他人利用网络技术非法入侵均有可能导致张先生的财产受到损失。最终法院判决支付机构赔偿张先生相应损失共计 20129 元。

4.网络融资平台用户资金被盗案

2012 年 11 月，上海陆家嘴国际金融资产交易市场股份有限公司(下称“陆金所”)运营的“稳赢”融资交易平台，部分用户 600 余万元资金被盗。经初步查明，犯罪分子通过买来的某银行 600 余万条账户信息，将储户账户绑到“陆金所”交易平台并通过该平台将资金转移到用假军官证开立的同名银行账户，利用“稳赢”网络融资交易平台绑定银行账户时无需提供密码且可一人同时绑定多个账户的漏洞，通过支付机构以购物退款的方式将资金转移到其实际控制的他名银行“网络账户”，以达到其转移赃款的目的。该案件暴露了以下问题：一是银行违反账户管理规定和实名审核要求开立假名账户；二是支付机构账户实名制落实不到位，对特约商户管理不严，为洗钱犯罪提供通道；三是部分网络交易平台存在安全漏洞，用户在网络融资平台注册的验证手续过于简单，且在绑定银行账户时未经银行验证。

5.网店店主利用某支付公司漏洞制作营业执照盗取资金

2014 年 3 月 5 日，嫌犯张某、刘某利用某支付公司网上平台在账户改密业务中的漏洞，盗刷数家企业在该支付公司支付账户内的资金共 20 余万元。涉嫌盗窃罪，被海淀区检察院批准逮捕。张某、刘某在某购物网站开店。在开店过程中，二人发现修改其网店的支付账户用户名和密码时，只需在网上向该家支付公司客服提交电子版营业执照即可，由于客服对电子版营业执照的审核不严，很容易受理通过。二人发现这一漏洞后，采取 PS 技术伪造其他公司的电子版营业执照提交修改密码申请，进而控制账户并盗窃资金。

6.快捷支付验证不足导致的客户资金被盗案件

托人代办信用卡的李先生由于将银行预留手机号码、身份证与储蓄卡的高清照片都泄露给骗子，尽管存款当天便惊醒，迅速去银行柜面关闭网银并更改预留联系方式，但仍未能避免三日后卡内现金被悉数盗刷而空的命运。更让李先生气愤的是，此番快捷支付扣除他的款项竟无需经过他银行卡支付密码的验证。记者获悉，开通快捷支付业务并不繁琐，只需在支付机构快捷支付页面提供本人的姓

名、身份证号码、银行卡号及银行预留手机号等有效个人信息即可快速开通，而后期支付也无需经过原有银行卡的支付密码验证，只需在支付页面输入支付密码或关联银行卡信息即可完成资金交易。对于为何支付转账等流程要越过银行卡支付密码的环节，支付机构方面对记者表示：“这是国际上的规定和惯例，不允许在网上支付的时候输入银行卡密码。”快捷支付业务模式里，银行的服务界面被屏蔽在客户的支付流程之外，银行从用户支付结算的前台，退到代理第三方清算的后台，只扮演‘账房先生’的角色，被动地处理来自支付机构的指令，不再认证用户的身份，不再掌握用户的支付行为。

7.利用网络支付平台盗划银行卡资金案

2015 年 3 月，中国人民银行四川省射洪县支行相继接到商业银行金融重大事项报告，称其客户赵某个人银行结算账户大额资金被盗划。

2015 年 3 月 11 日，赵某分别向银行反映其 5 个银行存款账户资金在 2015 年 3 月 7 日至 9 日期间遭到连续盗划二十余次，金额累计达到 21.9 万元，期间被屏蔽了手机动账短信提示。通过查询赵某 5 个银行卡个人银行结算账户交易流水，发现其资金通过上海某网络支付机构划至北京一家公司账户，系客户个人身份信息被不法分子盗取，不法分子冒用客户在网上注册三方理财公司所致。该盗划事件的特点在于屏蔽了银行客户手机动账短信提示功能，并关联客户所有银行卡个人结算账户。经各方努力，截至 5 月，客户被盗资金全部被追回。

8.不法分子利用支付平台从事虚假交易实施诈骗

广东省公安机关经侦部门在侦办一起涉嫌合同诈骗案件时发现，犯罪嫌疑人吴某、文某、曾某等人虚构现货交易平台，通过第三方支付机构将被骗群众账户的亏损资金转移至犯罪嫌疑人所控制账户非法牟利。初步统计两个平台涉及受害群众近 4000 名，涉案金额 1 亿余元。与以往虚假大宗现货交易平台直接收取被害人资金、修改数据侵吞钱款的手法相比，这种方式更加隐蔽和难以打击，应予关注。