反洗钱面临新风险　互联网金融如何扬长避短

日前，中国互联网金融协会(下称“互金协会”)发布《互联网金融从业机构反洗钱和反恐怖融资风险管理及内控框架指引手册》(简称《框架手册》)。互金协会表示，将按照监管政策要求，结合最新反洗钱实际，根据市场变动、风险变化等对《框架手册》进行动态调整和逐步完善。待条件成熟后，将联合其他行业协会，研究将《框架手册》上升为互联网金融反洗钱工作的行业规则，持续推进互联网金融反洗钱和反恐怖融资工作。那么，我国目前的反洗钱形势如何？互联网金融企业如何进行金融反洗钱工作？

新挑战倒逼新规则

“我国反洗钱工作的组织架构，是由经国务院授权的中国人民银行作为最高行政主管部门，依据我国的《反洗钱法》，并基于央行‘反洗钱 3 号令’(2016 年 12 月出台的《金融机构大额交易和可疑交易报告管理办法》)等，要求我国所有的金融机构和特定非金融机构在经营管理中必须履行反洗钱义务。”复旦大学经管学院中国反洗钱研究中心主任严立新在接受《上海金融报》记者专访时表示。

“要履行反洗钱义务，金融机构必须使用三大核心手段。”严立新表示，“一是‘了解你的客户(KYC)’，包括客户的基本身份信息、职业背景等，还要对这些信息进行持续了解和更新。二是针对大额交易和可疑交易，及时报送至人民银行。三是要对客户的身份资料和交易信息进行记录和保存，即在需要核验时，这些记录能够重新完整复盘交易全过程，包括资金来源、金额大小、资金性质、资金流动频率、资金流向、交易名目等。”

“现阶段，国内外反洗钱和反恐怖融资工作面临新挑战。一是洗钱总量逐年增长，频度提高，小额、多批次、多名目。二是洗钱活动不断向非银行机构‘外溢’。在银行业反洗钱总体水平不断提升的形势下，直接通过银行洗钱已越来越难。很多不法分子和犯罪组织开始将洗钱活动向反洗钱意识相对较弱、制度漏洞较多的非银机构、互联网金融机构扩张渗透，这给整个金融系统履行反洗钱义务增加了相当的难度。三是新科技、新金融模式，尤其是数字网络技术的高速发展和广泛应用，也被不法分子所滥用。四是洗钱、恐怖融资日趋全球化、网络化、智能化和复杂化等。”严立新进一步指出。

有鉴于此，互金协会明确，互联网金融本质仍属于金融，从业机构均应纳入金融反洗钱监管范围，同样执行金融反洗钱法律法规及其他监管规定、国际反洗钱标准、反洗钱行业规则。

据了解，《框架手册》严格遵循人民银行确定的“风险为本”反洗钱方法和相关工作要求，并结合互联网金融及反洗钱工作的最新发展，提供了一个可为广大从业机构开展反洗钱风险管理体系和内控机制建设借鉴参考的框架性文件。

《框架手册》要求，从业机构应定期或不定期评估洗钱风险和合规风险，根据风险评估的结果采取相应的反洗钱风控措施。应在风险高的领域里采取强化的反洗钱风控措施，在风险低的领域里可以采取适度简化的反洗钱风控措施，不断提升反洗钱工作的有效性。同时强调，如出现超出自身风险控制能力的情形，从业机构不得与客户建立业务关系或进行交易；已经建立业务关系的，应中止交易并考虑提交可疑交易报告，必要时终止业务关系。

互金协会强调，由于互联网金融业态众多、模式各异、创新速度快，行业相关的洗钱和恐怖融资风险复杂多变，因此可能出现反洗钱监管政策和行业规则不能针对互联网金融行业反洗钱的新问题、新风险。

“《框架手册》并非具有强制法律效力的文件，而是对央行 3 号令、国办 84 号文、银发 235 号文等规章制度的行业性细化和补充，是针对互联网金融行业的指导性文件，为互金企业的反洗钱工作提供了一个参照范本。”严立新表示，互联网金融行业包括第三方支付、网贷、众筹等多重业态，目前仅第三方支付机构就有 200 多家，每家机构的具体情况又有所不同。然而，我国监管部门的执法资源有限，监管科技的研发和应用存在迟滞，导致对互联网金融业态的监管不够充分，除行业头部的十几家平台外，对中后部机构实际监管的覆盖度和深度显得不够。此外，相比银行类机构，互联网金融机构的反洗钱意识较差，反洗钱投入也相对较小。

对此，《框架手册》明确，从业机构及其工作人员，特别是董事会、高级管理层，要提高反洗钱意识，建立符合监管期望、与自身社会责任相适应、有利于增强持续经营能力的反洗钱风险管理体系和内控机制。

发挥技术优势识别风险

值得关注的是，《框架手册》指出，从业机构应当发挥互联网金融行业的技

术优势，发展和创新风控工具，实现反洗钱风控的数据化，在保持基本政策稳定性的前提下，加快风控工具研发实施的速度。那么，互联网金融机构该如何发挥技术优势呢？

“由于传统金融机构在‘搜索引擎、社交网络、云计算、大数据’四要素建设中的天然缺陷，在数据采集范围、数据完整性等方面存在极大不足，难以支持复杂情景模式下的分析要求，无法对金融数据进行全面有效的运用，尤其不利于‘了解你的客户’这一预防和化解一切风险基础的落实。同时，金融业反洗钱监管部门无法直接获取海关、税务、工商等其他行政执法机构的电子信息。虽然工商、海关、税务等部门都已拥有自己的信息系统，但这些信息无论在体制上还是技术上，都不能为金融情报信息分析充分使用。”严立新表示，“在反洗钱过程中，互联网金融机构拥有更大的技术优势，通过大数据、自动化、人工智能等手段建立基础的模型，背后是大量的算法，实时抓取数据，并进行多因子交叉比对后，可发现异常交易或可疑行为。”

“交易要特征化，特征要指标化，指标要模型化，模型必须系统化，系统必须工具化，工具必须可视化。”严立新强调，“反洗钱就是对客户了解的越详细、越完整、越真实、越准确、越及时，机构的风控能力就越强。建立和完善基于‘金融云安全’理念和模式的反洗钱网络，将成为未来维护金融安全的必然选择。”

据悉，目前已有互联网公司在相关领域有所探索。以腾讯为例，腾讯安全开放灵鲲监管科技平台、天御星云风控平台等，面向泛金融领域解决新业务场景中的安全问题。其中，灵鲲已接入全国超 15 个重点省市的金融监管单位，累计监测金融风险平台超过 1.1 万家；天御系统上线以来已为中国银行、招商银行等数百家客户提供业务服务。

“在金融领域，安全唯成本中心论的现状正逐步改观，安全生产力价值逐步被印证。”腾讯副总裁马斌在接受《上海金融报》记者采访时表示，“以往，银行的线下交易也就几百单左右，而现在线上交易动辄就是几十万的申请量，如果不能运用技术手段，仅用传统方法识别不良用户将非常困难。”

支付宝安全事业部总裁芮雄文对《上海金融报》记者表示，为解决安全难题，支付宝已通过引入人工智能、机器学习等技术，对各类可疑交易进行深入分析，通过不断优化的算法模型，对可疑用户进行有效识别。

不过，严立新也指出，对客户个人信息的保护是反洗钱工作中的最大问题，要防止互联网金融企业以营利为目的，无度、无限制地获取和使用客户的隐私信息。

“央行将研究制定云计算、人工智能、区块链等技术应用的监管规则，对技术架构、安全管理、业务连续性等方面提出管理要求。引导信息技术在金融领域合理运用，纠正部分机构‘有技术就滥用’，‘有技术就任性”的乱象’。”中国人民银行科技司司长李伟在近日举行的第四届全球金融科技(北京)峰会上指出，用个人隐私换取些许便利得不偿失。个人隐私和信息保护工作做不好，久而久之，可能会造成数字恐慌和对技术的担忧。因此，央行对金融科技的监管思路是要强化金融信息的安全保护，明确覆盖金融信息收集、传输、销毁全周期的策略，访问控制、宣传引导加强金融信息的保护，持续提升全民金融信息安全的重要性。

（来源：上海金融新闻网。转引自：复旦大学中国反洗钱研究中心。时间：2019 年 7 月 17 日。网址：http://www.ccamls.org/newsdetail.php?did=35481。访问时间：2019 年 7 月 22 日 14:22。）