



一生保障 | 在你左右

了解反洗钱知识，远离洗钱犯罪

中英人寿2015年反洗钱宣传资料

合规管理部 2015年11月

Serve with
C.A.R.E.

前 言

针对集资诈骗、电信诈骗、“钓鱼网站”诈骗、出售信用卡用于洗钱、地下钱庄等涉众型洗钱犯罪活动频发的态势，为进一步提高社会公众对洗钱和恐怖融资危害的认识，增加反洗钱和反恐怖融资意识，我们制作了以下反洗钱有关的知识。请您认真学习，保护自己，远离洗钱犯罪。

目 录

- 一、 *反洗钱知识问答*
- 二、 保护自己，远离洗钱
- 三、 常见洗钱案例

一、反洗钱知识问答

1. 什么是洗钱？

“洗钱”是指：将犯罪所得赃款通过金融机构、保险公司、证券公司等合法途径，转移、隐瞒、掩饰犯罪所得赃款的性质和来源，使其变为貌似合法收益的不法行为。

2. 什么是反洗钱？

反洗钱是指为了预防通过各种方式掩饰、隐瞒毒品犯罪、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、金融诈骗犯罪等犯罪所得及其收益的来源、性质的洗钱活动，依照《中华人民共和国反洗钱法》规定采取相关措施的行为。

3. 反洗钱的内容有哪些？

反洗钱就是依法采取措施进行预防洗钱活动的行为，这些行为包括多方面的内容，如客户身份识别、大额交易和可疑交易报告、保存客户身份资料和交易记录，以及依法进行的反洗钱检查、调查等。

4. 什么是反洗钱义务主体？

由于金融机构和特定非金融机构是最易于被洗钱者用作洗钱的渠道和洗钱发生的高危领域，因此，在中华人民共和国境内设立的金融机构，以及按照规定应当履行反洗钱义务的特定非金融机构，便成为反洗钱义务主体，而金融机构更成为反洗钱义务的核心主体，保险公司属于金融机构，理应承担反洗钱的义务。

一、反洗钱知识问答

5. 什么是客户身份识别制度？

客户身份识别制度，也称“了解你的客户”，是指金融机构在与客户建立业务关系或与其进行交易时，应当根据法定的有效身份证件或其他身份证明文件，确认客户的真实身份。同时，了解客户的职业情况或经营背景、交易目的、交易性质以及资金来源等。它是金融机构在预防洗钱活动中所构筑的第一道防线。

6. 什么是大额交易和可疑交易报告制度？

大额交易和可疑交易报告制度是指金融机构或非金融机构在经营过程中对超过规定金额以上的或有洗钱嫌疑的资金交易依法向反洗钱信息中心报告的制度。它是金融机构在预防洗钱活动中所构筑的第三道防线。其中可疑交易报告制度是有关反洗钱国际标准和各国反洗钱法律都有规定的防范洗钱活动的核心措施。

7. 金融机构应保存客户身份资料和交易记录的期限是多少？

(1)客户身份资料，自业务关系结束当年或者一次性交易记账当年计起至少保存5年。(2)交易记录，自交易记账当年计起至少保存5年。

8. 反洗钱工作会不会侵犯个人隐私和商业秘密？

不会的。《中华人民共和国反洗钱法》重视保护个人隐私和企业的商业秘密，并专门规定对依法履行反洗钱职责而获得的客户身份资料和交易信息要予以保密，非依法律规定，不得向任何组织和个人提供。同时，反洗钱行政主管部门和其他依法负有反洗钱监督管理职责的部门、机构履行反洗钱职责获的客户身份资料和交易信息，只能用于反洗钱行政调查；司法机关依法获得的客户身份资料和交易信息只能用于反洗钱刑事诉讼。

一、反洗钱知识问答

9. 洗钱活动有哪些途径或方式？

常见的洗钱途径或方式有：

- ◆ 通过境内外银行账户过渡，使非法资金进入金融体系；
- ◆ 通过地下钱庄，实现犯罪所得的跨境转移；
- ◆ 利用现金交易和发达的经济环境，掩盖洗钱行为；
- ◆ 利用别人的账户提现，切断洗钱线索；
- ◆ 利用网上银行等各种金融服务，避免引起银行关注；
- ◆ 设立空壳公司，作为非法资金的“中转站”；
- ◆ 通过买卖股票、基金、保险或设立企业行各种投资活动，将非法资金合法化；
- ◆ 通过购买彩票进行洗钱；
- ◆ 通过购买房产进行洗钱；
- ◆ 通过珠宝古董交易和虚假拍卖进行洗钱。

10. 谁是洗钱活动的受害者？

洗钱为犯罪分子转移和掩饰非法资金、使不法分子达到占有非法资金的目的，从而帮助、刺激更严重和更大规模的犯罪活动。洗钱活动严重危害经济的健康发展，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。洗钱活动造成资金流动的无规律性，影响金融市场的稳定。洗钱活动损害合法经济体的正当权益，破坏市场微观竞争环境，损害市场机制的有效运作和公平竞争。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和运营风险。洗钱活动与恐怖活动相结合，还会危害社会稳定、国家安全并对人民的生命和财产形成巨大威胁。

目 录

- 一、 反洗钱知识问答
- 二、 *保护自己，远离洗钱*
- 三、 常见洗钱案例

二、保护自己，远离洗钱

1. 远离网络洗钱陷阱

截至目前，我国网民数量已高达5亿多人。在我们获得网络时代的快捷信息和高效沟通的同时，不法分子也利用网络快速传播非法信息，在更广的范围内从事违法犯罪活动。近年来破获的网银诈骗、互联网非法集资等网络洗钱案件警示我们，对于网络信息要仔细甄别，不要轻易通过网银、电话等方式向陌生账户汇款或转账；对于网络信息要时刻警惕，不可因贪占一时便宜而最终落入骗局。

2. 选择安全可靠的金融机构

合法的金融机构接受监管，履行反洗钱义务，是对客户和自身负责。根据我国《反洗钱法》规定，金融机构在履行反洗钱义务中获取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，确保金融机构的隐私权和商业秘密得到保护。

网上钱庄等非法金融机构逃避监管，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，而且无法保障客户身份资料和交易信息的安全性。一个为您频繁“通融”、违规经营的网上钱庄可能也为犯罪分子提供便利，让犯罪的黑手染指您的账户。您能放心让这样的网上钱庄帮您打理血汗钱吗？

选择安全可靠、严格履行反洗钱义务的金融机构，您的资金和个人信息才更安全。

二、 保护自己， 远离洗钱

3. 不要出租或出借自己的身份证件

- ◆ 出租或出借自己的身份证件，可能产生以下后果：
- ◆ 他人借用您的名义从事非法活动；
- ◆ 可能协助他人完成洗钱和恐怖融资活动；
- ◆ 可能成为他人金融诈骗活动的“替罪羊”；
- ◆ 您的诚信状况受到合理怀疑；
- ◆ 因他人的不正当行为而致使自己的声誉和信用记录受损。

4. 不要出租或出借自己的账户、银行卡和U盾

金融账户、银行卡和U盾不仅是您进行金融交易的工具，也是国家进行反洗钱资金监测和经济犯罪案件调查的重要途径。贪官、毒贩、恐怖分子以及其它犯罪都可能利用您的账户、银行卡和U盾进行洗钱和恐怖融资活动，因此不要出租或出借自己的账户、银行卡和U盾既是对您的权利的保护，又是守法公民应尽的义务。

5. 不用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法之一。有人受朋友之托或受利益诱惑，使用自己的个人账户（包括银行卡账户）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。请您切记，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。

目 录

- 一、 反洗钱知识问答
- 二、 保护自己，远离洗钱
- 三、 **常见洗钱案例**

1-非法经营POS机提现

1



信用卡套现

黄先生

在线联系

手机:XXXXXXXXXX

网址:www.taoxianxinyongka.com

1.自2007年11月22日起,朱某利用伪造证件申办“××经营部”、“××服务部”、“××书店”POS机3台,并雇佣多名员工,在网上发布POS机套现信息。

2.朱某采用分散套现信用卡、分散交易金额及分散转入POS机“三分散”方式,试图掩饰非法套现犯罪活动。



2

3



3.朱某将套现资金从公司账户转入个人账户,立即通过网上银行转出或ATM提取,将套现资金付给“客户”,当天账户几乎不留余额。

4.朱某为十余名信用卡持卡人套取现金约672.4万元。2011年3月25日,山东省某市中级人民法院依法宣判被告人朱某犯非法经营罪,判处有期徒刑3年,缓刑3年,并处罚金8万元。



4

2-虚假的网上支付

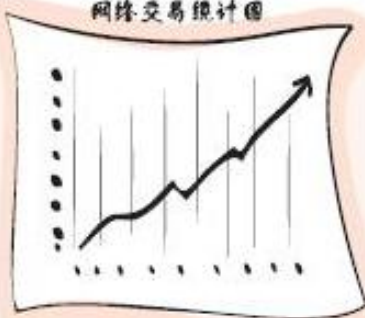
1



1. 王某在工作中获得了大量个人信息和信用卡申请表，通过伪造签名、篡改联系电话和账单地址，王某冒领他人数十张信用卡。

2. 王某指使梁某冒用他人身份证件开立多个网上支付账户和网上店铺，王某则以冒领的信用卡大肆刷卡“购物”。

网络交易统计图



2

3



3. 梁某收到资金后迅速转入多个第三方支付平台账户，再汇集到梁某、王某持有的银行卡账户中，完成洗钱。

4. 多名信用卡所有人收到银行催款通知或发现信用不良记录后，纷纷向公安机关报案。最终，王某因金融诈骗罪获刑，梁某因洗钱罪被起诉。



4

3-不翼而飞的网银巨款



1. 张先生的手机收到一条短信，提示他的网银需要升级。张先生立即登录短信提供的网址，进行操作。

一旦用户在“钓鱼网站”上进行操作，犯罪分子就可以通过木马程序窃取用户的账号和密码。

2. 两天后，张先生再次登录网银准备给家人汇款时，发现账户中的上百万元已不翼而飞！警方调查发现，这是一个典型的“钓鱼网站”诈骗案。



3. “钓鱼网站”与真正的银行官方网站非常相似。

4. 犯罪分子利用窃取的用户账号和密码登录网上银行，将受害者资金转到其所控制的账户，并通过ATM多次提现，完成洗钱。



4-麻烦不断的网上钱庄汇款

1



1.2010年以来，杜女士在海外务工的丈夫因某地下钱庄手续费低廉，多次通过其将收入汇回国。

2.2011年杜女士的丈夫又汇出一笔钱，但杜女士却迟迟没有收到。同时，该地下钱庄在网上的频繁操作引起了警方怀疑。



2

3



3.警方调查发现，该地下钱庄利用海外汇款业务为犯罪分子清洗黑钱，杜女士也因涉嫌洗钱，多次受到警方询问。

4.虽然杜女士最终消除了嫌疑，但着实虚惊一场。



真没想到被卷入洗钱，老公的辛苦钱差点就回不来了!

4

5-老乡熟人的网上洗钱圈套



1. 香港人程某以好处费为诱饵，指使沈某回老家组织他人办理多张信用卡。



2. 沈某通过其兄沈A找老乡熟人共办理信用卡280余张。



3. 程某和沈某通过各种网上支付和交易进行洗钱，涉及账户交易达120亿元。

4. 某地人民法院依法对被告人沈A、沈某和程某（香港）进行宣判。



6-网络诈骗的集资通道

1

××公司经营房地产、生态农业开发等项目，收益可观，现募集项目开发资金，每月5%—10%的回报。本金两年后随时可归还。



1. 李某在网上发布高息借款信息，谎称经营各种高收益项目。李某常在第一笔借款后按时偿还本金和高额利息，在获取他人信任之后，即以各种理由拒绝兑现借款承诺。

我账户上的钱已经上亿了。哥，你这招真好使！

2. 赵某在明知李某进行网络诈骗的情况下，仍然将自己的账户交给李某使用，用于接收各种受骗款。



2

我不会亏待你的！

3



3. 赵某用银行账户的钱代李某购买别墅、商铺和住宅。

这罪名也一人一个，还真不“亏待”我啊！

4. 案发后，李某因非法吸收公众存款罪被判入狱，赵某也因洗钱罪获刑。



4

7-彩票中奖的玄机



8-非法集资借道房地产

我的利息是银行利息的两倍。看看，这儿还有红头文件哩。



1. 张某打着为“国家重点工程集资”的幌子，大量伪造政府公章、红头文件，向多个省市的社会民众非法吸收存款上亿元。

我账户上的钱已经上亿了。哥，你这招真好使！



2. 叶某在明知张某资金为非法吸收的公众存款的情况下，将银行账户借给张某使用。

我不会亏待你的！



3. 叶某利用自己的银行账户，代张某购买别墅、商铺和住宅。

这罪名也一人一个，还真不“亏待”我啊！



4. 案发后，张某因非法吸收公众存款罪被判入狱，叶某也因洗钱罪获刑。

9-身份证被盗用阴差阳错成网上逃犯

因为被盗用了身份证，在短短4个月时间内，某市的曲先生先后两次被江苏、上海两地警方当成网上逃犯“抓获”。这一系



列麻烦只因曲先生在春节前一次醉酒后弄丢了钱包和身份证。尽管他马上在报纸上刊登了身份证遗失证明，并在当地公安局补办了身份证，但遗失的身份证还是被犯罪分子盗用。由于犯罪嫌疑人至今未被抓获，曲先生还不得不一再向警方进行解释。

提醒：小提醒：

居民身份证是证明居民身份的有效证件，具有特定的法律意义和效力。随着社会交往和社会经济的快速发展，身份证的使用频率越来越高，因身份证保管、使用或管理不当而引发的各类案件和纠纷屡屡发生。大家应妥善保管身份证，丢失后要及时向公安机关报告，同时登报挂失。在曲先生的事件中，由于他及时挂失登报，最起码有了向公安机关解释的依据。

此外，身份证具有很强的法律证明力，经常被法院视为判断利益归属主体的依据，因此，身份证一旦被盗用，很可能因为没有其他证据而判身份证主人承担相应的法律责任。

10-假警察查洗钱诈骗1

2009年3月15日，休息在家的李女士接到一个语音提示电话称：“您的电话6252……已欠费，我们准备给您停机，如有疑问请按9选择人工服务。”李女士从未申请过该电话号码，但仍按了“9”键。电话被转接，一名自称电信局工作人员的男子详细询问了李女士姓名、身份证号后，告诉李女士可能遇到诈骗了，并称已将电话转接至公安机关。

随后，一名自称北京市昌平公安分局经济案件侦查队民警“高军”的男子打来电话，在自报姓名和警号后，“高警官”说：“你

10-假警察查洗钱诈骗2

的名下确实有这个号码，用来扣费的招商银行卡涉入一起全国性洗钱案。”随后，“高警官”把电话转到“反洗钱中心”，一名自称中心主任的男子警告李女士：“您的账号涉案将被冻结，否则钱会被犯罪分子转走。”“中心主任”表示，如果希望财产不被冻结，必须在当天下午1点前把钱转到安全的账户内。

这一番编织严密的骗术果然取得了李女士的信任。随后，李女士在“中心主任”的电话遥控下，通过ATM把几张银行卡中共计259万多元的现金全部转到了“中心主任”指定的“安全账户”。在操作完成后，“中心主任”称48小时后他会同李女士联系，并要求李女士绝对保密，否则若影响案件破获，后果自负。

两天后，“中心主任”没有联系李女士，李女士才意识到上当受骗了，只得赶紧报案。



10-假警察查洗钱诈骗3

此类诈骗案件的主要特点是：

>>

- 诈骗分子一般选择独自在家的老年人为行骗目标；
- 使用语音电话提示后转接人工的方式，市民往往会习惯性地相信通话对象就是电信工作人员；
- 诈骗分子往往冒充警察、电信公司或其他政府机构工作人员多次给事主打电话，设下层层圈套；
- 诈骗分子往往利用事主对ATM不熟悉的特点，要求事主在转账界面输入一组所谓密码确认，而这组密码实际上是被骗取的金额。



TF 小提醒：

公众在接到类似电话时，可以通过下列三个渠道核实信息：

- 拨打电信公司统一客服电话进行核实；
- 通过当地公安分局的值班电话对“民警”身份进行核实；
- 拨打银行统一客服电话，向银行进行咨询。

一定要做到不轻信，不盲从！



一生保障 | 在你左右