

网络科技公司疑似诈骗洗钱案

一、案情概述

- 企业名：A 公司
- 案由：疑似利用疫情期间恐慌心理诈骗

中国建设银行反洗钱人员在人工分析异常交易过程中发现成立时间较短的 A 公司，其账户经过开户后两个月的沉寂期后启用，并发生频繁交易，近期交易与新冠肺炎疫情发展曲线相符。截止 2020 年 3 月，仅一个多月的集中交易累计金额两千多万元人民币，累计交易笔数一万多笔，资金交易呈现“分散转入、集中转出、快进快出”的特征，交易频度和交易金额与公司的经营范围、成立时间、注册规模严重不符。

公司法定代表人失联，并与其他人员在多家公司交叉任职及持股，这些公司的空壳公司特征显著。贷方交易对手众多，包含一千多个个人主体，是借方交易对手主体个数的几十倍。资金来源地区较分散，来源于华北、华东、华南、西南等地区的三十余个省市，大部分为国内疫情较严重地区，对口罩等防疫物资需求迫切，符合受骗人群地域特征。下游交易对手地域相对集中，部分资金转出至他行个人账户，以切断资金链，通过跨行资金划转，切断银行对资金流向的追溯；超 80% 的资金流向数十个疑似空壳公司账户，将不法所得集中转移，规避风险。

交易摘要基本与企业正常生产经营无关，且存在贷方对手求购口罩的描述。但可疑主体仅仅是一个主营业务为提供网络服务的空壳公司，既不是口罩生产企业，也不具备售卖口罩的资质，涉嫌违规经营。贷方以“小额交易”为主，金额为 100 的倍数，借方金额多为 10000 的倍数。频繁使用代理服务器以规避监管，网银交易 IP 地址经常变更，多数显示为境外，且与数个主体共用 2 个 IP 地址。

判断 A 公司存在团伙电信诈骗嫌疑，异常交易时间段集中在疫情爆发期间，疑似利用人们在疫情发展阶段防疫物资短缺的恐慌心理实施诈骗，并归集、划转、过渡诈骗资金。该公司近期因涉嫌口罩诈骗案件被公安机关冻结账户资金，进一步印证了中国建设银行的判断。

二、客户基本情况

01 客户基本信息

A 公司，注册资本：数百万元人民币（实缴），企业类型：有限责任公司（自然人独资），行业：互联网和相关服务，登记状态：存续，经营范围：网络技术服务等。法定代表人为 B，执行董事兼总经理为 C。

02 客户账户情况

A 公司在中国建设银行开立一个对公结算账户，因多人使用同一联系电话于 2020 年 4 月被开户网点暂停非柜面交易。

三、资金交易情况

01 总体情况

2020年1月到2020年3月，A公司的账户累计发生交易一万多笔，涉及金额累计两千多万元，其中借方交易一千多笔，交易金额一千多万元，贷方交易一万多笔，交易金额一千多万元。

02 资金来源情况

账户资金来源较分散，主要来自于来源于华东、华南、西南、华北、东北等地区的三十余个省市，涉及一千多个主体，包括在国有银行、股份制银行、城市商业银行、农信社等多家银行开立的一千多个个人账户、在支付宝开立的支付账户和数十个公司账户，主要通过网上银行、手机银行、三方平台等渠道转入。

03 资金去向情况

资金归集到A公司的账户后，立即通过企业网银渠道转出，资金集中流向华东、华南、东北等地区的十余个个人主体、支付账户和E公司等几十个公司主体，收款人开户行涉及国有银行和股份制银行。

四、可疑点分析

01 客户身份、账户异常情况

(1) 空壳公司特征突出

A公司注册不足半年，成立时间短；开户预留联系电话为手机号，无固定电话，与负责人联系方式一致；注册地址为位于小区民宅。尽职调查显示，开户时留存的电话均已无人接听，无法联系到公司法人，疑似失联；调阅该账户流水，发现资金交易对手、频率、用途与其实际注册的经营范围有较大差距，空壳公司特征显著。

(2) 公司代理注册特征明显

该公司法定代表人B，华中地区某市人，到华南地区某市异地注册公司，其名下关联企业有数个，均在华南地区某市注册，公司高管均为B和C，成立日期集中在2019年末。

这五家关联企业成立时间仅间隔一周，注册资金相同；B和C交叉任职且为华中地区某市人；公司联系方式均为手机号；公司经营范围几乎完全一致，均为软件和信息技术服务业；公司地址均为步行街门面或居民小区内，但未实际经营。综上，B和C疑似通过批量成立“空壳公司”开立对公账户并出售给犯罪分子用于从事违法活动或洗钱活动，从中牟利。

(3) 账户异常

账户开立时开通了企业网银、单位结算卡等电子银行服务，几乎未发生柜面交易，频繁通过网上银行等非面对面交易渠道进行交易，借贷方交易金额基本相等，账户过渡性质明显。可疑主体注册成立几天后即开通了基本户，说明具有迫切的交易需求，但实际上开户后存在近2个月的沉寂期，于2020年2月启用账户并频繁交易。启用前仅发生少量介于几角至十几元的零星交易，交易对手主要为支付宝账户，疑似测试账户状态是否正常。

02 资金交易可疑点

(1) 交易频繁、资金量巨大，与可疑主体规模不符

A公司频繁交易时间段仅为1个月，累计交易超过一万多笔，交易金额接近两千多万元，交易金额及频率与该公司仅成立不足半年、未实际经营、经营地址

位于居民小区、主营业务为提供网络技术服务的资产规模严重不符，远超日常结算所需。

(2) 交易时间异常

超四分之三的交易（涉及金额两千多万元，笔数一万多笔）集中在 09:00—21:00 之间，其余时间段交易较为平均，但在凌晨 00:00—3:00 之间存在一个晚间交易的高峰，平均每小时发生交易几百笔/几十万元，与人们正常的生活状态不符。在 1 月 20 日国家正式公布新冠肺炎疫情开始后，可疑交易账户开始启用并频繁交易，其中 2020 年 2 月至 3 月期间，累计发生交易一万多笔/两千多万元，占报告期总交易金额的 99.99%，交易时间段与新冠肺炎疫情发展的时间曲线相符，疑似可疑主体通过疫情爆发造成的防护物资恐慌实施诈骗。

(3) 上游交易对手多且地域分散，下游交易对手地域集中但对手相对固定

- 贷方交易对手众多，包含一千多个个人主体，是借方交易对手主体个数的几十倍。个人账户累计交易金额高达一千多万元，占贷方交易金额超 90%。数百个主体与可疑账户为一次性交易，占贷方交易对手个数的超 30%，单点流入特征显著，疑似个人主体在单次交易后立即发现被诈骗而停止后续交易。

- 资金来源地区较分散，来源于华北、华东、华南、西南等地区的三十余个省市，大部分为国内疫情较严重地区，对口罩等防疫物资需求迫切，符合受骗人群地域特征。

- 下游交易对手地域相对集中，小部分资金转出至他行个人账户，以切断资金链，通过跨行资金划转，切断银行对资金流向的追溯；超 80% 的资金（交易笔数近千笔，交易金额一千多万元）流向 E 公司等几十个对公账户。通过追踪借方主要交易对手的工商注册信息及开户信息，发现这些公司存在一定的关联性并有相同的司法冻结记录，表现为：

全部成立于 2019 年 7 月—2019 年 11 月，与 A 公司注册时间接近，经营周期较短，账户交易大部份通过网银等非面对面方式交易，多以非生产型企业形式出现；注册资金最低十万元，最高几百万元，未实缴；超 60% 公司法定代表人关联（在公司中担任高级管理人员，如法人、股东、董事、监事等）1 家以上的公司，最多关联多达十余家公司，平均每家公司法定代表人关联 3 家以上的公司；公司法定代表人年龄相差较大，涉及 60 后到 00 后各年龄层，均为异地开户，户籍地址遍布全国各地，年龄最小的仅为 20 岁；公司经营范围集中在批发业、软件和信息技术服务业；所有公司的注册地址为小区民宅或模糊地址，且多家公司共用。

涉及公司多被中国建设银行报送过可疑，部分公司涉嫌刑事案件而被有权机关单向冻结账户，且至今账户仍被冻结。交易行为没有真实的贸易背景，银行账户资金往来的规模和频率与公司注册资本明显不匹配，账户过渡性质极其明显，疑似为过渡诈骗资金而成立的空壳公司，实现账户资金的大量快速转移。

(4) 规避柜面交易，多户划转，交易模式异常

- A 公司账户启用后频繁发生资金收付，100% 的交易使用网上银行、手机银行、第三方支付等非柜面支付手段，层级分明，疑似分户流转诈骗资金；借贷方累计交易金额仅相差一万多元，仅占总交易金额的不足 0.1%，账户过渡性质明显，存在规避监管嫌疑。

- 频繁进行跨行跨地区交易，跨行交易累计交易一万多笔，交易金额达两千多万元，占总交易笔数的超 85%，占总交易金额的超 80%，交易对手账户开立

在我国境内多家银行（跨行账户身份难以核查），多维度进行资金过渡与转移，以此掩盖资金来源、性质、用途。

● 防疫电信诈骗的主要套路是利用微信等网络平台宣称自己有渠道筹集或拥有口罩等防疫物资，诱骗要求受害者上当。其交易表现为：资金通过多人归集到 A 公司账户后，在 1-5 分钟内通过网上银行、手机银行等电子银行渠道转出，多为同一天或次日凌晨通过支付宝等三方平台提现，疑似将诈骗资金频繁通过各级分类账户分层划转隐匿转移资金。

（5）交易备注异常，与正常经营不符

贷方交易备注中出现“订购 XX 只口罩款”的描述，交易日期为 2020 年 3 月凌晨，此时市场上口罩仍属于稀缺产品；对应的贷方汇入金额为几万元整，由此可推断可疑主体用于诈骗的口罩价格为几元一个，应为一次性医用或民用口罩，远低于同期市场同类口罩价格。数天后，该可疑交易账户被有权机关单向冻结，疑似与此相关。

此外，很多贷方交易备注为“字母+数字”，疑似某种暗号或会员号，交易金额多为整数，与正常的经营性资金交易特征不符。

A 公司账户交易较少发生正常企业经营相关的工资、货款、物流、税款等交易。

（6）交易金额异常，特征显著

贷方以“小额交易”为主，单笔交易金额多为 100 元的倍数。当账户收到多笔贷方汇入交易时，在 1-5 分钟内集中转出，借方交易以“大额交易”为主，金额为 10000 元的倍数，存在构造性资金交易，如交易金额为 49900 元、49990 元、49999 元等，控制在 5 万元以下，有意逃避大额资金监管。

（7）IP 地址显示位于境外，账户呈集中控制状态

A 公司 2020 年 2 月仅交易 20 天，但累计使用代理服务器几十次，与数个公司和个人共用 2 个 IP 地址，IP 归属地为菲律宾某市，与公司注册地址、开户地址均不相符。账户呈集中控制状态，疑似通过租用境外服务器或使用代理，混淆真实地理位置，掩盖真实交易地点和资金最终去向，涉嫌团伙过渡转移资金。

五、最终结论和采取的措施

综合以上客户身份、交易情况等分析，中国建设银行认为 A 公司疑似利用人们在疫情发展阶段防疫物资短缺的恐慌心理实施诈骗，并利用公司账户过渡和转移诈骗资金，交易频率较高，涉及金额较大。中国建设银行形成重点可疑交易报告上报人行和公安机关，并将其风险等级调为高风险，对其账户采取限制非柜面交易管控措施，加强跟踪监测，并根据监管机关的要求作进一步核查与管控。

该公司近期因涉嫌口罩诈骗案件被公安机关冻结账户资金，进一步印证了中国建设银行的判断。

（来源：中国互联网金融协会微信公众号）