



远离违法犯罪
警惕洗钱风险

远离违法犯罪 警惕洗钱风险

反洗钱知识宣传手册



目录 Contents

一、前言

一、前言	1
二、选择安全可靠的金融机构	2
三、主动配合反洗钱义务机构进行身份识别	3
四、做好个人账户分类管理	5
五、严禁出租、出借、出售、购买银行账户（银行卡）	6
六、合理选择交易方式，大额交易和可疑交易将被报告	7
七、不要用自己的账户替他人提现	9
八、增强风险意识，防范电信网络诈骗	10
九、谨防“首付贷”等购房融资被用于洗钱	11
十、远离非法买卖外汇活动	12
十一、远离“套路贷”理性消费借贷	13
十二、拒绝高利诱惑、远离非法集资	15
十三、警惕“虚拟货币”、“区块链”骗局	17
十四、保护自己、远离洗钱反洗钱案例介绍与评析	19
十五、举报洗钱活动，维护社会公平正义	24

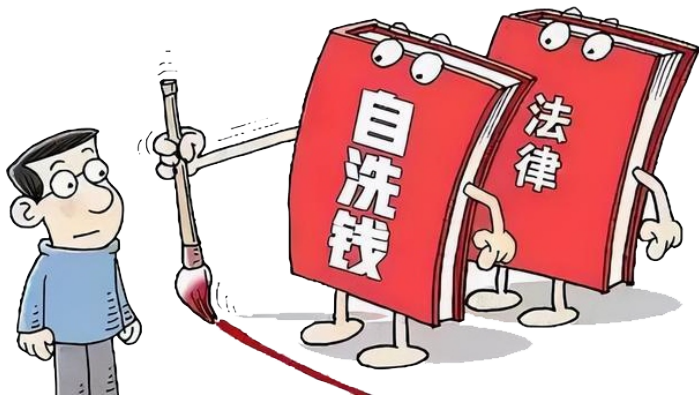
洗钱，是指将上游犯罪所得及其产生的收益，通过各种手段掩饰、隐瞒其来源和性质，使其在形式上合法化的行为。

近年来，随着毒品犯罪、黑社会性质的组织犯罪、恐怖活动犯罪、走私犯罪、贪污贿赂犯罪、破坏金融管理秩序犯罪、金融诈骗犯罪等上游犯罪活动日益增多，与之相伴的洗钱犯罪问题亦日渐突出，不仅破坏了我国金融秩序，而且危害到经济安全和社会稳定。洗钱的危害越来越引起全社会的广泛重视：洗钱为犯罪分子隐藏和转移犯罪所得提供便利，为犯罪活动提供进一步资金支持，助长更严重和更大规模的犯罪活动，洗钱活动削弱国家的宏观经济调控效果，严重危害经济的健康发展；洗钱助长和滋生腐败，败坏社会风气，腐蚀国家肌体，导致社会不公平，损害国家声誉；洗钱活动危害合法经济体的正当利益，破坏市场微观竞争环境，妨害市场机制的有效运作和公平竞争；洗钱活动造成资金流动的无规律性，影响金融市场的稳定；洗钱活动破坏金融机构稳健经营的基础，加大了金融机构的法律风险和运营风险。为深入贯彻习近平总书记重要指示批示精神，落实中央、省、市及安顺市反洗钱、反恐怖融资、反逃税工作部门联席会议制度关于预防和打击洗钱犯罪的安排部署，切实保障广大人民群众合法权益、维护社会和谐稳定，确保实现洗钱犯罪案件的快侦、快诉、快判。

二、选择安全可靠的金融机构

合法的金融机构必须接受国家金融管理当局的监管，履行反洗钱义务，对客户和机构自身负责。根据《中华人民共和国反洗钱法》的规定，金融机构对依法履行反洗钱职责或者义务获得的客户身份资料和交易信息，应当予以保密，非依法律规定，不得向任何单位和个人提供，确保金融机构客户的隐私权和商业秘密得到保护。

地下钱庄、非法外汇交易平台，以及打着金融创新、虚拟货币、区块链、互联网金融等旗号的非法机构逃避监管，不仅为犯罪分子和恐怖势力转移资金、清洗“黑钱”，成为社会公害，而且无法保障客户资金和财产的安全。选择安全可靠、严格履行反洗钱义务的金融机构，个人资金和信息才会更安全、更有保障。



三、主动配合反洗钱义务机构进行身份识别

开办业务时，出示真实有效身份证件

有效身份证件是证明个人真实身份的重要凭证。为避免他人盗用个人名义从而窃取个人财富，或是盗用个人名义进行洗钱等犯罪活动，开立账户、购买金融产品以及以任何方式与金融机构建立业务关系时，须做到以下几点：

- 出示有效身份证件或者其他身份证明文件；
- 如实填写个人身份信息；
- 配合金融机构现场核查身份证件的真实性，或以电话、信函、电子邮件等方式确认身份信息；
- 回答金融机构工作人员的合理提问。

如果不能出示真实有效身份证件或者其他身份证明文件，金融机构工作人员将不能为其办理相关业务。

存取大额现金时，请出示有效身份证件

凡是存入或取出5万元以上人民币或者等值1万美元以上外币时，金融机构须核对客户的有效身份证件或其他身份证明文件。这并非限制个人支配自己合法收入的权利，而是希望通过这样的措施，防止不法分子浑水摸鱼，保护资金安全，创造更安全、更有效的金融市场环境。

代人办理业务，代理人应出示代理人和被代理人的有效身份证件

金融机构工作人员需要核实交易主体的真实身份，当委托他人代为办理业务时，需要对代理关系进行合理的确认。

特别提醒：当代理他人开立账户、购买金融产品、存取大额资金时，金融机构需要核对被代理人 and 代理人的有效身份证件。

身份证件到期更换的，请及时到金融机构更新相关信息

金融机构只能向身份真实有效的客户提供服务，对于身份证件已过有效期的、超过合理期限仍未更新的，金融机构可中止办理相关业务。

不要出租或出借自己的身份证件以及账户、银行卡和U盾

出租或出借自己的身份证件以及账户、银行卡和U盾，可能会产生以下后果：

- 他人盗用您的名义从事非法活动；
- 协助他人完成洗钱和恐怖融资活动；您可能成为他人金融诈骗活动的“替罪羊”；
- 您的诚信状况受到怀疑；您的声誉和信用记录因他人的不当行为而受损。

四、做好个人账户分类管理

I类户是“钱箱”，用于存放个人的工资收入等主要资金来源，安全性要求高，通常需要在银行柜面开立。

II类户是“钱夹”，用于个人日常刷卡消费、网络购物、网络缴费等，可以采用数字证书或者电子签名开立。

III类户是“零钱包”，用于金额较小、频次较高的交易，如常见的手机扫码支付，可以采用数字证书或者电子签名开立。

● III类户任一时点账户余额不得超过2000元；

● III类户消费和缴费支付、非绑定账户资金转出等出金的日累计限额合计为2000元，年累计限额合计为5万元。

根据实际需要开立账户，同一个人在同一家银行（以法人为单位，下同）只能开立一个I类户；同一法人银行为同一个人开立II类户、III类户的数量原则上分别不超过5个。

请注意，务必妥善保管个人信息，如身份证号、银行卡号、手机号、短信验证码。不法分子往往通过各种诈骗形式诱导用户提供个人信息，利用这些信息诈骗用户资金或者假名注册支付账号、申请银行账户等，更有甚者被冒名参与洗钱或从事恐怖融资等非法金融活动。在各种泄露的个人信息中，最容易被网络犯罪集团用来牟利的就是手机号码、身份证号码、银行卡号和短信验证码这类直接关系到账户安全的信息。

五、严禁出租、出借、出售、购买银行账户（银行卡）

自2019年4月1日起，银行和支付机构对公安机关认定的出租、出借、出售、购买银行账户（含银行卡，下同）或支付账户的单位和个人，组织购买、出租、出借、出售银行账户或支付账户的单位和个人，假冒他人身份或者虚构代理关系开立银行账户或支付账户的单位和个人，5年内暂停其银行账户非柜面业务、支付账户所有业务，并不得为其新开立账户。



自2019年6月1日起，银行为客户，开立账户时，应当在开户申请书、服务协议或开户申请信息填写界面醒目位置告知客户出租、出借、出售、购买账户的相关法律责任和惩戒措施，并载明以下语句：“本人（单位）充分了解并清楚知晓出租、出借、出售、购买账户的相关法律责任和惩戒措施，承诺依法依规开立和使用本人（单位）账户”，由客户确认。

六、合理选择交易方式大额交易和可疑交易将被报告

符合下列情形的交易，金融机构将向中国反洗钱监测分析中心报告：

- 自然人、非自然人的大额现金交易：境内和跨境的报告标准均为人民币5万元以上（含5万元）、外币等值1万美元以上（含1万美元）；

- 非自然人银行账户的大额转账交易：境内和跨境的报告标准均为人民币200万元以上（含200万元）、外币等值20万美元以上（含20万美元）；

- 自然人银行账户的大额转账交易：境内的报告标准为人民币50万元以上（含50万元）、外币等值10万美元以上（含10万美元），跨境的报告标准为人民币20万元以上（含20万元）、外币等值1万美元以上（含1万美元）。

符合下列情形的，如未发现交易或行为可疑的，金融机构可以不报告：

- 定期存款到期后，不直接提取或者划转，而是本金或者本金加全部或者部分利息续存人在同一金融机构开立的同一户名下的另一账户；

- 活期存款的本金或者本金加全部或者部分利息转为在同一金融机构开立的同一户名下的另一账户内的定期存款；

- 定期存款的本金或者本金加全部或者部分利息转为在同一金融机构开立的同一户名下的另一账户内的活期存款；

- 自然人实盘外汇买卖交易过程中不同外币币种间的

转换。需要注意的是，金融机构发现或者有合理理由怀疑客户、客户的资金或者其他资产、客户的交易或者试图进行的交易与洗钱、恐怖融资等犯罪活动相关的，不论所涉资金金额或者资产价值大小，都会向中国反洗钱监测分析中心提交可疑交易报告。

因此，慎重保管个人身份证件和账户，合理选择交易方式，可避免涉嫌洗钱，影响个人生产生活学习等合法需要。

金融机构按照规定报告大额交易不影响金融业务的正常办理。



七、不要用自己的账户替他人提现

通过各种方式提现是犯罪分子最常采用的洗钱手段之一。有人受朋友之托或受利益诱惑，使用自己的个人账户或公司的账户为他人提取现金，为他人洗钱提供便利。然而法网恢恢，疏而不漏。请切记，账户将忠实记录每个人的金融交易活动，请不要用自己的账户替他人提现。



请注意，个人持境内银行卡在境外提取现金，本人名下银行卡（含附属卡）合计每个自然年度不得超过等值10万元人民币。超过年度额度的，本年及次年将被暂停持境内银行卡在境外提取现金。

个人不得通过借用他人银行卡或出借本人银行卡等方式规避或协助规避境外提取现金管理。

个人持境内银行卡在境外提取现金，外币下由每卡每日不得超过等值1000美元调整为等值1万元人民币；人民币卡管理维持每卡每日不得超过等值1万元人民币。

八、增强风险意识，防范电信网络诈骗

● 坚持账户实名制，不向他人出售账户或者协助他人开户；

● 保护个人信息安全，不轻易向他人透露个人信息、账户信息、支付信息等；

● 不参与买卖银行账户、银行卡、POS 机等；

● 做好个人账户分类管理，建议将 II 类户、III 类户用于网络支付和移动支付业务；

● 不信、不盲从未经证实的转账信息；

● 如果不慎遭遇电信网络诈骗，要保留微信、QQ、短信等往来信息，以及ATM转账、网银转账、手机银行转账、支付宝支付、微信支付等转账凭证或者信息，便于警方锁定犯罪嫌疑人。

为了保障自身资金安全，建议关注电信网络新型违法犯罪典型手法及应对措施、转账汇款注意事项，认识到买卖账户的社会危害，强化个人金融信息保护意识。在日常生活中，要注意保管好自己的身份证、银行账户和支付账户，妥善保护个人信息、账户信息、金融交易信息等，确保自己的个人金融信息等隐私信息不受侵害。



九、谨防“首付贷”等购房融资被用于洗钱

以下购房融资都是违规的：

● 房地产开发企业、房地产中介机构为购房人垫付首付款或采取首付分期等其他形式变相垫付首付款，通过任何平台和机构为购房人提供首付融资，以任何形式诱导购房人通过其他机构融资支付首付款，组织“众筹”购房；

● 互联网金融从业机构、小额贷款公司以线上、线下或其他任何形式为购房人提供的首付融资或相关服务；

● 房地产中介机构、互联网金融从业机构、小额贷款公司为卖房人或购房人提供的“过桥贷”“尾款贷”“赎楼贷”等场外配资金融产品；

● 个人综合消费贷款等资金挪用于购房。

请注意，房地产开发企业、房地产中介机构应要求房屋交易当事人以银行转账的方式支付购房款，并使用交易当事人的同名银行账户；发生退款的，应按原支付途径，将资金退回原付款人的银行账户。如确需使用现金支付的，当日现金交易单笔或累计达到人民币5万元以上的，应在交易发生之日起5个工作日内向中国反洗钱监测分析中心报送大额交易报告。

十、远离非法买真外汇活动

最高人民法院、最高人民检察院联合发布的《关于办理非法从事资金支付结算业务、非法买卖外汇刑事案件适用法律若干问题的解释》中明确规定，非法买卖外汇行为扰乱金融市场秩序，情节严重的以非法经营罪定罪处罚。非法买卖外汇行为包括倒买倒卖外汇、变相买卖外汇等行为。倒买倒卖外汇，是较为传统的非法买卖外汇行为，指不法分子在国内外汇黑市进行低买高卖，从中赚取汇率差价，即俗称的“换汇黄牛”。变相买卖外汇，形式上不再是一手交钱，一手交汇，而是将交易过程分割开来，分别在境内、境外进行。

在正规外汇交易场所进行外汇兑换，远离地下钱庄、境外炒汇投资平台。未经批准擅自开展外汇期货和外汇现金交易的行为均属于违法行为，参与双方不受法律保护。

在我国，经营结汇、售汇业务需要经国家外汇管理部门的批准，外汇买卖也必须在指定场所办理。获得结汇、售汇业务经营资格的主体包括：(1)外汇指定银行，例如中国银行、建设银行等；(2)经外汇管理机构批准，经营个人本外币兑换特许业务的非金融机构；(3)中国外汇交易中心（仅限于经批准的会员单位）

个人购汇，六“不得”：

- 不得虚假申报个人购汇信息；
- 不得提供不实的证明材料；
- 不得出借本人便利化额度协助他人购汇；
- 不得借用他人便利化额度实施分拆购汇；
- 不得用于境外买房、证券投资、购买人寿保险和投资性返还分红类保险等尚未开放的资本项目；
- 不得参与洗钱、逃税、地下钱庄交易等违法违规活动。

十一、远离“套路贷”理性消费借贷

一般来说，“套路贷”通常以民间借贷为幌子，通过与被害人签订借款合同，制造借贷假象，并以“中介费”“保证金”“行规”等各种名目骗取被害人签订明显不公平的合同条款，并故意拖延还款日期，造成被害人违约，从而收取高额违约金等。

【套路1】虚假宣传吸引用户

用户A在平台B上看到“0抵押、0担保”的虚假宣传，被“低息”“短期”“急用钱”等因素诱惑借贷。

【套路2】诱骗用户签虚假合同

平台B收集用户A手机通讯录中的相关信息、身份证号等，并让用户A按平台要求签订虚假合同或协议。举个例子，用户借款5000元，平台以收取“服务费”为由扣除700元，实际到手只剩4300元，合同签订金额则为15000元（谎称是“行规”）。

【套路3】单方认定违约

平台B故意拖延还款日期致用户A债务逾期，并要求用户A全额偿还还因逾期虚假增高的债务，如债务中5000元增高到1500元，这种“套路”赚的就是服务费和逾期费。

【套路4】恶意垒高借款

用户A短期没法偿清债务时，平台B推荐其他不法平台借款给用户A，也就是造成用户A用后账还前账，最终欠款成“滚雪球”效应，越滚越大。

【套路5】软硬兼施索债

用户A无力偿还，平台B软硬兼施讨债，集中表现为暴力与软暴力交织使用，泼油漆、撬锁、敲诈亲友等，给被害人造成无休止的骚扰。

谨记：

- 理性借贷

要树立正确的消费观，量入为出；不要贪图一时享乐，不计后果，盲目借贷。

- 不轻信虚假宣传

一味宣传“无须审核、无抵押、无担保、无利息”的网络借贷平台往往暗藏玄机。

- 选择有贷款资质的正规渠道借贷

避免向一些“小额贷款公司”或者专门从事高利贷放贷的网贷机构借款。

- 但凡钱款往来，务必留存证据

还款时尽量选择有迹可循的转账方式，并注意留言标明资金用途，若采用现金还款，要让对方及时写收条。

- 若不幸陷入“套路贷”要及时报警

在遭遇不法分子恐吓、骚扰等暴力催收时，请第一时间报警，避免遭受财产损失和侵害。

十二、拒绝高利诱惑、远离非法集资

非法集资是指单位或者个人未经有关部门依法批准，以发行股票、债券、彩票、投资基金证券或者其他债权凭证的方式，向社会公众募集资金，承诺在一定期限内给出资人还本付息。还本付息的形式除以货币形式为主外，也有实物形式和其他形式。

非法集资的常见手段

- 承诺高额回报

不法分子为吸引群众上当受骗，往往编造“天上掉馅饼”、“一夜成富翁”的神话，通过暴利引诱许诺投资者高额回报。为了骗取更多的人参与集资，非法集资者在集资初期，往往按时足额兑现承诺本息，待集资达到一定规模后，便秘密转移资金或携款潜逃，使集资参与者遭受经济损失。

- 编造虚假项目

不法分子大多通过注册合法的公司或企业，打着响应国家产业政策、支持新农村建设、实践“经济学理论”等旗号，经营项目由传统的种植、养殖行业发展到高新技术开发、集资建房、投资入股、售后返租等内容，以订立合同为幌子，编造虚假项目，承诺高额固定收益，骗取社会公众投资。有些不法分子假借委托理财名义，故意混淆投资理财概念，利用电子黄金、投资基金、网络炒汇、电子商务等新名词迷惑社会公众，承诺稳定高额回报，欺骗社会公众投资。

●以虚假宣传造势

不法分子为了骗取社会公众信任，在宣传上往往一掷千金，采取聘请明星代言、在著名报刊上刊登专访文章、雇人广为派发宣传单、进行社会捐赠等方式，加大宣传力度，制造虚假声势，骗取社会公众投资。有些不法分子利用网络虚拟空间将网站设在异地或租用境外服务器设立网站。有的还通过网站、微博、微信、QQ等平台，传播虚假信息，骗取公众投资。一旦被查，便以下线、不按规则操作等为名，迅速关闭网站，携款潜逃。

●利用亲情诱骗

不法分子往往利用亲戚、朋友、同乡等关系，用高额回报诱惑社会公众参与投资。有些参与传销的人员，在传销组织的洗脑或人身强制下，为了完成或增加自己的业绩，不惜拉拢亲朋好友、同学或邻居加入，使参与人员迅速蔓延，集资规模不断扩大。

如何防范“非法集资”

计算银行贷款利率和普通金融产品的回报率，明显偏高的投资回报很可能就是投资陷阱。

通过政府公开信息和网站，对相关企业是否具备发行、销售股票、债券或者其他金融产品的资格进行查询。

对于陌生人低风险、高回报的投资建议和反复劝说，要多与其他懂行的家人、朋友和专业人士仔细问询、商量，审慎决策，切不可抱有侥幸心理，盲目投资。

如果实在无法判断是不是属于非法集资，还可以向政府金融办、公安、工商、金融监管机构等部门咨询，了解清楚后再作决定。

十三、警惕“虚拟货币” “区块链”骗局

一些不法分子打着“金融创新”、“区块链”的旗号，通过发行所谓“虚拟货币”、“虚拟资产”、“数字资产”等方式吸收资金，侵害公众合法权益。此类活动并非真正基于“区块链”技术，而是炒作“区块链”概念并进行非法集资、传销、诈骗等违法行为。

●网络化、跨境化明显

依托互联网、聊天工具进行交易，利用网上支付工具收支资金，风险波及范围广、扩散速度快。一些不法分子通过租用境外服务器搭建网站，实质面向境内居民开展活动，并远程控制实施违法活动。一些个人在聊天工具群组中声称获得了境外优质“区块链”项目投资额度，可以代为投资，极有可能是诈骗活动。这些违法活动资金多流向境外，监管和追踪难度很大。

●欺骗性、诱惑性、隐蔽性较强

利用热点概念进行炒作，编造名目繁多的“高大上”理论，有的还利用名人“站台”宣传，以空投“糖果”等为诱惑，宣称“币值只涨不跌”、“投资周期短、收益高、风险低”，具有较强的蛊惑性。在实际操作中，不法分子通过幕后操纵所谓虚拟货币价格走势、设置获利和提现门槛等手段非法牟取暴利。此外，一些不法分子还以ICO、IFO、IEO等花样翻新的名目发行代币，或打着共享经济的旗号以IMO方式进行虚拟货币炒作，具有较强的隐蔽性和迷惑性。



● 存在多种违法风险

不法分子通过公开宣传，以“静态收益”（炒币升值获利）和“动态收益”（发展下线获利）为诱饵，吸引公众投入资金，并利诱投资人发展人员加入，不断扩充资金池，具有非法集资、传销、诈骗等违法行为特征。

此类活动以“金融创新”为噱头，实质是“借新还旧”的庞氏骗局，资金运转难以长期维系。

十四、保护自己、远离洗钱 反洗钱案例介绍与评析

根据《中华人民共和国刑法》第191条规定，明知是毒品犯罪、黑社会性质的组织犯罪、恐怖活动犯罪、走私犯罪、贪污贿赂犯罪、破坏金融管理秩序犯罪、金融诈骗犯罪的所得及其产生的收益，为掩饰、隐瞒其来源和性质，有下列行为之一的，没收实施以上犯罪的所得及其产生的收益，处五年以下有期徒刑或者拘役，并处或者单处洗钱数额百分之五以上百分之二十以下罚金；情节严重的，处五年以上十年以下有期徒刑，并处洗钱数额百分之五以上百分之二十以下罚金

- （一）提供资金账户的；
- （二）协助将财产转移为现金、金融票据、有价证券的；
- （三）通过转账或者其他结算方式协助资金转移的；
- （四）协助将资金汇往境外的；
- （五）以其他方法掩饰、隐瞒犯罪所得及其收益的来源和性质的。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，处五年以下有期徒刑或者拘役；情节严重的，处五年以上十年以下有期徒刑。

◆ 逃税案例

某银行发现客户赵某借记卡账户交易异常，每日有大量个人将款项存入该账户，交易频繁，交易涉及全国大部分省市，北方城市较多，但单笔金额小，一般为千元左

右，并定期通过网银业务将资金集中划出。该银行从基层网点获取的客户尽职调查信息反映，曹某为X保健品有限公司的法定代表人，在该银行开立了单位结算账户，但交易并不频繁。

反洗钱监管部门接收可疑交易线索后，对X保健品有限公司的背景情况进行了调查，发现X保健品有限公司系中美合资企业，主要生产牙膏系列产品。根据上述信息，反洗钱监管部门认为曹某、赵某个人账户资金交易可能与公司行为存在内在联系，决定将可疑交易移送公安机关。经公安机关侦查发现，X保健品有限公司法定代表人曹某在负责公司经营期间，采用销售不开发票、收入不入账等手法，将公司部分销售收入汇入原公司出纳赵某在该银行的个人账户内，随后再转入其个人账户内，隐匿销售收入达4000万元，涉嫌偷逃增值税500余万元。

案例评析

1、赵某个人账户交易非常频繁，且单笔金额小，没有规则性，因此其资金交易应该和经营行为存在某些内在联系。2、赵某个人账户频繁交易不存在时间阶段性，每天都有发生，因此巩固了对其从事经营活动资金结算的判断。实际案例中，有些个人账户也会出现上述频繁、单笔金额小的收付特征，但是注意观察其交易的时间一般集中在国定假日及双休日，经侦查发现主要是由于国定节假日银行停止办理对公结算业务，一些企业为了保证节假日生产经营活动资金结算的正常进行，故选择个人账户进行资金结算，待工作日再将资金全额转入企业账户。3、该案中赵某账户资金来源地域非常分散，与其资金去向曹某所在单位经营牙膏的生产经营特点吻合。

◆地下钱庄案例

80多岁的香港人陈先生一直在内地经商，他与某国商业银行深圳一支行行长沈某认识多年。因年纪大了，陈先生想把在内地的产业卖掉，回头香港养老。2012年年初，沈某得知后，声称可以通过自己手中的外汇指标，帮陈先生帮其手中的人民币换成港币，转回香港，但需要200万元好处费。陈先生同意让沈海生帮忙。随后，陈先生将6337余万元分3次汇到沈海生指定的李某账户上。前两次转账后，陈先生的香港账户都有收到港元。第三次汇款后，陈先生的香港账户只收到了部分款项，还有800万元一直没有收到。经陈先生多次追问，沈某才承认他根本没有外汇指标，而是通过地下钱庄操作。沈某辞职潜逃时，仍有625万元没有归还陈先生。

根据警方调查，陈先生的钱汇入李某账户后，在短时间内又被转移到5个可疑账户，随后又迅速向100多个账户转移资金。警方对200多个银行账户进行梳理，一个地下钱庄逐渐浮出水面。

警方将叶某、郑某等30余人抓获，捣毁地下钱庄窝点6个，查获银行卡300余张，涉案金额高达120亿元。

案例评析

“地下钱庄”为逃避海关监管，转向利用职业“水客”少量多次非法携带货币出境洗钱。水客集团被称为“金融蚂蚁”，小批量为“地下钱庄”携带超额货币出境。职业“水客”以40-55岁中老年无业妇女为主，入境时不携带违规物品，出境时携带货币以赚取少量的带工费。“水客头”与带钞“水客”形成雇佣关系，一般由“水客头”在境内派发具有统一包装标识的货币到香港后由专人交接并支付带工费，已经形成了一套分工明确的走私“作业”流程。

◆恐怖融资案例

B国的一家金融机构报告有一个年收入1.7万美元的个人客户，其账户一年的交易额却达到356万美元。调查人员进一步调查发现这个人根本不存在，账户是用伪造的身份开立的。

进一步调查发现这个账户与国外的一家慈善组织有关，账户被用来通过伪造的计划为恐怖组织筹款。在B国，政府会另外再给慈善组织笔捐款，约为捐赠款的42%。所有进入该账户的捐款都被调查，同时慈善组织也向政府主张权利要求政府兑现额外的捐款。实际上，捐款很快被退回了捐赠人，所以慈善组织没有收到任何真正的捐款。但是慈善组织却保留了政府的捐款，诈骗了超过114万美元的资金。

案例评析

本案说明有关联的账户是如何被用来从事非法活动，表明身份确认程序的重要性，同时也表明监管发现账户的异常交易对于识别洗钱和打击恐怖组织的经济来源都是非常有帮助的。

◆诈骗案例

两家公司的“老总”在QQ上要钱，会计立即汇款，不料把钱汇给了骗子。

警方介入后决定从赃款流向入手，经调查发现两家公司被骗的钱多次被转账，骗子的网络账号和网银转账是在同一个IP地址上登录的，而两笔被骗的钱被充值到了一个支付宝账号上，通过这些信息，锁定了犯罪嫌疑人之一的潘某。潘某交代，他在朋友家吃饭时认识了“阿陈”，对方说“网络诈骗来钱快”，潘某则说自己能把钱“洗白”，两人一拍即合，开始了合作。随后，潘某花700元，买了10张身份证及对应的银行卡、U盾，用来接收“阿陈”

的赃款。每次“阿陈”利用网络账号诈骗得手之后，就打电话告知潘某。收到赃款后，潘某用网上银行买游戏点券，在网上低价出售，再从绑定的银行卡中体现，与“阿陈”分赃。人民法院认定潘某犯掩饰、隐瞒犯罪所得罪，判处有期徒刑7年，并处罚金10万元。

案例评析

1、提高风险防范意识。设置QQ密码不要过于简单，且一定要对QQ密码设置保护。不要随便接收陌生人发来的邮件，防止因中了木马病毒而导致QQ号码被盗，尽量将财务电脑和其他电脑分开，减少病毒传染的可能性。聊天时，不要轻易向陌生人泄露个人信息。电脑要安装杀毒软件定期查杀。

2、公司、企业要加强内部管理，完善财务管理制度，规范资金进出流程。接受领导重大工作指示特别是涉及款项往来等经济事务时一定要慎重，务必通过电话或者当面进行核实和确认，尽量不要通过QQ等网络工具进行沟通，最大限度地减少因管理疏漏而给犯罪分子可乘之机。



十五、举报洗钱活动，维护社会公平正义

为了发挥社会公众的积极性，动员社会的力量与洗钱犯罪做斗争，保护单位和个人举报洗钱活动的合法权利，《中华人民共和国反洗钱法》特别规定任何单位和个人都有权向中国人民银行或公安机关举报洗钱活动，同时规定接受举报的机关应当对举报人和举报内容保密。

每个公民都有举报的义务和权利，欢迎所有公民举报洗钱活动及线索。所有举报信息将被严格保密。

发现洗钱活动，可以通过以下途径举报。

▲向公安机关举报

▲向中国人民银行各分支机构反洗钱部门]举报

▲向中国反洗钱检测分析中心举报

举报电话：010—88092000

举报信箱：北京市西城区金融大街35号32-134信箱

收件单位：中国反洗钱检测分析中心

电子信箱：fiurepot@pbc.gov.cn

举报网站：www.camlmac.gov.cn

反洗钱，人人有责。

打击洗钱，遏制犯罪。

举报洗钱，利国利民。

保护自己，请您远离洗钱活动。

打击洗钱犯罪，构建和谐社会。

打击洗钱犯罪，维护金融安全。

打击洗钱犯罪，维护金融秩序。

遏制洗钱活动，维护国家利益。

履行反洗钱义务，维护金融秩序。

履行反洗钱职责，严惩洗钱犯罪。

提高反洗钱意识，防范洗钱风险。

了解反洗钱知识，遵守反洗钱法规。