362--中国银监会办公厅关于客户信息安全有关风险提示的通知  
（银监办发〔2013〕211号）

各银监局，各政策性银行、国有商业银行、股份制商业银行、金融资产管理公司，邮政储蓄银行各省级农村信用联社，银监会直接监管的信托公司、企业集团财务公司、金融租赁公司：

近期，上海公安机关破获公安部督办的“11.7”特大复合型信用卡诈骗、洗钱案。为加强银行业金融机构客户信息安全管理，消除风险隐患，现就有关风险提示如下：

一、“11.7”特大复合型信用卡诈骗、洗钱案有关情况

“11.7”特大复合型信用卡诈骗、洗钱案犯罪嫌疑人盗取银行个人客户资金达600余万元。该案犯罪过程是：

（1）圈定目标。犯罪嫌疑人在几州个人名录网等非法网站上购买了数家商业银行客户信息，并从中筛选出若干个存款余额较大、未开通网银业务、密码设置简单的客户为作案目标。（2）冒名开户。犯罪嫌疑人通过假军官证开立与作案目标同名的银行账户。（3）绑定账户，犯罪嫌疑人将作案目标账户与其同名账户同时与第三方支付公司绑定。在绑定过程中，利用简易网上银行功能，对作案目标账户的资金流水进行查询，从而获得在“稳赢安E贷”网络融资平台验证注册用户的验证信息，顺利通过身份认证。（4）盗划资金。犯罪嫌疑人以投资为名，先将作案目标账户内资金转到该网络融资平台，再以撤资为由，将资金转入犯罪嫌疑人控制的同名账户，最终盗取作案目标账户资金。

二、本案反映出的主要问题

（一）互联网个人信息买卖等违法犯罪现象较为突出。以公民个人信息为核心的产品，已形成成熟的犯罪链条。上游是个别部门和行业从业人员将履职过程中获取的公民个人信息出售或以其他方式非法提供给他人：中游是利用互联网数据交易平台，出售公民个人信息牟利：下游是犯罪分子利用此类公民个人信息进行盗取资金、绑架、敲诈勒索、诈骗等违法犯罪行为。

（二）银行业金融机构在个人客户信息安全管理上存在漏洞和风险隐患。一是银行业金融机构内部员工兜售、泄露个人信息的案件时有发生，本案中，某银行信息技术管理部原员工为谋取非法利益，利用其维护数据的工作便利，非法提取、复制了该行个人存款信息800余万条，并将上述信息打包出售。二是伪造身份开设账户现象依然存在。有关商业银行未能有效识别假军官证开立的同名账户，为犯罪嫌疑人盗取资金提供了便利。三是网上银行，特别是简易网银功能安全防范措施不足。四是网络交易风险提示缺失。本案中被害人账户均未开通网银功能，巨额资金通过网络划转过程中从未要求进行安全认证或发出任何形式的提示。

三、监管要求

（一）切实提高认识，加强组织建设和责任落实。客户信息安全保护涉及各个部门和岗位，各银行业金融机构要充分认识客户信息安全管理的重要意义，明确揩定牵头负责部门，积极组织协调行内各部门加强信息安全管理，有效防范声誉风险和法律风险。

（二）加强客户信息安全管理的规章制度建设和执行工作。重新检视数据安全管理的相关制度、流程、系统，重新评估各类相关业务风险控制措施的有效性。加强客户信息全生命周期管理，完善客户信息全流程控制。逐步建立客户信息的分级分类保护机制。针对存在的漏洞和风险隐患，要在制度、技术、员工教育方面采取有效措施，切实防止信息泄露和滥用。

（三）防范外部风险传染。按照《关于加强电子银行客户信息管理工作的通知》（银监发[2011]86号）要求和相关监管规定，审慎评估与第三方机构的各项合作。加强外包环节客户信息保护，在合同巾明确客户信息保密和访问控制要求。防范外包服务活动中客户信息泄露风险。

（四）加强网上客户信息泄露情况的主动监测。银行业金融机构要积极利用互联网等多种技术手段和工具，主动监测客户信息泄露情况，发现案件线索及时向公安机关报案，积极配合公安机关的侦查工作。

二〇一三年八月十四日