2024年9月23日 星期一 责编:哈欣 美编:孟宪东 TIANJINDAILY 天津日报

骗子转账分分钟 反诈响应毫秒级

——银行业守好反电信网络诈骗“第一道防线”

■本报记者 岳付玉

在银行后台,看到一张张电信网络诈骗涉案账户交易明细截图,心理素质再好的人都会忍不住倒吸一口凉气:骗子在账户收到被骗人转来的钱之后,分分钟就跨行转到几个二级账户,再从二级账户转N个三级账户……这期间如果不及时拦截,这笔钱很快就会转到境外被取现,就像饿狼分食羔羊一样,转眼间吞食殆尽。

犯罪分子转移诈骗资金最核心的介质是银行账户。因此,聚焦账户的攻防之战分秒必争,其紧张曲折有时超过影视剧情。多家金融机构发布新近发生的、来自银行一线的反电信网络诈骗案例,可以感受到当下网络诈骗之猖狂、骗术之“新奇”,也以此提醒广大市民提高警惕,切实保护好“钱袋子”。

9月是“金融教育宣传月”。日前,天津金融监管局联合人行天津市分行、天津证监局、市地方金融管理局共同启动了宣传月活动。多家金融机构向市民强化提示提醒,普及防范非法金融活动、电信网络诈骗和理性投资知识,提升市民风险识别能力,力争“防患于未然”。

案例1

孟大爷:骗子催我30分钟内转账,幸亏被拦住了

日前,在天津农商银行西青赛达园区支行,年近70的孟大爷急匆匆赶来办理转账业务,要把自己银行账户中的3万元转入一张开户在陕西省渭南市的银行卡中。

银行柜员袁祥益询问孟大爷汇款用途,以及是否认识收款方。孟大爷说自己是参加义务捐款活动,钱转过去之后,对方还会返还,并且会给挺高的利息。这个解释立即引起了袁祥益的警惕。

他提出能否看看孟大爷手机上的聊天记录。老人答应了。小袁这一看心里就有了数。他自然不能帮孟大爷办转账,而是叫来大堂经理稳住老人、劝阻他转账,同时拨打了报警电话,警察很快到场,在银行工作人员和警察的共同讲解下,孟大爷慢慢明白过味儿来,他的钱保住了!醒悟过来的他再给骗子发信息,对方知道骗术被识破,“蒸发”了。

■案例分析:

就孟大爷与骗子聊天的截图,天津农商银行相关人士分析其中的疑点:

1. 通过手机与客服沟通进行转账存款:这是电信网络诈骗的常见手段之一,诈骗分子通常会冒充银行客服,通过电话或即时通讯软件诱导受害者进行转账,而正规的银行业务通常不会通过这种方式进行。

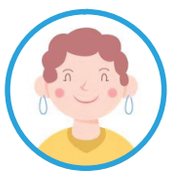
2. 转账要求在30分钟内完成:诈骗分子为了增加紧迫感,常常会设置一个不合理的转账时限,迫使受害者在没有充分思考的情况下匆忙转账。

3. 客服要求汇款完成后以截图作为存款凭证:正规的银行业务不会要求客户提供转账截图作为凭证,这是一个明显的诈骗特点。

近期,在邮储银行天津市红桥区佳安里支行也发生了类似情景。今年5月6日,客户王大爷到该网点来办理汇款。理财经理张珂鑫询问得知,王大爷要往户名为四川绵竹杜甫酒业销售有限公司的对公账号汇款2万元,用于购买12瓶杜甫典藏酒,老人解释说实则是为了购买该公司股权——该公司工作人员称这个酒的股票年底即将上市,现阶段可以用非正规渠道为王大爷购买内部私募的8000股股权,但款项用途只能写购买12瓶酒,因为涉及公司上市保密工作。对方还反复强调让王大爷只跟银行工作人员说买酒,不要透露其他信息,打款有时限,错过了股权就被抢光了……张珂鑫拨打了报警电话。经北辰网警甄判,这是一起电信网络诈骗无疑。

案例2

李女士:被拉进财务“工作群”,“领导”让我转账



今年6月下旬的一天,一阵电话铃声在中国银行天津市西青区高新支行对公柜台响起。

“您好,请问是中国银行高新支行对公柜台吗?我好像遭遇了电信诈骗,转出去了96.5万元,麻烦您帮帮我!”电话那头传来某企业财务人员李女士焦急的声音。

“您先别着急,您身边还有其他同事吗,让他马上报警,您把汇款信息叙述给我,我帮您查一下。”当班柜员王翠宁了解到情况紧急,第一时间在核心系统查询汇款情况,并将电话转交给经验丰富的董宝旭经理。

“收款人的开户行是兰州一家银行的支行!”董宝旭在获知该信息后,第一时间同那家银行网点取得联系,询问该笔资金是否到账,并协同属地派出所等单位,限制收款人账户非柜面业务,对相关涉案账户申请紧急止付。

“李女士,别担心,我们已经同收款银行取得联系,您的被骗资金已被成功拦截!”董宝旭长长地舒了一口气。

据李女士介绍,当天,她和单位一位“同事”被拉进了一个“工作群”,看着群内熟悉的头像及昵称,李女士便放松了警惕,开始在群内互动聊天。“领导”先是试探性地询问李女士回款情况及账户余额,见李女士“上钩”便安排她紧急支付一笔大额货款96.5万元。李女士完成转款后,“领导”仍要她继续汇款。这个行为一下引起了她的警觉,她立刻致电中国银行天津高新支行请求帮助。

好在通过异地警银联动,中国银行天津市西青区高新支行以最快的速度将涉案资金全额止付在涉案账户内,为受害人挽回了这笔大额资金。

“我写这封信是要向董宝旭、王翠宁两位工作人员表达我对您和您的团队的无尽感激和赞许。”7月1日,李女士和单位领导专程前往中国银行西青高新支行网点,送上一封手写的感谢信及一面锦旗。

■案例分析:

银行业内相关人士介绍,此类诈骗大概有这么“三部曲”:一、突如其来的好友请求。诈骗分子会突然通过QQ、微信等社交平台添加财务人员为好友,并备注为领导姓名;二、伪造的身份信息。诈骗分子会使用伪造的领导照片、名片或聊天记录,以增强其身份的可信度;三、紧急且模糊的转账要求。一旦建立联系,诈骗分子会迅速以“紧急业务处理”“项目合作”等为由,要求财务人员立即转账至指定账户,且往往不提供详细的转账说明或合同文件。

案例3

朱女士:说我开通了带货功能,不关闭会扣钱

7月16日,兴业银行天津市南开区支行上演了一场“火线救援”,保住了朱女士的350万元养老钱。

当天下午5点21分,该营业厅主任接到客户朱女士的求助电话,称自己一个人在家,遇到一些紧急事件需要转账至指定账户,并已提前支取定期存款400万元到活期账户,但在转出一笔50万元后手机网银无法继续使用,希望银行将剩余资金尽快全部转出。

“通过电话描述,我们初步判断该客户突然支取定期并大额转账交易存在异常可疑,联想到我行一直以来对电信网络诈骗的培训知识,我们判断这是一起典型的针对老年人的网络诈骗,于是迅速与客户取得联系。”营业厅主任告诉记者。

南开支行了解到朱女士是接到某电商平台客服的电话,声称她开通了带货功能,如不关闭会一直扣钱,关闭该功能需要核验客户绑定账户,将绑定账户的资金转到客服提供的“核验账户号”,核验后再转回才能关闭该功能。

支行工作人员立即阻止朱女士继续转账,并第一时间协助拨打110报警。在银行员工和办案民警的一再劝说下,朱女士最终放弃继续转账,成功保住了350万元。截至目前,办案民警仍在为她全力追讨已被骗的50万元资金。

■案例分析:

兴业银行天津分行相关负责人表示:“犯罪分子利用老年人社会交往简单、信息闭塞的弱点,采用小额回款、QQ视频、远程操作等手段令他们一步步陷入网络诈骗的圈套。”

无独有偶,近日,一位女士来到招商银行天津新技术产业园区支行,要求提前支取未到期的定期存款10万元。在交流过程中,支行大堂主管吴征细心询问,这位女士说这笔钱是用来支付孙女学费的,但当核实收款信息时却发现,收款人并非其孙女本人。吴征当即提高了警惕。进一步沟通后,该女士告知她“孙女”一直在通过QQ全程指导她操作。吴征意识到可能存在电信网络诈骗风险,立即建议客户电话联系其孙女确认情况。这位女士表示QQ上的“孙女”告诉她手机损坏无法进行电话联系,但在吴征坚持劝说下,她将信将疑拨了她孙女的电话号码。电话通了!其孙女一头雾水说根本没要学费……

案例4

某商户:骗子注册相似邮箱,险被骗38万美元

72小时,38万美元!今年3月,兴业银行天津分行通过警银密切配合、总分行协同联动,与天津市公安局反诈中心成功堵截一起大额跨境涉诈资金汇出,将被骗资金全款追回。

2月28日,某商户(简称A公司)通过兴业银行天津分行向境外合作伙伴汇款38万美元。在确认收款信息无误后,天津分行给其办理了购汇、付汇手续。3月5日,A公司财务人员突然向兴业银行天津分行的客户经理反馈,说他们的“境外合作伙伴”声称收款信息有误、国外不能入账,请银行赶紧止付并把资金重新汇到该“境外合作伙伴”提供的另一个账户里。兴业银行天津分行照办了。

3月6日,A公司财务人员急匆匆向兴业银行塘沽支行反馈,说国外那个收款方好像注册了跟他们真正的境外合作伙伴同名的公司和相似邮箱,可能涉嫌欺诈!他们已向公安机关报案。兴业银行天津分行紧急行动起来,加急委托总行向国外发送止付申请报文,还提示A公司通过其美国的中介公司在境外办理相关保全措施并向美国反诈机构报案。

与此同时,天津市公安局反诈中心也第一时间组建警务协同任务群,指令滨海新区公安局派警处置。当晚22:20分,兴业银行天津分行组建警银专项处置中心,安排专人实时跟进。经核查,A公司的钱款仍在汇入银行账户,尚未实际入账。但因时差问题汇入银行处于非业务办理状态,暂无法进一步开展止付工作。

兴业银行天津分行警银专项处置中心工作人员紧盯账户进展,3月7日上午7点左右,核实被骗资金已被汇入银行截留,资金安全得到保障!3月8日下午16:05分左右,被骗资金从中间行(花旗纽约)经兴业银行总行全额返还至A公司账户。

■案例分析:

兴业银行天津分行方面介绍,此次涉案交易呈现新特征:骗子通过注册同名公司、相似邮箱等方式,利用跨境信息差采用科技手段拦截混淆账户信息,进而实施诈骗,这也体现出未来反诈工作事中监测及阻断的重要性。

新骗局提示

五大诈骗类型高发 企业受骗案件上升

银行业内相关人士介绍,目前电信网络诈骗呈现新特点:

五种诈骗类型高发,分别是刷单返利、虚假网络投资理财、冒充电商物流客服、虚假征信、虚假网络贷款。

据介绍,网络诈骗的诈骗窝点主要在境外,集中在缅甸北部、柬埔寨、菲律宾、阿联酋等国家和区域。针对网络诈骗的攻防对抗持续升级加剧,涉及对外贸易资金对冲、大额取现、跨境取现、购买黄金等。此外,网络诈骗还呈现出国际化趋势和高科技特征,体现在诈骗对象国际化、诈骗团伙成员国际化,以及诈骗分子利用数字人民币、虚拟货币转移涉诈资金等。

除了个人被骗,企业遭受电信网络诈骗的案件数量也呈上升趋势。前不久,就有诈骗分子利用AI换脸冒充某公司老总,成功骗得公司财务人员打款。天津农商银行相关人士告诉记者,部分企业内部财务管理不严,未严格执行财务管理制度中关于网银U盾分权限管理的规定,导致一人持有全部U盾的高风险情形频发。这为不法分子提供了可乘之机,他们通过技术手段如植入木马、病毒等,非法获取财务人员敏感信息,进而利用这些信息实施精准诈骗,诱导财务人员将企业资金转至犯罪分子控制的对公账户,造成了重大经济损失。

行业在行动

共同织就“天罗地网” 快速网住诈骗分子

几家银行提供的涉案账户交易明细显示:骗子的账户进账很频繁,有时半个小时之内能转入五六笔钱,金额从几万元到几十万元不等,可见其“工作”成效之高。这背后,是一个个被骗者的痛与泪。

银行业内相关人士介绍,一个完整的电信诈骗流程为:骗子收集诈骗信息—对受骗人实施诈骗—受骗人向诈骗分子账户(一级账户)转账—诈骗资金转移—赃款洗白。其中受骗人向诈骗分子账户转账、诈骗资金转移为核心环节。

犯罪分子转移诈骗资金最核心的介质是银行账户。因此,银行机构在反诈行动中具有不可替代的重要作用。银行客户的受骗资金进入到犯罪分子掌握的账户,但还没有脱离公安机关和银行能追溯的“资金链”,还有可能挽回损失。因此,银行如何有效通过数据特征、犯罪线索、交易行为,识别到犯罪分子和受害人(账户),是这一环节最核心的工作。

我市多家银行成立专项工作组,定期升级迭代规则模型,建立健全电信网络诈骗处理机制等,结合运用大数据、机器学习、流式计算等关键技术手段,对疑似诈骗信息进行实时监测和拦截,并采取有效措施予以阻断。记者在天津农商银行了解到,今年2月,诈骗分子收到50万元大额被骗资金后,试图使用境外POS转出时触发了该行自主研发的“事中拦截模型”,交易被实时阻断,50万元涉诈资金全部拦截,早于公安管控时间,协助公安将被骗人资金全部返还。4年来,该行的涉诈账户风险监测模型已核查风险交易上千万笔,拦截可疑资金超亿元,协助有关机关为受骗群众返还资金超千万元。

魔高一尺,道高一丈。在与诈骗分子的攻守对抗中,银行的反诈系统要实现实时毫秒级智能监测拦截,并且还要精准、稳健。这其中,多级联动、跨平台合作变得越来越重要。

银行业内相关人士介绍,诈骗分子在一级账户收到骗来的资金之后,通过转入到二级、三级账户完成洗钱,最终将资金取出。公安机关在办案时管控的主要是一级账户,仅占诈骗分子所有账户的10%,其二级、三级账户因为分散在多家银行多个平台,拦截起来难度增大。银行业内相关人士因此呼吁各家机构和平台尽可能实现相关数据信息共享,共同织就“天罗地网”,把诈骗分子快速网住。

记者手记

当走进银行的后台,查阅电信网络诈骗涉案账户的一笔笔交易明细,回看银行监控拍下的一幕幕拦截录像,你会有怎样的感觉?触目惊心,后背发凉,还是暗自庆幸?

想到了电信网络诈骗猖獗,没想到电信网络诈骗如此高频上演。很多银行网点都曾遇到过,每家银行都能提供不止一个拦截案例。

是骗子太狡猾,还是被骗的人太傻?

借助高科技手段,骗子的欺诈“段位”确实越来越高,AI换脸,盗号冒充亲友、老板,种种以假乱真不说,还深谙人性的弱点,利用被骗者的认知盲区、贪心、孤独等,精准出击。

银行反诈大数据显示,被骗子盯上最多的人群,并非信息相对落伍的农村居民,而是都市女性,中老年人居多,其中的女性单身者更是其眼里的“香饽饽”——她们对网购、社交软件并不陌生,自认为防范意识强,其实很容易被攻陷。

“不见面”“不接触”是多数电信网络诈骗案件的显著特征。心理专家王国荣此前接受采访时建议,如果接到各种电话、QQ或微信等联系让汇款,您应该第一时间直接联系上您的亲友、熟人,“直联”的方式可以识破绝大多数的骗术。

近年来,针对花样翻新、层出不穷的诈骗手段,全国公安机关开展“云剑”“断卡”“断流”“拔钉”等专项行动,对相关违法犯罪依法严打、紧抓不放。银行也发挥网点“第一道防线”的作用,在人工核实交易真实有效性的同时,依托物联网大数据等科技手段,提升甄别事前、事中可疑交易的能力,取得一定成效。但骗子依然心存侥幸,且诈骗过程已形成灰黑产业链,因此打击网络诈骗任重道远。

保护好“钱袋子”,每个人都是自己的第一责任人。