□马跃萁

大数据时代，更多不同形式的网络贷款进入了大众的视野，“不附条件”的审查、“当天放贷”的诱惑、“无担保、抵押”的吸引使得众多急需用钱的消费者跃跃欲试，但同时也让各种诈骗分子巧立名目、有机可乘。有的不法分子通过伪造监管文件，对消费者实施诈骗，正如本文的案例中讲述的。

案情简介：银行员工精准识别网贷诈骗

近期，一名女性客户侯某来到某银行某支行，表示自己需要立即办理调高非柜面业务支出业务。柜员随即为客户办理，并请侯某出示提高日限额所需的响应辅助资料，侯某却表示不能提供响应材料支持其调额需求。

据了解，侯某目前的日限额为5000元，但她表示今日一定要取出1万元。该行运营主管与客户展开了沟通，详细询问侯某的情况与需求。侯某讲述中，不断提到自己的资金被冻结，“贷款”“提款”等情况。运营主管敏锐地察觉到了异常。果然，柜员查询之下，侯某账户并无冻结记录等其所描述的异常情况。

柜员帮助其舒缓了情绪后，侯某的表述逐渐清晰，事情原委也开始明朗起来。原来，侯某需要2万元周转资金，于是她决定上网找找“路子”。通过微信中的“搜一搜”，一个名为“京东金融
”的贷款平台吸引了她的视线。于是，她在该平台上填写了基本信息。

不久之后，一个归属地为香港的号码拨来，向侯某确认贷款需求后表示后续会有其他的贷款专员跟进此事。不一会儿，侯某便在微信上收到了好友添加请求。这名微信好友指示侯某下载所谓的“官方APP”填写贷款资料（包括其身份信息及银行卡信息）。

接着，侯某被告知其银行卡号有误，无法放款。该微信账号更谎称侯某银行卡被冻结，请示其“领导”“张总”后，向侯某出具了一份名为“中国银行保险监督管理委员会关于《贷款人侯××认证以及解冻贷款账户》的通知”，要求侯某通过“默信”APP予以解决。果然，神秘的“张总”在“默信”对侯某说，需要向指定账户中打款1万元用于“解冻”，并表示解冻后会将贷款总计3万元转入侯某账户。这才有了案例开头所述侯某来银行调整限额一事，银行员工精准识别出这是一起“冒充监管”进行网贷诈骗的案件，该行员工立刻协助客户向辖区派出所报警，并将客户卡内资金冻结，为客户挽回资金损失。

案例分析：网络诈骗构成犯罪

诈骗罪是指以非法占有为目的，用虚构事实或者隐瞒真相的方法，骗取数额较大的公私财物的行为。《中华人民共和国刑法》第二百六十六条规定，诈骗公私财物，数额较大的，处三年以下有期徒刑、拘役或者管制，并处或单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。目前电信诈骗手段层出不穷，普通客户难以辨别极易上当受骗。

本案中，诈骗分子试图非法占有客户侯某的1万元财产，故意通过上传虚假网贷链接，拨打虚假电话，下载第三方APP，冒充监管人员，虚构事实，使客户陷入账户冻结的错误认知，从而做出转移财产的决定，其行为明显构成诈骗，具有明显的社会危害性。根据国家相关法律规定，诈骗公私财物达到一定数额的，将构成犯罪。因此，银行员工发现诈骗行为后，立即协助客户报警处理，使诈骗行为止于未遂，保障了人民群众的财产安全。

银行员工敏锐察觉疑点，精准识别连环骗局，揭露了危害老百姓的“诈骗术”；体察客户真情，阻止客户资金流失，守住了老百姓的“钱袋子”。

风险提示：谨防不法分子冒充监管部门实施诈骗

广大消费者必须保持平和心态，不要轻易相信“天上掉馅饼”，要主动学习、了解更多金融知识，提高识别诈骗的能力，做好个人资产的风险防范，最大限度地保护自身合法权益不受侵害。同时也应主动下载“国家反诈中心APP”，自觉防范电信诈骗，并积极举报身边的电信诈骗，净化身边的金融环境。

（一）银保监局无权冻结任何单位和个人的银行账户。根据银保监会的授权和统一领导，银保监局依照法律法规对辖内银行保险机构实行统一监督管理、保护消费者合法权益，但无权直接冻结任何单位或个人的银行账户，更不会向消费者收取任何形式的保证金、认证金等名目的费用。消费者遇到类似情况要保持头脑冷静，切勿被不法分子所谓“账户资金被冻结”“将承担法律责任”等说辞迷惑，不要轻信谎言，以免落入骗局。银保监局不会上门回访或委托第三方机构合作开展维权业务，保险消费者务必提高警惕，增强风险防范意识和识别能力，谨防不法分子冒充监管部门实施诈骗，保障个人财产安全。如果接到相关电话，应当第一时

间向保险公司（官网公示的电话）或监管部门核实并反映情况。遭遇诈骗造成损失的，应保留相关证据、线索，并及时向公安机关报案。

（二）厅堂引导重细节，多看多问多提醒。银行员工在引导客户办理业务时，与客户多沟通,了解资金用途，密切关注客户办理业务时的情绪与意向，有效甄别客户所提供的信息的真实性,对有违常规的人和行为多留心、多关注、多提醒，不让一笔可疑交易从手中漏过，避免客户的账户资金遭到损失，做好防范电信诈骗风险提示和柜面防范工作。

（三）银行员工多学习，遏制风险在源头。银行一线人员需加强业务知识更新及专业能力提升，把好客户资金出入的第一道关，提高员工防范电信诈骗的意识，加强对柜员、大堂经理
及保安人员等的防诈安全教育培训，要求柜员、大堂经理及保安人员多观察、勤沟通，善意提醒客户对可疑电话、短信等要警惕与防范，避免客户资金损失，担起资金流出“防火墙”的职责。同时也应持续做好金融知识普及的工作，积极向客户宣讲、解释银行业务办理常识、电信诈骗犯罪特点等，并通过柜面宣传引导、张贴提示标语等方式告诫客户不要轻信各类中奖信息、退款信息等，提醒客户保护好自己的密码和存款介质。

网络诈骗等违法犯罪猖獗，强化账户开户源头性风险迫在眉睫。作为直接面对客户的商业银行，我们应该认真学习异常开卡特征，灵活地将理论知识用到实际工作中去，按照“了解你的客户”原则审慎办理业务，发现异常行为及时进一步核实，及时反馈，及时总结，及时汇报，全力以赴，按照“断卡”行动原则切实防范涉案账户，将风险遏制在源头，切实保护金融消费者的合法权益。

（作者单位：招商银行西安分行）