证券违法典型案例报道选·编

2010 年编

经济管理出版社

第八章　其他案件报道

导　　读

随着互联网技术的日益发展和普及，一些传统的违法犯罪行为也逐渐改头换面，呈现出网络犯罪的新特点。盗窃证券账户就是这样一种新型盗窃犯罪行为，其典型作案流程为：不法分子通过向投资者计算机种植木马病毒，伺机窃取投资者账户密码，然后操控投资者账户，与自己控制的账户之间反复对敲交易某些证券，赚取价差，把投资者账户的资产，蚂蚁搬家式地倒腾到自己控制的账户，致使投资者在不知情的情况下蒙受损失。

虽然作案手法与传统犯罪形式截然不同，但盗窃证券账户依然构成了《中华人民共和国刑法》第二百六十四条所规定的盗窃罪，是不折不扣的犯罪行为。不法分子窃取他人资金账号及交易密码后，在他人不知情的情况下高价买进或低价卖出某一股票，同时自己账户低吃高抛同一种股票从中获利。在主观上，是为了通过盗买盗卖股票非法占有被害人的财产；在客观上，是在被害人不知情的情况下，非法占有了被害人的财产，符合盗窃罪的构成要件，应当依法追究刑事责任。

盗窃证券账户行为破坏正常的交易环境和秩序，直接损害投资者利益，性质恶劣，危害性很大。并且，此类行为利用高科技手段，作案手法隐蔽，不法分子反侦查能力较强，对监管和调查人员提出了更高的要求。对于伸向证券市场的黑手，证券监管部门高度警觉，建立了一整套发现、预警、监管和执法机制，做好了相应的准备，并会同公安机关快速反应，密切协作，及时查处盗窃证券账户案件，切实保障投资者的合法权益。

在互联网应用日益普及的今天，投资者在享受网上交易方便、快捷的同时，也应对网络安全保持必要的警觉，防患于未然。在使用过程中，应小心避免电脑被植入木马程序，切勿将账户密码设置得过于简单，避免长期使用一个密码不更换。一旦发现账户被盗，应在第一时间报案。同时，证券期货经营机构也可积极开发一些新的技术和服务保障措施，比如采取U盾、认证卡等措施，切实保障网上交易和投资者账户的安全。

附：有关法律规定

《中华人民共和国刑法》

第二百六十四条 盗窃公私财物，数额较大或者多次盗窃的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；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；有下列情形之一的，处无期徒刑或者死刑，并没收财产：

（一）盗窃金融机构，数额特别巨大的；

（二）盗窃珍贵文物，情节严重的。

《最高人民法院关于审理盗窃案件具体应用法律若干问题的解释》（法释［1998］4号）

第三条 盗窃公私财物，“数额较大”、“数额巨大”、“数额特别巨大”的标准如下：

（一）个人盗窃公私财物价值人民币五百元至二千元以上的，为“数额较大”。

（二）个人盗窃公私财物价值人民币五千元至二万元以上的，为“数额巨大”。

（三）个人盗窃公私财物价值人民币三万元至十万元以上的，为“数额特别巨大”。

第四条 对于一年内入户盗窃或者在公共场所扒窃三次以上的，应认定为“多次盗窃”，以盗窃罪定罪处罚。

编者按：

世间万物，有其利，必有其弊，互联网也如此。如今信息时代，网络让人们沟通无限，但网络安全问题随之而来，网银失窃、虚拟货币失窃、私密信息泄露，甚至连网络菜园里的白菜被盗等事件已有发生。在证券市场，投资者享受着网络交易的便捷，但证券账户安全性同样面临新挑战。

据悉，我国证券市场起步晚，但快捷程度全世界领先。在证券交易系统设计、开发、维护和升级的过程中，安全性始终是诸多考虑因素中的关键因素之一，在监管规则制定的过程中，交易安全制度保障始终是硬条条，在证监会“三位一体”的执法体制中，任何涉及交易安全的线索都将引起一系列快速、标准监管动作。可以说，我国资本市场对网络盗窃早已重视并张网以待。2009 年春天，就有那么一伙人以身试网，结果被逮个正着。

故事起源于证券交易所监控室实时监控系统自动抓捕到的一起异常交易。报警声响起不久，线索报告送到证监会稽查局，经当地证监局、公安部门密切协作，犯罪嫌疑人现场被逮，随后，犯罪团伙主要成员归案。经司法机关缜密侦查，认定犯罪嫌疑人违法交易达 2300 多万元，盗买获利达 105 万余元。人们即将看到的是，犯罪分子或将被处于无期徒刑的判决。

记者近日走访上海证券交易所、证监会有关部门、湖北证监局、荆州公安局等办案机构，并采访有关办案人员，解析案情以警戒市场参与者、增强投资者自我防护意识。

伸向证券账户黑手——熊冬冬团伙盗窃案始末

《21 世纪经济报道》于海涛　上海、武汉、北京报道

网络菜园里的白菜被偷了，可能影响你的情绪，或许会想办法再种上。如果你证券账户被人盯上了，恐怕就有大麻烦了。

上海股民杨先生就遭遇到了这种事。当他在 2009 年 2 月 18 日查询资金账户时发现，账上的数十万元资产已不翼而飞，只剩下了几百元！

“通过向投资者计算机种植木马病毒，伺机窃取投资者账户密码，然后操控投资者账户，与自己控制的账户之间反复对敲交易某些证券，赚取价差，

把投资者账户的资产，蚂蚁搬家式地倒腾到自己控制的账户”，刚刚侦破了“熊冬冬”团伙盗窃证券账户案件的荆州市公安局网侦支队政委李恩忠对记者说。

荆州警方提供的数据显示，目前已经查实，“熊冬冬”团伙控制的账户分布于湖南、湖北两省的多个地区，交易证券金额高达2370余万元，从中获利105万余元。

此案的最新进展是，2009年12月7日荆州市检察院已经送达荆州市中级人民法院提起公诉，建议对主犯判决刑期为无期徒刑。本月底开庭审理。

一、结网捉贼

4月27日上午10时52分，上海证券交易所实时监控系统警报急促响起：某证券交易价格一分钟内涨幅达9.6%，成交价格异动明显。

“监控人员随即查看交易记录，发现华泰证券荆州某营业部交易的‘方××’账户低买高卖获利，其交易对手方是国泰君安证券郑州花园路营业部交易的‘孟××’账户高买低卖发生亏损，初步判断，交易行为疑似同一人控制，作案分子可能就是我们跟踪多时的涉嫌盗窃他人账户人员。”上交所市场监察部人士对记者说。

按照证券执法协作机制，上交所立即采取行动。一方面，立即向中国证监会报告相关情况，在证监会的统一协调下，向作案地所在的湖北证监局、当地公安部门通报刚刚发现的新线索并建议其立即采取行动。另一方面，即刻通知被盗方账户交易所在的证券营业部，要求其立即联系客户，确认账户被盗用情况，建议其采取有效措施防止被盗用事态进一步扩大，并及时向警方报告情况。同时，上交所还通知涉案账户交易指定证券营业部，密切跟踪账户交易动向，着手准备客户开户资料、交易IP、资金账户资料等相关材料。

“接到上交所和稽查局的电话，局领导非常重视，迅速反应，立即作出全面部署。”湖北证监局相关人士对记者说。

一是立即将此新情况通报给了湖北省公安厅，并请求迅速侦查，力争尽快破案；二是迅速向华泰证券荆州该营业部有关负责人了解相关情况，并明确要求对涉嫌盗用账户进行实时监控；三是协调该营业部及时向荆州警方反映情况，积极配合警方行动。

承办此案的湖北荆州市公安局网监支队，经过缜密调查，发现“方××”账户网上登录地址是：荆州市荆州区“天佳”网吧。

时钟的指针指向上午11：35，一张大网已经织成，捉贼行动开始。

“等我们赶到网吧，嫌疑人已经溜了!”负责此次行动的“总策划”——荆州市公安局网监支队政委李恩忠对记者说：“我们继续监控‘方××’账户，发现其在下午2：45又在沙市区‘九州网城’网吧上线十分钟，遗憾的是，等我们赶到，又下线了!”

“为避免打草惊蛇，湖北证监局与证监会稽查局汇报后，建议华泰荆州营业部先不要冻结‘方××’账户的资金划转，全力以赴地配合荆州警方的侦破工作。”前述湖北证监局人士表示，在当日上午收市时，“方××”账户已被荆州警方和华泰荆州营业部监控。

当天行动无果，荆州网监支队连夜召开紧急会议。“会上我提出，不能只盯着证券交易时的IP，因为证券交易部门提供的IP，有延时情况，定位后赶到现场为时已晚，重要的是盯住他的资金转移。”李恩忠说：“随即，我们联系了‘方××’账户资金存管的当地工商银行，对资金账号进行了监控”。当晚，警方兵分四路，分别监控工商银行账户异动、作案账户交易所在营业部、荆州区和沙市区相关网吧。4月28日上午8时48分，银行侦查组发现目标——嫌疑人正在某ATM机取款。结果毫无悬念，嫌疑人熊冬冬在取款现场被抓获。

二、“三枪”累犯

“交易所、稽查局、证监局、公安机关的‘四位一体’协同作战机制在这个案子的查处过程中效率非常高，各个环节衔接非常顺畅。”湖北证监局相关人士说。

实际上，抓捕行动只是执法过程中的精彩情节之一，对证券账户盗窃的跟踪早已开始。

2009年2月，上海证券交易所监控发现，托管在华泰证券荆州某营业部的“赖××”账户，从对手方低价买入、高价卖出证券，获利较大，对手方则低价卖出、高价买入该证券，亏损严重，其交易行为导致该证券价格异常波动。初步判定，这一行为可能涉嫌盗窃他人账户资金。上海证券交易所立即安排专人关注此类异常交易。

收到上海证券交易所的报告以后，证监会稽查局立即将线索交给湖北证监局进行非正式调查，并要求一旦发现涉嫌犯罪的证据，立即通报司法机关尽快介入。

湖北证监局的调查结果显示，2 月 11 日，赖××在华泰证券荆州某营业部开立证券账户，并于次日存入资金 5000 元。

“2 月 16 日至 18 日，赖的账户频繁通过网上下单，表现为从固定交易对手方低价买入、高价卖出证券，而其交易对手方则低价卖出，高价买入证券，赖的账户获利较大，而交易对手方账户亏损严重。”前述湖北证监局人士说。

相关交易资料显示，“赖××”账户的交易对手方有 7 个账户，分别托管于全国各地，如国联证券上海邯郸路某营业部、中信建投江西吉安市井冈山大道某营业部等 7 个不同的营业部，而其下达交易指令的 IP 地址与赖的账户交易的 IP 地址基本一致，均为湖南常德（与湖北荆州毗邻）。

经向上述营业部核实，上述 7 个账户都不是本人操作。也就是说，“赖××”存在盗用他人账户交易的嫌疑。

3 月 2 日，根据《中国证券监督管理委员会、公安部关于在打击证券期货违法犯罪中加强执法协作的通知》有关规定，湖北证监局正式以局函将有关情况通报湖北省公安厅，请求公安机关依法立案侦查。

湖北省公安厅研究决定，案件由湖北荆州公安局侦查，最后确定由该局网监大队承办。

经证监会稽查局协调，交易所、湖北证监局和荆州警方建立了直接通报情报和密切协助执法的工作机制。

然而，窃贼却丝毫没有停手的表示，接下来的行为几乎疯狂。

3 月 15 日，上海证券交易所再次发现，托管在广发证券武汉民权路营业部的“陈××”账户出现与“赖××”账户类似的异常交易情况。经证监会稽查局协调，湖北证监局及时督促该营业部向警方反映情况，并启动紧急预案，对“陈××”账户交易、转托管、资金存取实行全面限制，成功制止犯罪嫌疑人取款。

“至 4 月 27 日，方××账户报警后，相关人员分析整理作案手法，基本确定该起事件与前几起事件可能系由同一人作案，有关情况立即通报了证监会稽查局、湖北证监局和当地警方。”前述上交所市场监察部人士对记者说。

实践证明，如此判断是正确的。

4 月 28 日，犯罪嫌疑人在取款时被抓现行，经审讯，自称熊冬冬。因此，在证监系统，此案正式命名为“熊冬冬团伙盗窃证券账户案”。

6 月 2 日，案件另外犯罪嫌疑人李伟、许敏被警方抓获。

三、2300 万：105 万的收益

根据熊冬冬的交代，他们是一伙人在做这个事，而他只是负责取钱，另外四名同伙分别是：李伟、许敏、管杰、陈建华（后两者目前在逃），其中李伟是主谋。

“他们分工比较明确，有在网上种植木马病毒的，有操作证券账户买卖的，还有专门负责取钱的”，李恩忠介绍说：“这些人之间都以见面方式进行联系，联络方式很原始，从不打电话，连公用电话都不用。”

李伟把这种方法叫做“拉登模式”，意指拉登被美军跟踪卫星电话信号轰炸过之后就再也不用任何通信设备，从而使自己在信息时代处于最原始的安全境地。

在此思路下，几人虽然在网络进行盗窃，但从不使用 QQ 和其他网络即时通信工具，不玩网络游戏，每次上网时间极短，“很难找到行踪”。

具备如此“高智商”的反侦查能力，令人惊叹！然而，记者从警方提供的资料看到，目前已经被逮捕的李伟、熊冬冬、许敏三人均是湖北省石首市人，二十岁左右，初中文化程度，无业。

“李伟是主谋，别人不知道怎么搞（用种植木马盗窃账户密码），是他提出来的，之前也因犯盗窃罪被深圳市南山区人民法院判处有期徒刑两年，刚刚刑满释放，出来就又开始干了。”李恩忠说。

据李伟向警方交代，他们选择账户有几个标准：一是不经常使用，以避免在短时间内被发现；二是账户上的钱数相对较多，至少要有几十万元，这样才方便买卖证券并产生价差以获利。

交易记录显示，在 2009 年 2 月 16 日至 18 日三个交易日中，“赖××”账户按此交易方式循环操作，与盗用账户发生 11 个品种的交易，累计买入 606 手，卖出 606 手，交易金额 680586.90 元，获利 50610 元（未计算交易成本）。

而来自荆州警方的数据显示，几个月时间内，熊冬冬团伙用盗取的账号共交易 21198 手，买卖金额高达 23730411 元，从中获利 1057613.4 元。

7 月 31 日，荆州市公安局将此案移送荆州市人民检察院审查起诉。

12 月 7 日，荆州市检察院向荆州市中级人民法院正式提起诉讼。

四、定性盗窃或刑至无期

“我们是以盗窃罪的罪名来起诉的。”荆州市检察院起诉处李涛处长对记者说，鉴于此案数额巨大，直接向荆州市中级人民法院提起诉讼。

实际上，在调查过程中，荆州警方曾提出两项罪名：输入计算机病毒罪、盗窃罪，但最终移送审查起诉时只保留了盗窃罪一个罪名。

“嫌犯人的目的是盗窃别人密码，最终盗窃资金，不是为了输入计算机病毒，输入病毒是达成最终目的的手段行为，同时也符合秘密窃取他人财物的构成要件。”李涛解释说。

至于刑期，由于盗窃数额巨大，检察院建议应处无期徒刑，是按照相关法规规定的最重情节的处理。

在熊冬冬团伙盈利的 105 余万元中，现金共计 40 多万元，已全部挥霍，其余资金被控制，属于盗窃既遂。

对于盗窃数额是否达到“特别巨大”的标准，由于各省区经济发展不平衡，故认定范围也不一致。如在高法的相关司法解释中，中部地区划定的基本范围是十五元到三十万元，湖北地区取了中间值，以十八万元为界限。显然，此案应属盗窃数额特别巨大。

“比如第一被告李伟，是犯意的提出者，在案件中负主要责任，同时在深圳因同一罪名盗窃罪被判过刑，五年之内重新犯罪的是累犯，应从重处罚”，李涛说：“当然，此案有点特殊，普通盗窃最高刑是无期，从重也只能从到无期。”

对熊冬冬和许敏，检察院建议处十年以上有期徒刑至无期徒刑。

值得注意的是，此案在检察院审查阶段曾两次退回公安补充侦查，原因是盗窃金额的计算方法不一致，以致盗窃数额不同。

目前盗窃数额有三种计算方法。

一是最简单直接的方法，即以被盗窃人账户的原有数额，直接减掉余下数额，即算做盗窃金额，不管中间差价和流失。

“这种计算方式比较简单，但弊端是，实际被告人占有的不一定是这个数额，（采用这种计算方式）对保护被告人的合法权益做得不够，对被告人

是十分不利的。”李涛说。

公安第一次移送审查时即以此种方法计算，后经充分沟通后换了第二种计算方法，即嫌疑人账户上盗窃后的钱和原始的钱之差，为盗窃数额。

第三种计算方式是扣减交易过程中的税收等流失，相对复杂，采用得不是很多。

12 月 7 日，荆州市检察院将此案送达荆州市中级人民法院进行起诉，法院已经受理，并将择日公开庭审。

“四位一体”联动　严打盗窃账户

《21 世纪经济报道》　于海涛　上海、武汉、荆州报道

随着熊冬冬团伙盗窃证券账户案的公开审判，利用木马病毒盗窃证券账户信息的真相，即将走进人们的视野。

来自湖北警方的信息显示，“熊冬冬”一案，涉及被害人分布在全国 11 个省，损失金额十分巨大。

“目前，我国证券市场网上交易金额总量占了同期市场交易总量的绝大部分，上述违法行为危害到资本市场正常交易秩序，损害了广大投资者的合法权益，属于依法重点打击的违法犯罪行为之一。”负责协办此案的湖北证监局相关人士说。

上海证券交易所相关部门负责人表示，本起案件的成功告破，证监系统与公安部门密切合作、快速联动是核心，证监系统内证监会、地方证监局、交易所三位一体快速反应是关键；证监人员和公安干警高度的责任心和良好的专业技能是保证。

可以预见，经过这次实战以后，对维护资本市场交易秩序，证监会、交易所、派出机构、公安机关之间的“四位一体”的联动机制将更有效。

一、交易所：敏锐发现

“熊冬冬团伙倒腾资金的手法是对敲，打价格差，殊不知，这恰好是把自己直接暴露在监控系统的电子眼之下。”一位上交所市场监察部人士说。

据介绍，我国交易所已建有专门的系统和机制，负责对涉嫌短线操纵、内幕交易等违法违规交易行为进行监控，快速发现、报告及反应的能力极强。在这方面，世界其他发达国家的资本市场很难达到这种水平。

首先是建有证券交易实时监控系统，具备报警发现能力。

此系统以报警驱动为主动牲，针对不同短线操纵手法，设计了不同的预警指标。这些预警指标涵盖了多类产品的多种短线操纵场景，具备及时发现市场操纵行为的能力。

“比如一下子有一个单子进来突然把价格改变达到设定数值，这个系统就报警，每天有一个团队做实时监控，发现可疑账户就会深入分析。而实时监控系统对（成交）价、（交易）量方面都设有相应指标，发现明显异常就会报警。”前述上交所市场监察部门人士说：“对这个系统来说，对敲这种作案手法很容易被盯上。”

熊冬冬案即属此类，当某些证券品种突然出现价格异常变动，且交易对手方为固定账户，自然难逃“电子眼”的巡察。

其次，交易所建有证券异常交易分析系统，具备分析报告能力。即在及时发现异常交易行为时，从中捕捉违法违规线索。

为此，上交所建立了证券异常交易数据分析系统，专门开发了针对各种短线操纵模式的分析模块，并在此基础上，不断进行总结并完善分析指标体系。

“很多行为的表现方式是一样的，比如都是股价异常波动，但有的是内幕交易，有的是操纵市场，还有其他的，比如盗买他人账户资产，要经过分析才能初步确定。”前述上交所人士称。

初步确定异动原因后，交易所即启用“监管综合干预措施”，主要目的是及时制止相关违法违规行为，以避免更大损失。

目前来看，对证券异常交易行为，上交所具备监管干预的手段和权力，包括口头提醒、书面警示、约见谈话、限制账户交易权限以及上报证监会查处等。

如熊冬冬案，在对赖××、陈××、方××等账户频繁与对手方买卖证券，导致成交价格异动后，交易所即协调相关营业部对上述账户的账户交易、转托管、资金存取等实行全面限制或监控，以成功制止犯罪嫌疑人取款，便于公安人员追踪嫌疑人踪迹。

二、证监会稽查局：运筹帷幄

“交易所定期和不定期都会有大量的监察报告报证监会稽查局，证监会稽查局安排专人受理、甄别和处理，所有的工作已经形成比较规范的程序。”一位监管部门人士对记者说，比如，涉嫌内幕交易或市场操纵的，有的启动非正式调查程序，有的直接启动立案稽查程序，非正式调查案件和立案稽查案件由派出机构和稽查总队实施调查。

熊冬冬案，在几个账户与一个账户之间发生对倒行为，最后的结果是资金以交易的形式流向另一账户，如果交易属于双方自愿，可能涉及利益输送，如果一方不知情，可能涉嫌盗窃。综合有关线索，盗窃的特征比较明显。

前述监管部门人士表示，与其他异常交易相比，从单次交易获利来说，熊冬冬案金额不算大。但是，这种违法行为的危害后果很严重，直接威胁投资者的信息，因此，从一开始，证监会稽查局就很重视这类线索。

该人士介绍，在2月上交所将“赖××”账户与7个交易账户进行对倒盈利的相关线索报至证监会稽查局后，证监会稽查局立即转至湖北证监局，请其及时采取行动，并与公安机关联系查处此事。至3月，托管在广发证券武汉民权路营业部的陈××账户出现与赖××类似的异常交易情况。

“当时的判断是很可能是同一伙人，开户都在湖北，为避免给投资者造成更大损失，稽查局立即协调湖北证监局及时督促相关营业部向警方反映情况。”前述人士说。

在上述人士看来，为提高执法效率，证监会稽查局在此案中创立了一种“简便程序”，实行情报传输的直接对接，即经稽查局统一协调后，交易所、湖北证监局和湖北警方建立了联系人制度，沟通、通报和协助实现无缝对接，保证了执法力量在无障碍运转的机制下以最短时间打击涉嫌盗窃者。

“从敏锐判断案件性质到确定一切工作围绕‘抓人’这个中心看，证监会稽查局干得的确很漂亮。”上述人士说。

在4月27日上交所监测到“方××”账户在以同样手法对倒相关证券时，该账户下单时间是10：52，而荆州警方在定位到该账户上网地址是某网吧，并赶至该地的时间是11：35。

43分钟，创下了从交易所发现线索到公安机关赶到犯罪现场的最短纪录。

三、派出机构：强力执行

“总结这起案件，证监会稽查局、地方证监局、证券交易所及证券经营机构各负其责、联动监管、快速反应的防范工作体系，和相关处理工作流程是十分有效的。”前述湖北证监局人士说。

在他看来，各环节的无障碍联动是“熊冬冬”案得以迅速告破的关键。

据介绍，湖北证监局接到此案线索后，相关领导立即研究，并作出具体部署为：一是立即将此情况通报给了湖北省公安厅经侦总队，并请其协调荆州市公安局组织人员迅速侦查，力争尽快破案；二是迅速向华泰证券荆州营业部有关负责人了解相关情况，并明确要求对涉嫌盗用账户进行实时监控；三是协调华泰证券荆州营业部及时向荆州警方报告；四是实时保持与上交所监察部、华泰荆州营业部及荆州市公安局等单位密切联系，随时掌握案情最新动态。

实际上，在追踪“方××”账户之前，相关各方已经过实战磨合，期间也经历过了各环节的逐步沟通和统一认识的过程。

“赖××这个案子是湖北局接手的第一起非法盗买账户的案子，有非常典型的意义，犯罪分子如果得不到应有的惩罚，投资者利益就得不到保障，由此引发风险不得了，因此，湖北局在致公安厅的函中，请求公安部门集中力量把这个事情当个大事来抓，迅速破案。”前述湖北证监局人士说。

同时，湖北局成立了专案组，赶赴荆州，与警方沟通相关证券交易的专业知识，并协助提供交易记录、相关线索，以及与交易所等部门及时沟通。

3 月“陈××”账户异常情况发生以后，交易所、湖北局、公安机关的协作配合就顺畅许多，至 4 月“方××”出现，在几乎“无缝对接”的全方位监管体系网下，仅经过一天时间，即抓获了熊冬冬。

“协同监管机制发挥了较好作用，交易所同志迅速提供材料，湖北局按稽查局指示，及时与公安联系，所有工作突出特点是快，为案子的破获创造了良好的条件。”前述人士说。

在他看来，查办此类案件有些做法值得总结，比如证监会稽查局在接到交易所监管专题报告后，可立即转发给相关派出机构对涉嫌盗用他人账户进行交易、非法牟利的行为进行调查取证，派出机构也要在第一时间通报当地省级公安部门，请求公安部门的支持和配合。

同时，派出机构要对涉嫌盗用他人账户客户开户托管的营业部对可疑账户实施实时监控，着手准备客户开户资料、交易 IP 地址、交易流水、资金流水等相关材料，全力配合调查。

此外，进一步健全和完善证监系统与公安部门密切配合、协同办案的工作机制也很必要。

“派出机构及时向当地公安部门通报情况，在搜集整理固定了相关涉嫌违法违规的证据后，立即移送公安部门立案查处。交易所及相关证券经营机构也要全力配合当地公安机关的调查取证工作，并为其提供相应的技术支持。”前述人士说。

四、公安机关：专业战术

熊冬冬案由湖北省公安厅经侦总队转给荆州市公安局经侦支队后，经分析，认为是一种网络犯罪，即转至网监大队。

“我不炒股，对股票不太了解，（湖北证监局相关人士）跟我说了情况以后我到网上看了一下，才知道有股票的几种交易形式，一般情况（股票交易）是 T + 1，点对点之间是可以对敲的。”专案组主策划、荆州市公安局网监大队政委李恩忠说。

在此认识下，李恩忠初步确定了追踪 IP 地址的作案方案。

首先调取犯罪嫌疑人上网信息，进行技术关联。发现其上网 IP 地址基本集中在荆州城区、公安县、石首市、湖南安乡、湖北武汉、湖北咸宁等附近地区。而对嫌疑账户与对方账户的交易 IP 地址核对发现，大多在一个点上。

“买方和卖方一般不会在一个地方，可以分析出是一个人在自己卖自己收，调过来大量数据是这样的，也有同伙作案的。在异地的，我们做数据重合，就可以知道整个过程，是不是一伙人。”李恩忠说。

4 月 27 日“方 × ×”账户被查到 IP 地址在荆州市荆州区“天佳”网吧，待警方赶到网吧，嫌疑人溜了！下午 2：45 再审该账户又在沙市区“九州网城”网吧上线十分钟，却仍未抓到。

“后来了解到证券交易规则中资金转账必须是 T + 1，第二天才能转账（证券转银行），这给我们以极好的机会。”李恩忠介绍说。

当即李恩忠联系了工商银行，请求对相关账号进行监控，使用“银行卡

报警系统”实施全程定位。

当晚，网监大队做出兵分四路的安排：一路坐镇工商银行监控账户异动；一路安排在荆州区、一路安排在沙市区、一路安排在华泰证券公司荆州营业部。

次日，根据银行卡报警系统的指示，公安人员在取款现场将熊冬冬抓获。

“在侦破的技术难度上说不是太难，但案子很麻烦，涉及证券交易等专业知识，这对公安机关是个挑战。”李恩忠说，随着违法行为和技术的花样翻新，专业知识的欠缺会是影响办案效率的一个至关重要的因素。

同样，此案在与检察院沟通时也遇到这个问题，未审查过此类案件的检察人员也需要重新了解相关专业知识，这在一定程度上也影响了案件审理进展。

网络犯罪高发　法律规制升级

《21 世纪经济报道》　罗诺　北京报道

或许在十年前，人们还无从想象，仅仅通过一个或许与你毫不相干的人点击几次鼠标，你银行户头的“血汗钱”便可能不翼而飞地进入别人的口袋，你的私生活的百态万象便可能成为“大众皆知的秘密”，甚至当你的手机被来自不同区域的电话打爆时，你可能还没有意识到，你已经成了网络犯罪的受害者。

无可争议，计算机和互联网的普及已经改变了世人的生活，同时带来些许隐忧。

目前，利用互联网络犯罪的形式可谓是多种多样，常见的有盗取他人网络账号、密码或虚拟货币、制作传播网络病毒等。还有的将网络作为犯罪场所或媒介，例如建立淫秽网站、发布卖淫信息等。

随着《刑法修正案（七）》以及相关司法解释的实施，规制此类行为有了更具针对性的法律依据。

一、网络犯罪种类繁多

由于通过计算机网络犯罪具有犯罪成本低、传播迅速，传播范围广，智

能性高、隐蔽性强、风险性低、危害性大等特点，利用网络进行金融犯罪的比例正不断升高。

2006 年 7 月开始，国内发生了多起网银账户被盗事件，包括工商银行、农业银行等，还有一些受害者专门成立了“工行网银集体受害者联盟”。

2007 年 5 月 25 日，一些网络黑客潜入湖南省红十字会网站，将上面的慈善账号改为他们进行诈骗的银行账号，现在 6 名涉案人员已经全部被抓获。

2008 年年初，海南省公安网监部门协助安徽警方将一名涉嫌实施 4 宗“网银”盗窃案的年仅 17 岁的犯罪嫌疑人钟某抓获，其涉案金额高达 6 万余元。

2009 年 4 月，某沪上知名公司高管在离职后伪造有关事实，通过黑客、第三方软件入侵的方式，冒用公司高管的邮件地址向公司客户及不特定对象大量发送电子邮件，引起了客户对公司信誉的强烈质疑，给公司带来了很多的负面评价，同时公司的业务也因此造成大量的损失。如此案例，举不胜举。

美国刑法学界把计算机犯罪分为三种：一是计算机滥用，指凡故意或过失以使用计算机的方法致使他人受损失或有损失危险的；二是与计算机相关的犯罪，指任何借助计算机知识以达到犯罪目的的犯罪行为，许多传统犯罪类型，但因为有计算机介入的犯罪大多数属于此类；三是计算机犯罪，指以欺诈或夺取的目的而执行程序，以陷他人于错误或欺诈的目的而获金钱、财产或服务，任何人恶意接近、改变、增减、损坏计算机系统、计算机网络或资料的，均为计算机犯罪，其中包括计算机欺诈、计算机辅助犯罪。

有据可查的世界第一例利用计算机网络犯罪案例产生于 1958 年的美国硅谷，但直到 1966 年才被发现，一位计算机工程师通过篡改程序的方式在银行存款余额上做了手脚，这也是世界上第一例受到法律追诉的计算机网络犯罪案。

而我国的第一起利用计算机网络犯罪案例则发生在 1986 年 7 月 22 日，港商李某在深圳某银行取款时，发现账户上 2 万元不翼而飞，而两个月后，同样在深圳，赵某存入银行的 3 万元港币也从户头离奇蒸发。而此案破获后，得知上述两笔款项均为同一犯罪分子利用计算机知识诈骗而去。

1989 年我国出现了由国内计算机人员开始设计的人为计算机“病毒”，并开始流传，但直到 1996 年中国才破获首例计算机病毒制造案。

正如上述案例所述，除了网络犯罪在犯罪过程中的种种特点外，其在犯

罪之后的侦破过程却又极其艰难。

有分析指出，互联网本身具有跨地域性、跨国界性，没有空间限制。网络信息散布迅速，基本上没有时空限制，影响范围极其广泛，层次极其繁多。而在网上来源网址可以假造，犯罪者身份有可能隐藏起来，加以网络犯罪证据极为有限，其证明力又大打折扣，而且极易被毁灭，所以追诉犯罪的证据问题变得非常关键。

二、法律规制渐明

今年2月18日实施的《刑法修正案（七）》对于惩治网络“黑客”的违法犯罪行为增加了相关条款，如利用技术手段非法侵入法律规定以外的计算机信息系统，窃取他人账号、密码、虚拟财产（如游戏装备）等信息，或者对大范围的他人计算机实施非法控制（如僵尸网络）等行为均有规制。

10月16日，最高人民法院、最高人民检察院公布的相关司法解释，正式将涉及计算机犯罪的“黑客”列入犯罪主体，这是国内第一次就计算机犯罪给出明确的司法解释。

与此同时，对于通过网络盗窃证券账户并通过买卖证券获利的行为在定性及量刑方面均有了明确依据。

“早期有关计算机犯罪方面的刑法条例不完善，对于利用计算机非法侵入他人证券账户进行倒卖获利的案件，一般都是只注重非法侵入他人证券账户进行倒卖获利的事实的认定，而即使这样‘侧重’之后，案件的审判还存在许多争议。”张路坦言。

2003年4月发生在江苏无锡的一起盗买盗卖股票案件便可窥见一斑。

2001年4月至2002年1月间，钱炳良通过非法手段获得殷阿祥、蒋汝初、叶梅英等16人的资金账号及交易密码后，以高吃低抛某一股票，同时在自己的资金账号上低吃高抛同一股票的方法，给被害人造成37.1万余元的经济损失，从中非法获利19.8万余元。

记者获得的一份该案资料显示，斯时，公诉机关认为，钱炳良多次盗窃公民财物，数额特别巨大，已触犯《刑法》第二百六十四条的规定，应当以盗窃罪追究刑事责任。

钱及其辩护人提出：指控盗用账户的证据不足；被害人的损失中有部分系协议平仓所致；故其行为属于操纵证券交易价格，不构成盗窃罪。

负责审理此案的无锡市中级人民法院则认为，钱炳良以非法占有为目的，秘密窃取他人财产，数额特别巨大，其行为已构成盗窃罪，判处其有期徒刑10年，剥夺政治权利2年，并处罚金人民币3万元。

一审宣判后，钱炳良不服，上诉于江苏省高级人民法院。

后者审理认为：钱以非法占有为目的，盗用他人账号和交易密码，采用在他人账户上高买低卖某一股票，同时在自己的账户上低买高卖同一股票的方法改变财产的持有状态，将他人财产据为己有。其行为符合盗窃罪的构成要件，应当以盗窃罪定罪处罚。并于2003年9月8日裁定驳回上诉，维持原判。

实际上，当时对于此案的焦点在于涉及“关于盗买盗卖股票行为的定性”和“关于盗买盗卖股票案件中的盗窃数额认定”。

据当时曾参与此案的江苏二中院的一名工作人员回忆，在此案审理过程中，对钱炳良的行为如何定性存在三种意见：

一是操纵证券交易价格罪，认为钱窃取被害人股票账户账号和密码的目的是获取不正当利益，通过非法侵入被害人的账户，以事先确定的时间、价格与自己进行股票交易，并在客观上影响所盗买盗卖股票的波动和交易量，其行为符合操纵证券交易价格罪的构成特征。

二是诈骗罪，认为钱在非法获取他人的股票账户账号及交易密码后，冒充他人向证券交易系统下达高价买进或低价卖出的指令，使自己账户低吃高抛该种股票从中谋取交易差价，其以非法占有为目的，实施欺骗手法获取他人钱财的行为符合诈骗罪的构成要件。

三是盗窃，被告人钱炳良窃取他人资金账号及交易密码后，在他人不知情的情况下高价买进或低价卖出某一股票，使自己账户低吃高抛同一种股票从中获利，符合盗窃罪的构成要件。

“我认为此案认定为盗窃罪是合理的。”张路告诉记者，在传统的盗窃案件中，盗窃罪在客观上表现为行为人通过秘密手段直接非法占有公私财物，上述此类案件中被告人不是直接非法占有被害人账户上的股票和资金，而是通过支付“对价”秘密窃取被害人账户上的股票，并通过买、卖股票的形式非法占有了其中的差价款。这种作案手段虽与传统的盗窃手段不同，但仍符合盗窃罪的构成特征：在主观上，被告是为了通过盗买盗卖股票非法占有被害人的财产；在客观上，被告是在被害人不知情的情况下，非法占有了被害人的财产。

那么，如果以盗窃案量刑，盗窃数额如何认定？

“如果被害人的账户中是现金部分的话，则以盗窃时候现金的部分作为认定，而证券的部分，那么则以该部分证券抛售后变现的获利部分认定。”张路解释说。

上述钱炳良案中，法院最终也是将被告的获利数额认定为盗窃数额。

“现在，按新刑法，如果钱炳良是通过非法入侵计算机信息系统或者采用其他技术手段，而获得被害人账户信息，即使其没有对该账户进行非法倒卖，但其行为也已经构成违法行为。而在后期的量刑中，其这部分违法行为也将被依法给予处置。”张路告诉记者。

反“黑”在行动——夯实网上交易防线

《21 世纪经济报道》　于海涛　北京报道

我国资本市场虽然起步较晚，但具有很多后发优势，其中之一是建立了便捷的电子交易系统。交易安全始终是系统开发、设计、维护、升级过程中考量的关键因素之一。在监管规则制定的过程中，交易安全制度保障始终是硬条条。在证监“三位一体”的执法体制中，任何涉及交易安全的线索都将引起一系列快速、标准监管动作。可以说，我国资本市场对网络盗窃早已重视并张网以待。

但同时，也要看到，互联网的安全问题已经不是哪一个行业单独面对的问题，证券业也难以独善其身。问题的解决，需要全社会的共同努力。

针对网络盗窃手段发展的趋势，近年来，证监会加强了证券、期货、基金等网络信息安全管理，以夯实网上交易安全防线。

记者获得的信息显示，2009 年以来，证监会专门开展以网上交易安全为重要内容的信息安全大检查，对全行业约 350 个机构门户网站和网上交易系统进行远程测试和监测。

“后来采取了一项强制性监管措施，即将机构信息安全水平与业务进行资格联动，行业各机构网上交易系统安全保障水平有了较大的提高。”一位监管部门人士对记者说。

与此同时，证监会于2009年6月发布了三个针对网上交易的信息技术指引，旨在防止网络攻击、网络仿冒、盗买盗卖及防灾难灾害。升级版的各项检查也在逐步进行。

前述人士介绍，证监会专门成立了证券期货业信息化工作领导小组，将信息系统安全作为维护资本市场稳定健康发展的关键环节来抓，不断提高信息系统安全保障水平。

一、经营机构："四防"

新的信息技术指引要求证券公司、期货公司、基金公司实现"四防"功能，即防网络攻击、网络仿冒、盗买盗卖、灾难灾害。

"防范这四方面风险，将有效解决网上交易的安全隐患，切实提高网上交易的安全防护能力，为投资者带来一个安全的交易空间。"前述监管部门人士说。

比如目前投资者最易受到损害的网络攻击。《指引》要求机构做五方面工作，具体包括：对网上信息系统合理划分安全域，在不同的域之间进行有效的隔离；部署包括防火墙，入侵检测或防护系统，防病毒、防木马系统等安全防护设施；建立定期扫描漏洞并修补的机制；对客户信息、交易指令等重要数据传输采取足够强度的加密措施；对提供给投资者下载的软件采取防篡改、防木马和防病毒等措施，切实提高网上交易的安全防护能力，防范网络攻击。

在防盗买盗卖方面，机构要为客户提供多种身份认证方式，除账户密码外，还至少向客户提供一种以上强度更高的身份认证方式，加强对网上交易客户身份和登录的合法性确认。

"机构也有责任防止用户使用简单口令，抵御连续猜测等针对客户账户的恶意攻击行为；同时网上交易客户端提供技术手段协助用户检查、清除木马等恶意软件，防范不法分子利用木马等黑客程序窃取客户账号和密码信息，进行盗买盗卖活动。"前述监管部门人士称。

对防止网络仿冒，机构被要求提供预留验证信息服务，在客户进行登录时向客户进行回显，帮助客户辨识正确的网上交易信息系统；同时服务端要能向客户提供可证明服务端自身身份的信息，以确保客户能查验服务的真实性，防范不法分子利用仿冒的网上交易信息系统进行诈骗活动。

当然，机构也要加强对交易委托的监控和投资者的提示。例如，通过对网上交易信息系统进行实时监控，建立异常事件的甄别、报警、处理和报告

机制以及通过多种方式提醒投资者加强账号、密码的保护工作来保证网上交易的安全。

二、投资者：四招自我防护

“从目前被盗窃的证券账户来看，账户密码的设置和保护有很重要的作用。”一位监管部门人士表示，有很简单但有效的“四招”可以自我防护，减少被盗用的风险。

一是口令、密码要有复杂度。不能用简单口令，如123456、666666等，要尽量复杂，比如英文字母和数字混合编排。同时不要用生日日期等易猜口令。

二是要定期或频繁修改口令，此办法可在账户被盗后第一时间阻止账户被操控使用，并及时发现账户是否被盗用，以减少损失。

三是注意口令、密码保护。

“不要使用不安全的计算机进行网上交易，如网吧、公用计算机等，在感觉有人偷看等不安全情况下避免使用。”前述监管部门人士说，自用计算机要做好安全保护，定期更新杀毒软件，防木马病毒盗窃，在网络上下载东西时要确认是否安全。

当然，不告诉他人或与他人共享账户密码、在输入口令时防止别人偷看也是比较实用的做法。

最后一招是不轻信假冒移动电话客户服务部门、公安部门等以各种借口要求提供用户名、口令。

“有些病毒用杀毒软件是杀不掉的，最好把计算机隔段时间就进行格式化，比较彻底地清除病毒。”前述人士说。

·记者手记·

扎紧篱笆　需多方努力

于海涛

世上事，预则立，不预则废。

我国证券市场对盗窃行为的发现、预警、监管和执法机制正在有效发挥作用，面对网络盗窃案件亦不必惊慌失措。

随着互联网技术的发展，网络犯罪是人们不可回避的现实问题，窃贼的

黑手正在伸向证券市场，我们应当保持必要的警觉，防患于未然。有关各方需要共同努力，扎紧篱笆，堵前来偷食的野狗于院外。

公安人员发现，被窃取的账户密码有一定的特征，比如长期使用一个密码不更换、密码设置过于简单等等。

“有的人为了操作简单、下单快，（密码）设六个1，我在查案子的时候就遇到过这样的情况，这不是等着被盗吗?”一位监管部门人士对本报记者说。

的确，有意识地防野狗，要从自己扎篱笆开始。荆州市公安局网监支队的李恩忠政委支招“两不要两要”。

一、不要从不明网站下载东西，如歌曲、软件等，很可能被绑定了木马病毒；二、事关资金交易的操作，如网上银行、证券交易等，不要在网吧等公共电脑上操作。

同时，计算机使用要经常做备份，并安装杀毒软件；还要定期格式化，以彻底删除那些不易杀掉的病毒程序。

对监管机构而言，获取交易IP地址或相关通信记录的证据十分关键。《证券法》赋予监管机构相应的查询权。记者了解的情况是，在办案过程中，这一权力的行使并不顺畅，监管机构需要有关方面的积极配合。

在保障交易速度的情况下，证券、期货经营机构可否积极开发一些新的技术和服务，比如采取U盾、认证卡等措施。

实际上，目前一些银行对储户账户中的金额发生变化时会有短信提醒等服务，便于客户第一时间知悉账户变动情况。

证券账户是否也可以考虑开拓类似服务？哪怕适当收些服务费，我想投资者应该愿意购买这种保险性质的服务。

扎紧篱笆，严防网络窃贼，需要各方共同努力。

违规委托理财自食其果　投资者更需“守土有责”

2010年1月7日　《上海证券报》　马婧妤

黄先生作为一名普通投资者，在申请设立资金账户，并签订《证券经纪业务

协议书》之初，或许并未对这几页薄纸上包括“规则说明”、“风险揭示”在内的内容给予足够的重视；小夏作为一名投资顾问，从第一次替黄先生下单到后来利用其账户擅自买卖股票，并因大额亏损，走向自杀的深渊，或许也只是起于一念之差。

而由此引出的投资者应当如何规范参与证券市场投资的问题，却值得深思。

一、违规私下委托操作引发越权交易

大户黄先生在某证券公司营业部（下称“营业部”）交易多年，因为投入资金较多，营业部指定职员小夏为黄先生提供股票交易相关联络服务。长期的联络使黄先生对小夏的信任日益增加，虽然营业部多次提醒黄先生妥善保存密码，不能委托员工进行操作，但为了方便，黄先生还是授权小夏设立了交易密码，采取黄先生下达交易指令，由小夏按指令进行股票买卖和资金转账操作的方式进行交易。

小夏获得交易密码后，一开始只是按照黄先生的指令进行操作，随着市场行情的变化，看到黄先生账户上有大量闲置资金，小夏不仅动起了打打交易量的心思，还心存侥幸，认为自己“不单纯是打交易量，也尽量做做差价”，让自己和客户都赚钱，可以两全其美。自此，小夏开始擅自在黄先生账户上大量买入、卖出股票，以获取佣金提成。

2008 年年初，黄先生从他人口中听说，他的账户内经常发生大额频繁交易，他起初并未重视，认为小夏不会将自己的交易密码泄露给他人，小夏自己也不会做翻炒股票的事情。但为慎重起见，黄先生 2008 年 1 月 31 日向小夏索要了交易单，小夏提供了汇总对账单，由于未看到交易明细，黄先生未发现异常。

2008 年 6 月，黄先生使用账户密码，第一次看到自己账户内股票交易的真实情况——大量频繁交易，以及由此产生的巨额印花税与交易手续费支出等损失 698 万元。黄先生此时才明白，自己贪图一时方便，酿造的是一杯苦酒。

随后，黄先生一纸诉状将小夏所在的营业部告上了法庭。认为小夏作为营业部职员，本应按照其指令进行股票交易，但越权擅自委托，造成巨额损失，营业部应承担相关责任。

二、厘清权责　违规者自食苦果

法院受理了黄先生一案，并将案件争议的焦点厘清为两点：一是营业部在接受黄先生委托代理股票交易过程中是否存在过失；二是上述过失是否为造成黄先生损失的原因及损失应当如何负担。

根据法院调查确认，黄先生开户时与营业部签订了《证券经纪业务协议书》及《风险揭示书》，其中明确提示，“投资者应当妥善保存交易密码，投资者密码失密可能造成损失，由于密码保管不当造成的损失客户需自行负担”；“营业部员工无权从事受托理财业务，客户不应与营业部员工签署任何形式的该类协议，否则由客户承担相应的法律和经济风险”；“客户应当在交易委托指令下达后三日内查询交易结果，如有异常应立即提出质询”。

而营业部在黄先生前去办理业务时，也多次当面对其进行了提醒。黄先生将密码告知小夏，私下委托小夏操作账户，并长期忽视查询交易结果的高风险行为，违反了与营业部的协议约定。

证据表明，该营业部《员工守则》、《尽职承诺书》等规定均明令禁止员工进行委托理财，小夏替黄先生买卖股票，属于营业部不知情的情况下，黄先生与小夏的私下交易，并非营业部指令小夏所为或小夏岗位职责范围内的职务行为。直至黄先生获知小夏擅自利用其账户实施大量交易之后，他们仍继续向营业部隐瞒交易内情。

法院认定，小夏利用密码下达委托指令是造成黄先生税费及价差损失的直接原因，而小夏之所以掌握密码，是由于黄先生主动提供，而非利用职务便利，采取不当手段盗取。任何掌握黄先生密码的人员都可能实施与小夏相同的行为，小夏并不因其具有营业部职员的身份而拥有更多便利。

综合有关因素，法院认为，黄先生在从事证券交易的过程中，违反与营业部的合同约定委托小夏进行股票交易，且没有及时查询交易结果，是造成其损失发生及扩大的根本原因。营业部在履行合同过程中无违约行为，对于相关损失的发生也没有责任，因发生违反合同约定行为而造成的损失，应由黄先生自行承担。

法院最终驳回了黄先生要求营业部赔偿损失并承担律师代理费的诉讼请求。

三、投资者更需“守土有责”

黄先生遭受了损失，为什么反倒要自负其责呢？法律专家表示，法院依据相关证据作出的判决，向社会和广大投资者传递出一个明确的，但却长期被社会公众忽略的重要信息，即无论是证券公司、从业者还是投资者，均需“守土有责”。

“黄先生与营业部之间的纠纷并非个别现象，在这类案件中，投资者往往缺乏合规意识，盲目信任他人，一旦造成投资损失，又转而向无过错的第三方提出赔偿诉求。”法律专家说，如果本案判决营业部承担最后责任，就有可能向公众传达出错误的信息，即司法机关对于投资者违反合同约定，随意向他人透露密码、随意委托从业者全权进行股票买卖、忽视交易结果的查询等高风险行为是持支持态度的。

“这不但会引发一定道德风险，还可能造成一部分人采取逆向选择行为，忽视交易风险，随意进行委托交易，盈利即享受收益，亏损则向证券公司索赔，这显然不利于证券市场整体安全，也不符合社会整体利益。”该专家表示。

部分从业者也指出，黄先生诉讼一案中，投资者对证券公司员工管理的严格性和有效性提出质疑，也足以引起证券经营机构充分反思。“作为受托人有责任针对营销、客服人员的执业特点，持续优化相关管理制度、内控机制和技术系统，采取多种有效措施防范道德风险和违法行为，充分保护投资者合法权益，为投资者提供更加优质的服务”。

据了解，目前我国相关法律法规明确规定，禁止证券公司在从事经纪业务时，接受客户全权委托，禁止证券公司员工私下接受客户委托办理股票交易事项。《证券经纪人管理暂行规定》从2009年4月13日起实施，该规定也对证券营销人员的禁止性行为及证券公司管理能力提出了明确要求。

而每个投资者在签订开户协议时，又都会接受关于保护密码安全、拒绝全权委托等违规行为的风险提示，并签字确认。这些要求无论对普通投资者还是证券行业从业人员来说似乎都应当属于基本常识。

“道理看似简单，但无论是投资者的交易风险，还是从业者的职业道德风险，都无法只依靠规章制度得以防范，证券市场的交易安全，还需要各个参与方都切实做到‘守土有责’，才能使制度得以执行、防范风险的目标得以实现。”业内专家表示。（本文涉及人物名字均为化名）