支付结算工作简报

（特刊）

2017 年第 19 期（总第 287 期）

中国人民银行支付结算司　　2017 年 11 月 28 日

编者按：自《中国人民银行关于加强支付结算管理 防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261 号）印发以来，银行业金融机构和非银行支付机构认真贯彻落实有关要求，在封堵异常开户、堵截诈骗资金转移、强化可疑交易监测等方面积累了丰富的实践经验。现通报有关典型案例，请人民银行分支机构、银行业金融机构和非银行支付机构借鉴参考，举一反三，进一步加强支付结算管理，筑牢支付结算安全防线，有效防范打击电信网络诈骗。

防范打击电信网络诈骗典型案例汇编

目　录

一、封堵异常开户案例

（一）拒绝残疾人、学生、中老年人群体异常开立银行卡案例

银行卡非法买卖为电信网络诈骗提供了资金转移渠道。诈骗分子利用部分群体防范意识薄弱的特点，组织诱骗群体开立并非法买卖银行卡。银行应加强对此类客户的开户审核，必要时拒绝客户办理业务，同时强化风险提示，宣传个人不得出租、出借、出售银行账户及惩戒措施，提升社会公众风险防范和法律意识。

案例 1：堵截诈骗团伙组织学生开立并非法买卖银行卡

【案情概况】

2016 年 12 月 17 日，光大银行郑州花园路支行发现当天要求通过远程视频柜员机开立银行卡及开通网银业务的客户人数较往常有所增多，人员多为 18-20 岁左右的在校学生，情况较为异常。

【处置措施】

银行立即启动应急预案，停止使用远程视频柜员机开立银行卡，由柜面受理开立银行卡业务，并在客户等待区先行了解客户开立银行卡需求，意在将疑似组团办卡人员隔离，并对他们进行分开谈话，了解开立银行卡的真实用途。经过银行人员反复提示非法买卖银行账户惩戒措施，学生们说出真相，原来诈骗分子是通过 QQ 群发布兼职广告，让在校大学生以朋友转账、父母打款、学校发奖学金等理由到各家银行开立银行卡并开通网银，再以 50 元一张的价格将学生们开立的银行卡买走。本次组团开立银行卡人员约 20 多人，互相均不认识。银行人员在了解情况后立

即报警。当民警对这些学生进行笔录时，诈骗分子一直通过电话催促他们交卡，并约定了交卡地点。警方就此顺藤摸瓜，于当日下午在交卡地点成功抓获3名诈骗分子,共收缴银行卡100余张。

案例 2：堵截他人利诱组织聋哑人集体开立银行卡

【案情概况】

2017 年 5 月 4 日，6 位聋哑人同时前往农业银行宜春市分行营业部要求开立银行卡。第一位聋哑客户开立银行卡后，随即将银行卡交给同行的另外一名聋哑客户，此异常举动令人生疑。

【处置措施】

银行人员通过文字与聋哑客户沟通，得知这 6 名聋哑人的领头人为龙某，其余 5 人开立银行卡后交给龙某以获取一定的报酬。银行立即报警，并告知龙某此行为可能涉及违法犯罪活动，并拒绝为同行的其他聋哑人开立银行卡，要求刚才已开立银行卡的聋哑人销户。民警到达网点后，登记了 6 名聋哑人信息，询问相关情况后对他们进行了现场教育。

案例 3：堵截诈骗团伙组织中老年人异常开立银行卡

【案情概况】

2017 年 4 月 7 日起连续多日，大量客户分批在平安银行武汉分行多家网点要求开立银行卡并开通高级版网银。客户均非本地户籍，年龄基本都在 50 岁以上，十几人到数十人不等同时进入网点。他们大多对开立银行卡原因不清楚，无法回答具体用途，部分人员表示用于投资理财，但不了解后续操作和投资流程，只是强调可因此获得较高的投资积分及回报。在被银行人员拒绝开立银行卡后，这些客户又改为结对的方式，分散前往其他网点，

部分网点还发现网点门外有人员指挥接应的情况。

【处置措施】

银行判断该异常行为疑似集资诈骗行为，经与客户深入沟通，部分客户吐露实情：上述客户均进入同一微信群，被组织进行收藏品或珠宝投资。该微信群指示客户开立银行卡和开通网银，利用手机银行查询到辽宁当代文化艺术品产权交易中心办理入金交易，然后下载宗易汇 APP 对接前海知融泓赫珠宝公司，最后将积分转给相关人员，具体目的不得而知。鉴于此，银行拒绝了该批客户开立银行卡、开网银的申请，并对客户进行风险提示，同时向各网点通报案例。

（二）拒绝以工资卡、签订批量支付协议名义大量异常开户案例

银行应关注以开立工资卡或签订批量支付协议名义进行的群体性集中开户及单位代理开户的情况，严格按照《中国人民银行关于加强支付结算管理 防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261 号，以下简称 261 号文）等要求，审慎办理批量性、集中性开户业务。

案例 4：堵截柜面异常办理工资卡

【案情概况】

2017 年 2 月 17 日、20 日，交通银行某分行柜面出现群体性办卡的异常情况，涉及 13 人次，多为一人办卡多人陪同。申请人多为外地户籍，并且均称是上海某电子科技有限公司员工办理工资卡，但这些客户回答问题前后逻辑关系相对混乱，因此具有群体性异常开户特征。

【处置措施】

银行迅速与上海某电子科技有限公司联系，被告知工资并不在交行代发，该公司也不清楚上述群体性办卡目的。银行因此未受理以上客户的业务。但当这些客户离去时，银行人员听到客户打电话告知他人办卡时不要提及工资卡。为防范以上客户再到其他网点开立银行卡，各银行网点通过微信群、电话、邮件等方式及时进行沟通，有针对性的加强审核，共同防范此次柜面群体性异常开立银行卡。

案例 5：封堵诈骗分子利用多张证件复印件开立银行卡

【案情概况】

2017 年 6 月 10 日，杜某到华夏银行重庆沙坪坝支行咨询批量开立银行卡事宜，称其为人力资源管理公司财务人员，负责招工输送到全国各工厂，现需为新招员工批量开立银行卡代发工资，当日其拿了约几百人的身份证复印件。经粗略查看，银行人员发现绝大部分非原件复印件。经询问，杜某单位基本账户开在他行，其抱着资料逐一找银行批量开立银行卡的行为令人生疑。

【处置措施】

当日，银行以批量开立银行卡需要被代理人身份证原件复印件为由，拒绝了杜某的要求。6 月 13 日，杜某再次对办理 130 名异地工人批量开立银行卡业务进行咨询，称银行可以派人上门核实或实地开立银行卡，并提出要在网点开立单位一般账户。而后续银行人员在逐一审核客户信息时，发现大量员工手机号前 8 位数段相同，其中约 38 名不同省市员工最后 3 位数为连号，杜某称是单位统一采购的电话卡。银行为防控风险，逐一拨打其员

工电话，发现一部分员工表现较为异常，如回答问题含糊不清、不能快速答出身份证号、地址、生肖回答错误、由他人接听电话、直接挂断电话或关机。同时，银行提出先给当地员工实地开立银行卡的要求被杜某一再改期，且自称杜某领导的张某多次来电要求尽快开立银行卡，否则会延误其单位代发工资，并称批量开立银行卡后会立即安排上门实地开立银行卡。鉴于上述异常情况，银行拒绝了其提出的要求。因客户批量开立银行卡资料一直留存在银行，当 8 月份银行再次与杜某进行联系时，杜某手机处于长期关机状态，微信也已无人应答。

【案例启示】

银行要严格执行“了解你的客户”原则，加强对异常开户行为的关注，严格联系电话号码与身份证件号码的对应关系，把控客户身份信息审核关。

案例 6：拒绝以已签订批量支付协议为名群体性异常开户

【案情概况】

2017 年 11 月 3 日，约 400 名个人客户分批结伴到光大银行广州分行辖属佛山、江门、中山、东莞、湛江分行网点柜台要求开立银行卡。经询问，客户均自称是“深圳全返通电子商务有限公司”会员，接到公司通过微信发布的通知，称公司已成功与光大银行签订批量支付协议，要求会员办理光大银行银行卡，并绑定银行卡用于返现。同一时段出现人数众多的群体性开户情况令人生疑。

【处置措施】

银行网点立即上报，与总行联系核实，证明该公司未与光大

银行签订任何支付协议。经查询，“深圳全返通电子商务有限公司”已被工商部门列入经营异常名录。银行迅速采取措施应对，要求各网点对客户进行风险提示，做好解释和疏导工作，严格按照261号文要求拒绝为此类客户开立银行卡，并将情况及时向当地人民银行和公安部门报告。

（三）堵截冒名开户、伪造证件开户案例

银行办理单位、个人账户开户时，应对开户申请人身份证件的有效性、开户申请人与身份证件的一致性和开户申请人开户意愿真实性进行核实，发现异常情况，应拒绝开户。

案例7：堵截冒用他人证件注册营业执照虚假开立单位账户

【案情概况】

2017年3月28日，张某携带本人身份证、营业执照、法人身份证原件到中国银行安徽省芜湖市分行营业部申请开立单位账户，银行人员按照客户提供的电话联系法人核实开户意愿，电话接听人无法准确回答身份证信息，借口信号不好挂断电话，再次拨打电话后，接听人却能够准确流利地说出所有身份证件信息，该变化情况令人生疑。

【处置措施】

银行人员通过中国银行核心系统查询法人身份证号码，发现系统内存有该法人个人客户信息。银行人员拨打系统留存电话后获悉，该客户并未成立公司，身份证件四年前曾遗失。银行当即报警，将张某身份证等资料移交给民警，民警随后带走张某让其协助调查。

【案例启示】

案例说明，虚假开户风险形式更加多样和隐蔽，银行不应满足于账户资料表面合规，还要结合日常工作经验，通过与客户交流核实、利用合法外部渠道交叉验证等方式深入核实信息。

案例 8：堵截持伪造身份证冒名开立个人账户

【案情概况】

2017 年 7 月 12 日，一男子持异地身份证至建设银行广西分行网点要求开户，银行人员在智慧柜员机为其办理开户时，发现该身份证没有磁性，遂引导至柜面开户。银行人员拿到客户身份证后仔细辨别本人和证件图像，确认脸型有八九分相似后，置于二代身份证鉴别仪上读取证件信息，但发现该证件已消磁。

【处置措施】

银行查询该身份证复印件历史影像时发现，该证件客户照片与银行留存的身份证历史影像中头像不一致，其它身份证信息相同。该男子否认去过公安局更换身份证，银行人员意识到该身份证可能是伪造证件，遂请该男子出示其它辅助证件，但其拒绝出具辅助证件并强烈要求退回该身份证，向银行人员索要不成后，该男子迅速离开银行网点。

【案例启示】

银行要持续做好风险审核工作，做到多观察、多询问和多提示，便于第一时间发现可能存在的风险点，通过加强源头封堵，防范电信网络诈骗犯罪。

（四）利用系统“黑名单”堵截开户案例

银行应当逐步建立“黑名单”系统，在本地、全国范围内共享各网点的风险信息。人民银行分支机构可以因地制宜在辖区内

组建异常开户“黑名单”系统，探索银行间共享风险防控信息。

案例 9：通过非法账户业务预警系统发现台籍诈骗人员

【案情概况】

2016 年 12 月 12 日，一男子带领两名台籍人士前来兴业银行厦门分行开立银行卡，银行人员与客户核对信息时，该名男子一直在旁代答，称开立银行卡主要用于结算工程款，并需要开通手机银行，此异常行为引起银行人员注意。

【处置措施】

银行人员登录“厦门市银行支付结算之家”非法账户业务预警系统查询发现，华夏银行、农业银行已拒绝为其中一名台籍客户吴某开户，原因为吴某疑似使用虚假信息办理开户，与可疑情况描述基本相同。另一名台籍客户苏某与吴某填写的是同一常住地址。银行报警后，警方到现场将台籍吴某等三人带走。

案例 10：通过电信诈骗风险交易事件管理平台发现诈骗人员

【案情概况】

2017 年 7 月，海南银行三亚分行报告，一名客户持身份证至辖区内网点申请挂失补办银行卡。

【处置措施】

银行人员通过电信诈骗风险交易事件管理平台查询时发现，该客户曾于当年 5 月被贵阳市公安局实施冻结账户处理，据此推断该客户可能涉嫌电信网络诈骗。银行一方面稳住客户，另一方面立即报警。民警将该客户带回调查，从其身上搜出多张可疑银行卡。

（五）堵截企图利用账户分类进行异常交易案例

个人账户分类管理政策的实施，对打击非法买卖银行账户发挥了重要作用，切实保护了个人资金安全。但诈骗分子犯罪手法不断翻新，利用账户分类规避监管就是其中之一，银行应密切关注电信网络诈骗的新形式，加强风险识别能力。

案例 11：堵截利用Ⅰ、Ⅱ类户升降级异常开户

【案情概况】

2017 年 3 月 14 日，林某来到民生银行闽江支行要求办理配有实体卡片的Ⅱ类户。经查询，林某已有民生银行Ⅰ类户，银行人员通过自助机具为其办理了Ⅱ类户，并配发实体卡片。随后，林某来到柜台，称其Ⅰ类户的银行卡已丢失，需办理无卡销卡，并将刚办理的Ⅱ类户升级为Ⅰ类户。林某对Ⅰ、Ⅱ类户升降级功能以及银行业务流程十分熟悉，引起银行人员的注意。

【处置措施】

经查询，林某办理的Ⅰ类户自 2016 年 12 月 23 日起频繁发生境外交易，且大部分交易与近期监管发布的出租、出借个人账户为地下钱庄中转套现的可疑特征相似。但林某称从未出境，同时不断翻看手机并接听电话。银行人员听到通话人指导林某，若银行不给无卡销卡，就称卡已丢失，过两天去异地要用，要求补一张马上能拿到的新卡。接完电话，林某改口称要办理挂失补卡，并要求立即拿卡。银行人员向林某解释，虽然其声称未出境，但交易记录却均为境外交易，向其提示了出借银行账户风险及惩戒措施。听到这些解释后，林某最终选择办理挂失补发原卡。

【案例启示】

诈骗分子投机于II类户开户数量不受限，采用频繁注销Ⅰ类户、升级II类户为Ⅰ类户等方式继续实施不法行为。银行应严格遵照制度、流程规范业务操作，做好客户风险提示。

二、堵截诈骗资金转移案例

（一）封堵电信诈骗转账案例

受害人遭遇电信诈骗被要求汇款时，其异常行为存在共性特征。银行应增强客户异常行为识别意识，及时向异常客户进行转账风险提示，普及电信网络诈骗常见的手段，谨防各类诈骗。

案例 12：七旬老人陷“民族大业”骗局 银行及时劝阻助止损

【案情概况】

2016年12月，一老人来到农业银行贵州省白云支行营业部，拟向一外地账户汇款100余万元。银行人员询问汇款意图时，老人称自己所有收支往来均是在国家财政部指导下进行，共有资产3000多亿元，并要向银行出示中央为其颁发的“聘书”。此语一出立即引起银行人员注意，怀疑老人卷入电信诈骗骗局。

【处置措施】

银行人员立即与老人沟通，并进行风险提示。老人自称从事“民族大业”工作，是贵州省“新基金会”副会长，前期已通过其他银行向该外地收款账户累计汇入500余万元。银行意识到老人涉嫌遭遇类似“民族资金解冻返还善款”的电信网络诈骗，随即报警，同时迅速协助老人换卡，修改卡密码，取消网银，再次对其进行风险提示，并对老人的账户实施重点监测，防范后续资金再次被转移。经警方立案侦查，诈骗分子以“解冻103库国家

财产”为借口，发展所谓“民族大业”有功人员6万余人，以收取“会员费”为名义骗取资金655万元。该案目前已被侦破，相关涉案人员已批捕。

【案例启示】

银行要向异常开立银行卡客户普及电信网络诈骗常见手段，提醒客户注重银行卡信息安全，不要轻信他人作出的大额返现或大额补偿等承诺，谨防“民族大业”类电信网络诈骗。

案例 13：劝阻客户参与非法集资 避免资金损失

【案情概况】

2017 年 3 月 21 日，七旬老人张某在一中年男子陪同下至恒丰银行青岛即墨支行开立银行卡，并要求存入现金 3 万元。银行人员发现开立银行卡目的等问题皆由陪同男子代答，但询问张某该男子身份时，张某却支支吾吾，该男子则替其回答说他们是亲戚。期间两人一直交谈，且有意回避银行人员，银行人员偶尔听到“收益高”、“保本”、“项目”等词，遂怀疑张某遭遇了非法集资诈骗。

【处置措施】

银行人员立即对张某进行风险提示，并提醒其购买非正规途径理财有可能存在诈骗风险，但张某坚决不听劝阻。银行人员以老人年纪较大，业务办理需要与其子女核实为由，获得了张某子女的电话并取得联系。张某儿子赶至银行，劝阻张某不要轻信陌生人介绍的理财产品，切勿购买。此时张某才恍然大悟，陪同张某的男子早已没有踪影。

【案例启示】

高收益理财类诈骗的受害人多为中老年人，开户时可能由陌生人员陪同。银行应提高对此类诈骗行为的敏感性，采取适当方式，了解客户真实意愿，谨慎办理开户业务。

案例 14：施计延缓汇款 保全客户资金

【案情概况】

2016 年 8 月 29 日，一老人至浙商银行天津和平支行要求汇款 3 万元给亲戚，汇款信息笔迹潦草的写在一张纸条上。银行人员一再向其确认是否认识收款人、明确了解汇款用途以及家人是否知晓，老人坚称收款人为亲戚，汇款用途却含糊其辞，但其坚持汇款。银行人员协助老人通过 ATM 转账输入收款人姓名时，老人说一直称其“小周”，不知道具体姓名，于是银行人员便要求老人与“小周”取得联系。在接通对方电话后，一南方口音的男子声称自己为周某，此时银行人员判断老人可能陷入电信诈骗。

【处置措施】

为延缓汇款，银行人员故意将周某名字输错为同音字，请老人确认，老人称就是这个名字，并坚持汇款。因未找到老人提供的对方工行开户行，老人再次与周某通话，通话时周某语气显得很焦急，让老人回复银行人员无论工行哪个开户行都行，抓紧汇款。银行人员选择了工行不对外办理业务的某省分行，并再次提示老人汇款风险，老人却依然要求汇款。汇款完成离开银行十分钟后，老人边与周某打电话边返回银行，称周某要与银行人员通话。银行人员接听电话后，周某质问银行人员为何资金还未到账，银行人员则请其咨询接收行。当日下午，民警带领老人重回网点，

称老人被人电信诈骗，而此时 3 万元汇款因账号与户名不符，已退回至老人账户。

【案例启示】

该案例中，银行人员主要发现以下疑点：客户为老年人且神色紧张；对收款人姓名及汇款用途含糊其辞，不愿正面回答；汇款期间与收款人长时间通话，明显由对方指导操作。这些疑点也是电信诈骗的显著特点，银行也据此提高了警惕，从而采取了有效措施保全客户资金。

（二）追回 ATM 转账诈骗资金案例

银行可视情况利用 ATM 延时到账功能，延缓疑似遭受电信网络诈骗客户的资金到账时间。对于客户提出的撤销转账申请，银行应迅速处理，最大限度挽回客户损失。

案例 15：协助客户撤销 ATM 转账

【案情概况】

2016 年 12 月 1 日，一位客户神色紧张的来到工商银行张家界永定支行，称刚接到一个未知电话，误以为是自己朋友，就直接按对方提供的账号，在 ATM 上跨行转账 28000 元。转完账后，客户越想越不对劲，怀疑自己被电信诈骗，遂急忙到银行寻求帮助。

【处置措施】

银行人员了解事情经过后，首先是安抚客户情绪，并告知客户，当日是人民银行账户分类新规实行的第一天，凡是在 ATM 进行非同名转账都是 24 小时后到账。在客户情绪缓解后，银行人员指导客户办理了转账撤销业务。整个事件处理时间不超过十分钟，客户资金全额退回。

案例 16：利用 ATM 延时到账 保护客户资金安全

【案情概况】

2016 年 12 月 1 日，高龄客户黄某至中国邮政储蓄银行来宾市中南路北支行申请开立银行卡。在填单过程中，黄某接到一个电话并告知对方自己已经在银行开立银行卡，全程都改用普通话交流，银行人员对此举动产生怀疑。

【处置措施】

银行人员与黄某不断交流，了解到开立银行卡是为了购买药材，当问及对方信息及电话号码来源时，黄某沉默不语。银行人员对黄某进行风险提示，并再三劝阻，但其执意开户。鉴于黄某已有 77 岁高龄，情绪也较为激动，贸然拒绝开户，可能会引发黄某身体不适，银行人员遂为其办理了开户业务。同时，考虑到黄某被骗几率极大，银行人员利用 ATM 延时到账功能，引导其到 ATM 转账 600 元，以争取缓冲时间，防止老人被骗。次日，黄某急匆匆进入网点，称已意识到自己被骗，咨询取消转账事宜。银行人员引导黄某在柜台办理了 ATM 转账撤销交易，及时保护客户资金安全。

（三）积极联系收款机构追回资金案例

部分受害人资金被诈骗分子辗转存入基金账户，用于申购基金。银行如遇类似情况，应指导受害人妥善保管交易验证信息，协助受害人协调收款机构，撤销相关交易，赎回被骗资金。

案例 17：帮助客户撤单 确保资金安全退回

【案情概况】

2017 年 5 月 6 日，张某到浦发银行紫荆山支行，称收到小

红书网站电话，有款项需退回，并给张某发送一条链接，要求其按链接步骤进行操作。但张某打开链接后，银行卡里的27677元被分两笔转走，同时其手机还收到两条含有校验码的短信。商家随即给张某打电话索要短信校验码，客户才觉得有异常，意识到遭遇了电信诈骗，请求银行协助追回资金。

【处置措施】

经查询，由于张某的银行卡开通了快捷支付功能，两笔款项均已从活期账户完成扣款，交易明细显示为银基通基金申购。银行人员一方面致电基金公司客服，请基金公司协助撤销或锁定此两笔交易；另一方面，同步在核心系统和手机银行客户端尝试撤单。经过不懈努力，张某的手机银行中成功撤单，两笔款项同步返还至其银行卡中。

【案例启示】

案例中，客户点击网页链接致使银行卡资金被划转至基金交易平台，幸而未向犯罪分子提供银行验证码，使资金暂时停留在申购阶段，为资金追回争取了时间。银行应尽最大可能，协助客户追回资金，保护客户资金安全。

案例18：协助给出解决方案 追回被骗资金

【案情概况】

2017年3月19日，王某到兴业银行宁德财贸广场支行，称其网购退货后应接收退款300元，当日凌晨接到冒充商家的诈骗分子电话，说退款需分期退回，要指导王某办理分期退款业务，实质上是诱骗王某在支付宝办理提供小额贷款的“来分期”业务。业务办理成功后，王某支付宝余额增加了4000元。诈骗分子谎

称增额为王某操作失误导致，要求王某点击诈骗分子发来的链接退回增额，否则需每天支付120元分期费用。王某信以为真，并按诈骗分子要求点击链接，其信用卡和理财卡中共计26700元随即被转走。王某急忙报案并寻求银行帮助。

【处置措施】

银行人员立即协助王某口头挂失银行卡，并查询到资金已转入华夏基金账户，诈骗分子以王某名义购买了华夏基金货币型基金。此时诈骗分子多次联系王某索要短信验证码，银行人员亲自实际购买华夏基金，发现基金申购、赎回、信息修改都需要验证码校验身份，遂怀疑诈骗分子为获取赃款企图将该基金赎回至自己账户或修改至自己名下。银行通过咨询基金公司得知，即使王某银行卡解挂，只要不提供短信验证码，基金账户资金也无风险。于是，银行人员指导王某不要向诈骗分子提供短信验证码，同时对银行卡解除挂失。在得到指导后，王某登入基金账户，申请了密码修改，并将基金赎回转至自己银行账户。次日，王某26700元资金安全到账。

【案例启示】

银行应强化支付结算知识宣传工作，警示各类支付风险，指导客户谨慎保管银行卡及相关验证信息，正确、安全使用各类支付结算工具。

（四）及时止付冻结账户、追回被诈骗资金案例

受害人资金遭受损失后24小时，是追赃的黄金时间。银行应保持电信网络诈骗敏感性，客户提出转账疑惑后，要及时予以核实，指导受害人报警，并按规定开展查询、止付、冻结等操作。

案例 19：轻信网购退款受骗　银行协助追回资金

【案情概况】

2017 年 7 月 14 日，民生银行某支行接到客户钟某咨询电话，钟某称昨日接到自称淘宝客服的电话，该客服对其近日所购商品信息及个人信息描述无误，称商品存在质量问题拟全额退款，需在其提供的支付宝网页链接中先行付款，商家后续赔付退款。钟某点击链接支付货款 119 元后，客服请钟某提供用于退款的银行卡卡号和退款验证码。钟某提供以后，却发现收到的提示短信显示转出资金 49999 元。对此，钟某提出了异议，该客服则表示是后台操作失误，再次提供验证码后资金将马上冲正。钟某提供验证码后，又收到转出资金 50000 元的短信提示，该客服表示是对操作失误资金进行冲正，须再次提供验证码。钟某提供验证码后又被转出资金 3482 元。此时客户卡上资金仅剩 0.31 元。电话挂断后，钟某感觉此事有些蹊跷，便致电民生银行。

【处置措施】

银行迅速采取如下措施：一是因该客户账上还有一笔定期存款，马上指导客户电话进行挂失。二是同步查询资金去向，通过银行核心业务系统查询该笔资金转入的户名。三是协助客户报警，将被诈骗金额及资金去向清楚告知后，警方对涉案账号进行快速查询、止付，24 小时内钟某被诈骗资金 103482 元全部退回原卡。

【案例启示】

该案例中，诈骗分子通过非法渠道获取受害人网购信息，借此实施诈骗，受害人极易上当。银行应加强对客户防范新型电信

网络诈骗的宣传教育，强化“不轻信来历不明的电话和手机短信”意识。当客户遇到诈骗时，银行应主动施策，全力协助客户追讨被诈骗资金。

案例 20：及时发现并止付诈骗分子账户

【案情概况】

2017 年 8 月 8 日，客户吴某在招商银行海秀支行要求办理挂失补卡业务。在办理业务过程中，吴某神色慌张，不停催促银行人员，这引起了银行人员的警觉。经查询，吴某账户涉嫌电信诈骗被公安机关实施紧急止付 48 小时，8 月 7 日止付失效，8 月 8 日处于预警状态。

【处置措施】

银行一边安抚吴某情绪，一边拨打南京市公安局反通讯网络诈骗侦查大队值班电话，告知警方吴某账户近期有一笔 10 万余元的进账，并将汇入卡号及卡主姓名提供给警方。警方及时与卡主苏某取得联系，被告知吴某是通过非法渠道窃取了苏某出行及身份信息，并冒充航空公司客服人员告知苏某航班晚点，以赔付延误费为由窃取苏某银行账户信息实施了诈骗。于是，警方再次对吴某账户实施控制措施，银行则立即拒绝了吴某挂失补卡要求。

【案例启示】

银行应密切关注客户办理业务时的情绪和意向，要多留心、多关注、多提醒。做到一看，看客户的精神状态；二听，听客户的话；三了解，了解客户的办理业务实际目的。

三、强化可疑交易监测案例

银行和支付机构应加强可疑账户交易监测工作，对列入可疑交易的账户应当进行核实，经核实后仍然认定账户可疑的，应当按规定暂停相关业务，并报送可疑交易报告。

（一）加强银行账户资金交易监测案例

案例 21：监测发现台籍人员集中开立银行卡异常情况

【案情概况】

2016 年 12 月初，中信银行无锡分行监测发现，有一批台籍人员集中开立银行卡并开通网银，这批台籍人员入境时间基本是 2016 年 11 月底且证件签发地均为广东，银行卡留存的手机号码均为泰州地区手机号，该批台籍人员账户交易存在异常情况，涉嫌电信诈骗。

【处置措施】

银行立即向人民银行南京分行和当地公安部门报告。经查，南京、常州等地也发现类似情况。2016 年 12 月 16 日，人民银行南京分行对此进行了通报。银行立即采取应对措施，于 12 月 16 日晚将涉及异常资金交易的 4 名台籍个人银行结算账户暂停账户非柜面业务，要求各网点办理台湾居民持“台湾居民来往大陆通行证”开户、开通网银等业务时强化审核，发现异常情况应拒绝开户；对 10 月 1 日后，客户使用“台湾居民来往大陆通行证”已开立 1000 多个个人银行结算账户的开户、资金交易情况进行排查，发现部分账户同时存在不同主体账户开户资料关联密切、账户资金快进快出、账户无余额或余额相对于交易额比例较低、不填写个人信息或开户资料信息虚假、账户交易多为非柜面交易方式等电信网络诈骗犯罪可疑特征，也符合通报提及的通行

证为近期新办、登记地址多为酒店或虚假地址的情况。银行已对排查发现的412户可疑账户进行暂停账户非柜面业务处理。

案例22：监测发现个人账户非柜面异常交易

【案情概况】

广发银行客户苏某，于2016年10月21日开立借记卡，并同时开通网银、手机银行且申领了KEY盾。2017年4月银行对该账户进行电话回访，预留联系电话归属地为异地且手机处于关机状态。

【处置措施】

银行立即对该账户进行重点监测排查，发现开户后该账户一直未使用，于2017年3月6日由他行同名账户试探性转入100元后突然启用，并发生大量交易，交易渠道均为非柜面交易。查看客户交易流水，3月6日至4月17日，账户交易量已达427笔，资金来源多为李某、各银行清算中心、某支付机构客户备付金等。资金去向均为个人，收款账户达55个，转出资金基本为100元的倍数且不固定。发现上述情况后，银行于4月19日对该账户实施了暂停非柜面业务的处理。

案例23：监测发现菲律宾籍人员账户异常交易

【案情概况】

2017年4月，渤海银行广州分行通过账户监测发现，3名菲律宾籍个人账户开户后无交易，约3个月后启用，并迅速在3个月内累计发生数千笔交易，交易极为频繁、总额较大，资金当日分散转入，相对集中转出，账户少有沉淀资金。3人账户交易对手固定，均为他行开户的若干个人。银行通过查询柜面异常开户

监控台账发现，此3人同日开立银行卡，并开通电子银行。2人开户留存地址一致，1人留存地址近似。根据其账户交易规律，银行高度怀疑3名非居民个人账户可能从事电信诈骗洗钱交易。银行人员拨打客户预留手机进行回访时，发现上述3人的手机已处于停机状态。

【处置措施】

银行对3人账户增加账户关注信息，进行非柜面交易功能限制，作为重点可疑交易上报人民银行。后续，银行又发现1名菲律宾籍个人存在类似情况，除了参照上述方式进行处置外，银行还对2015年以来菲律宾籍客户的开户和交易情况进行了全面排查。

（二）加强支付账户资金交易监测案例

案例24：监测发现网络兼职招聘类电信网络诈骗

【案情简介】

支付宝接到客户举报，经调查后发现一个网络兼职招聘类电信诈骗团伙，该团伙人员分工明确，分别负责财务、外宣、客服、培训、注册等。其作案手法是在赶集网、58同城、论坛以及聊天平台上发布虚假工作岗位，诱导受害人注册IS语音聊天账号，要求受害人通过银行卡、支付宝账户转账等方式交纳99至499元不等的押金，之后以工种不同、收入不同让受害人再次以前述支付方式缴纳99至499元不等的工种费用等。当客服环节诈骗完成后，客服将受害人推送给培训人员，再以交纳培训资料费为由让受害人缴纳38至88元不等的培训费用。此后，培训人员再将受害人推送给注册人员等进一步实施诈骗，诈骗完成后将被害

人删除拉黑。

【处置措施】

2017 年 5 月至 9 月初，支付宝风险行动中心配合各地公安部门对涉案人员组织分工、人员身份等进行排查，协助侦办“328 网络兼职招聘打字员专案”，截至 6 月份，警方共抓获涉案犯罪集团成员 800 余人，刑拘 600 余人，起诉 485 人，涉案金额 4000 多万元。同时，支付宝对涉案账户采取账户限权、资金冻结等一系列措施。

【案例启示】

支付机构要提醒客户提高自身安全意识，针对缴纳押金、培训费等费用的兼职提高警惕，不轻信诈骗分子投资回报高、从业门槛低、工作时间短、快速致富等谎言。

案例 25：监测发现“做法消灾”类电信网络诈骗

【案情简介】

财付通接到客户投诉，通过挖掘账户昵称、设备关系、资金流水等信息和回访部分客户，发现广东湛江地区存在从事“做法消灾”类网络诈骗的犯罪团伙，涉及近百个微信账户。诈骗团伙有组织的通过百度贴吧、百度知道、微博等渠道宣传情蛊法术，将受害者引流到微信平台。团伙人员微信账户昵称大多以某某法师、先师命名，且一人可能扮演多个角色，自称是“情蛊门”、“黄老堂”和“羋情门”等的仙师，有可消灾解难、扭转运势的独门法术等，利用开展法事先行收费、贩卖虚假开光转运圣物等方式诱骗受害人进行微信转账。通过分析诈骗账号资金流水情况，财付通确认该类诈骗交易 7000 余笔，涉案诈骗资金超过千

万，涉及的受骗用户超过2000名，分散在全国各地，且大多为中老年人。

【处置措施】

财付通对近百个涉案诈骗账号及作案人信息进行限制，立即公布“做法消灾”诈骗识别策略，并实时拦截高度疑似诈骗交易，及时作出风险提示。2017年7月，财付报送线索数据并配合公安部门开展排查。9月初，警方已在湛江、广州打掉4个“做法消灾”犯罪团伙，抓获犯罪嫌疑人110余人，冻结涉案金额超过1000万元，初步统计涉案金额超过4000万元，受害人超过5000人。

【案例启示】

支付机构要加强对新型电信网络诈骗识别和打击，通过日常用户投诉与支付机构自身交易风险识别模型，及时识别风险，对可疑账户及时处理，减少客户损失。同时，通过APP、公众号、官网、短信等各渠道加强典型电信网络诈骗案例宣传，提高客户甄别能力。

报送：范一飞副行长。

发送：人民银行上海总部金融服务一部，各分行、营业管理部、省会（首府）城市中心支行、深圳市中心支行支付结算处，大连、青岛、宁波、厦门市中心支行会计财务处。

抄送：条法司、科技司、反洗钱局；国务院打击治理电信网络新型违法犯罪工作部际联席会议办公室、中国银联、中国支付清算协会。