近年来互联网金融飞速发展，第三方支付、网络信贷、P2P等互联网金融模式迅猛发展，新冠疫情后互联网技术更是深刻地融入了日常生活，影响传统金融模式。互联网为普通大众提供了更加多元化的金融服务，提高了社会金融服务效率，提升了农村金融普惠性服务水平，大大增强了金融产品的覆盖面和支付的快捷性和便利性，为现代金融体系注入新活力，为经济发展带来巨大机遇的同时，洗钱风险隐患也不断暴露，“大众创业，万众创新”的背景下，各类金融产品的创新和发展速度加快，加上互联网金融“跨行业”、“跨业态”、“跨地域限制”、“技术密集”等特点，大大增加了金融交易的复杂程度和资金的追朔难度，如何规范互联网金融发展，有效防范洗钱风险，已成为焦点。

1. 调研背景及意义

（一）洗钱犯罪形势更加严峻、复杂。

互联网金融的开放性、匿名性等特点为洗钱活动提供了极大便利，互联网金融时代下洗钱犯罪形势愈加严峻。一是洗钱犯罪数量攀升。根据反洗钱报告统计， 2020年全国检察机关共批准逮捕洗钱犯罪 221 人，同比涨幅超过100%，提起公诉 707人，同比涨幅超过300%，网络的高效发展和大范围应用，越来越多的犯罪分子选择了利用互联网的渠道洗钱。二是洗钱犯罪渠道拓宽。互联网金融的发展迅速，交易更加便捷的同时也拓宽了洗钱途径。互联网金融悄然改变着传统洗钱方式，例如：犯罪分子由利用传统银行赌场洗钱转变为利用赌博网站来洗钱、以及伴随互联网技术衍生出的利用比特币、游戏卡券等虚拟物品进行洗钱。2019年泉州市一起重大的网络洗钱案件中，犯罪分子以网络科技有限公司的名义在互联网上搭建“第三方支付平台--通宝支付，通过平台代理持有的大量他人实名的支付宝账号和绑定银行卡，为“商户”提供非法资金支付结算业务。三是洗钱涉案金额增长。近年来，利用互联网洗钱的案件涉案金额不断增长，据调查统计，2013
年，我国涉及利用互联网实施洗钱罪的案件平均每件涉案金额约为 1775.7
万元，2015 年平均每件涉案金额增长到了约为 2004.8 万元，到了 2016
年，平均每件涉案金额则增长到了约为 2742.03
万元。不断增长的涉案金额对我国的经济和社会造成严重危害。

（二）监管防控体系逐步规范、有力。

《反洗钱法》颁布后，我国加快了监管体系建设，陆续出台《金融机构反洗钱规定》《金融机构大额交易和可疑交易报告管理办法》《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》，不断完善监管体系，在新时代反洗钱与反恐怖融资面临的新形势下，我国研究形成了一系列新时期下的反洗钱工作部署，力求缩小管理漏洞，补齐短板，达到预防、遏制洗钱犯罪的目的。一是完善立法体系，2015年7月，中国人民银行等印发《关于促进互联网金融健康发展的指导意见》，

加强对六类业态监管；2016年4月，党中央、国务院部署开展互联网金融风险专项整治工作；2018年以来，一行两会相继印发了《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》、《法人金融机构洗钱和恐怖融资风险管理指引（试行）》，将更多的互联网金融业态纳入反洗钱和反恐怖融资统一监管框架下；2019年6月24日，中国互联网金融协会发布《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》，归纳总结了境内外从业机构反洗钱最佳实践，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；2021年3月，刑法修正案生效实施，将“自洗钱”行为单独构成洗钱罪，与上游犯罪数罪并罚。二是健全监管体系，2010 年颁布的《非金融机构支付服务管理办法》，首次将第三方支付纳入到了反洗钱监管中，2017年 8 月，国务院下发“三反意见”，将“建立完善的反洗钱、反恐怖融资、反逃税体系”作为新形势下工作目标，明确了反洗钱行政主管部门、税务部门、公安部门的牵头职责，深化了我国洗钱协同治理机制。2018年《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》，提出建立监督管理与自律管理相结合的反洗钱监管机制，同年在国家机构改革工作中将金融行业监管模式调整为了“一委一行两会”，将银监会与保监会合并成银保监会，整合了监管资源，扩大了行业监管范围，增强了监管力度，缩小了跨行业监管壁垒。新的监管格局对洗钱和其他金融犯罪的打击力度更强，形成了监管合力和有效分工，互联网金融从业机构的监管由央行负责，监督其履行反洗钱义务；互联网金融犯罪，由公安部调查、打击、处置，既有分工又有协作。

1. 反洗钱工作迎来的困难与挑战

尽管监管政策、监管措施在不断更新完善，但是互联网技术、云计算以及大数据广泛应用、迅速更迭，金融产品、金融工具加速创新，监管往往相对业务创新迟滞一步，新技术带来新变革，洗钱、恐怖融资关违法行为也因变革和发展有了新的选择，反洗钱工作面临新的挑战。

（一）互联网金融简易快捷，为洗钱犯罪提供了方便。

与传统金融业相比，互联网金融交易门槛更低，服务可得性和便捷性更高，这也使得犯罪分子通过互联网交易洗钱变得更加容易。一是洗钱不受时空限制。根据“网贷之家”数据统计显示，2019年以来，全国市场实际运营的P2P网贷机构由高峰时期的约5000家的规模连续下降，几乎“全灭”，这些爆雷平台分布在全国31 个省（市）和地区，涉及行业包括医疗、美容、教育、汽车、休闲等。互联网金融突破传统金融“跨行业”、“跨业态”、“跨地域“的限制，犯罪分子可以在任何时间任何地方不受限制地使用账户，增加了执法部门、金融监管部门、金融机构的追踪资金难度。二是资金转移速度加快。“ｅ租宝”爆雷案件中，犯罪分子举着“互联网金融”的幌子，虚构投资项目，骗取投资者的资金， 通过 “ｅ租宝”搭载P2P平台的形式，以虚假项目、虚假三方、虚假担保制造P2P集资假象，多采用网银转账

以及大额存取等方式，将集中转入的资金快速分散转出，并通过多种途径再汇集，隐匿资金来源与去向。互联网交易可以在短时间内实现数次资金转移，为犯罪分子转移资金、混淆资金来源、规避反洗钱监管创造了条件。三是加速资金性质转换。互联网商户通过正常商品作为橱窗展示，可以轻而易举地掩盖为网络赌博、毒品等违法经济活动提供服务。2020年4月福建南平警方摧毁特大网络犯罪团伙，捣毁洗钱窝点31个，非法网络支付平台40个，犯罪分子通过四方支付平台，绑定大量银行卡及微信、等第三方支付账户进行交易，为境外网络赌博、网络色情、网络诈骗等团伙进行洗钱。

（二）互联网金融立法不足，给洗钱监管带来了盲区。

一是立法制度不完善。目前洗钱罪的上游犯罪范围相对狭窄，法律规定洗钱罪的上游犯罪包括：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、金融诈骗犯罪七种洗钱违法活动。伴随着近年来互联网的飞速发展带来的洗钱方式不断更新，这七种上游犯罪已经不能满足司法实践的需要。例如，2016年泉州的某案件中，嫌疑人利用开立的网店为赌博、诈骗等犯罪分子洗白非法收入由于赌博罪、诈骗罪、转移非法收入均不属于洗钱罪的七种上游犯罪，最终嫌疑人被判定为掩饰、隐瞒犯罪所得、犯罪所得收益罪。据不完全统计，2017-2020年利用互联网进行洗钱的犯罪案件中，最终被认定为洗钱罪的案件仅2.1%，立法不足造成重罪轻判，进而加剧利用互联网进行洗钱的犯罪行为的蔓延。二是监管制度不完善。一方面相关部门通过反洗钱的现场、非现场检查，督导金融和非金融机构的反洗钱相关工作的展开，发现问题后采取一定的措施，而互联网金融创新速度快、交易数据多、资金流转迅速，传统的监管方式相对滞后，监管制度建设速度跟不上互联网金融更新换代速度。另一方面反洗钱监管部门间协作不够到位， 当前我国建立的反洗钱部际联席会议制度，由23个成员单位组成，但会议制度的形式相对不够正式、规范，成员之间协作不足，造成监管重叠的同时，可能相互矛盾，部门间尚未形成高效协作模式。

（三）行业反洗钱意识不足，加剧行业洗钱犯罪滋生。

一是互联网行业内部控制机制不健全，部分互联网金融机构内控部门形同虚设，仅是简单的点对点报送数据，大额交易没有深入剖析，可疑交易及案例的排查不到位，部分互联网金融机构甚至没有设立有关反洗钱工作的专门部门，或者专门人员负责反洗钱工作和相关情况的上报。二是联网金融平台的从业者中，具备金融背景的不多，基本都缺少反洗钱常识，对洗钱的敏感度还相对不足，对洗钱治理工作不重视，职责履行不到位。

1. 风险防控对策分析及国际经验借鉴

（一）补短板，完善立法。

健全高效的金融法律体系，是保障互联网金融健康发展的基石，积极构建完善的互联网金融法律体系，引导互联网金融健康稳健发展。第一，扩大洗钱上游犯罪范围。参考借鉴国外立法以及国际公约，将掩饰、隐瞒犯罪所得、犯罪所得收益罪，纳入洗钱罪的上游犯罪，例如欧美国家将洗钱罪规定为一系列包括金融欺诈犯罪、恐怖主义犯罪、腐败犯罪等一共250多种罪名的犯罪。第二，扩大洗钱犯罪主体范围。例如美国为了适应互联网金融发展新形势，将洗钱罪的立法进行了完善，首先将电子货币纳入了反洗钱的规制范围中，并将钱罪上游犯罪的本犯、金融机构、非金融机构和互联网服务提供者纳入洗钱罪的主体范围，同时通过立法明确虚拟货币交易平台、第三方支付平台等互联网金融平台的反洗钱义务。完善互联网金融法律法规，完善以《反洗钱法》为核心的反洗钱法律体系，制定适用于互联网金融的法律规范，为互联网金融发展提供必要的制度支撑。

（二）严监管，加强防控。

第一，完善互联网金融监管体系。一是扩大监管范畴，坚持“风险为本原则”，将第三方支付、P2P网贷平台、电信运营商等涉及互联网金融的从业机构纳入监管范畴，建立互联网金融参与主体的反洗钱制度体系，明确各行业应当履行的反洗钱法定义务，例如俄罗斯反洗钱监管对象不仅仅是局限于金融机构，而是将自然人和法人均列入反洗钱执法对象范围，并由专门的执法权力机关对法人和自然人履行反洗钱义务进行监督管理。第二，明确互联网金融监管内容。确保反洗钱监管有效涵盖互联网金融各行业、各环节，禁止进行非支付类产品非法在线转账支付，防止各类互联网金融账户演变为洗钱分子利用的“过渡账户”，确保互联网金融产品符合安全和规范的要求，督促企业加强自身内控合规建设，提高风险防范能力，为互联网金融的发展提供规范化的秩序以及优质的发展环境。

（三）强内控，尽职调查。

互联网金融机构要认真执行反洗钱义务，尽职客户身份识、资金交易监测、妥善保管交易记录，构建涵盖事前、事中、事后的全生命周期监管客户的洗钱风险管理内控制度。第一，事前把控，建立反洗钱首道防线。完善客户身份识别制度，合理设计业务流程、操作规范。构建客户准入制度，完善实名制认证方式，明确禁止、建立或维持业务关系的情形；制定客户尽职调查程序，了解客户身份基本信息，了解实际控制客户的自然人和交易的实际受益人，切实做到“了解你的客户”。第二，事中监控，筑牢反洗钱工作基石。在“了解你的客户”基础上进一步拓展至了解客户的数据。将客户尽职调查贯穿交易的生命周期，收集包括客户账户信息、资金用途、转账地址、IP地址、历史交易数据等，对客户的交易数据进行精准化管理、精细化分析，建立客户风险分析模型，将采集到的客户身份信息、资金信息、交易信

息转化为模型参数，形成适合模型处理的标准数据集，分析客户风险等级。例如蚂蚁金服利用大数据技术，通过交易地址对比IP地址初步判断账号是否存在被人操控的风险。通过大数据模型，全方位分析，判断客户洗钱风险状况，及时监测和记录大额和可疑交易，提高数据分析智能化程度，提高网络洗钱响应的准确性及敏感度，筑牢事中监测链条。第三，事后管理，巩固反洗钱安全墙垒。遵循风险为本和审慎均衡的原则，将客户分为低风险、较低风险、中风险、高风险和禁止类五类，针对不同的客户，制定不同的监管措施，同时妥善保存资金交易金额、种类、方向等方面的交易记录，为反洗钱刑事侦查提供真实可靠的数据信息，利用互联网大数据做好深度挖掘，能够在客户身份识别、异常行为监测、趋势判断等方面提供有力帮助。

（四）善沟通，数据共享。

第一加强宣传，增强反洗钱意识。对于客户，广泛宣传，提升客户对反洗钱工作的认知、理解和支持。对于工商、公安、税务等相关政府工作单位，加强沟通和合作，打造良好的反洗钱工作环境，形成全社会共同预防、报告、查处、打击洗钱行为的反洗钱合力，构建“防打”结合的反洗钱机制。第二加强合作，建立大数据平台。要深入高效开展数字金融反洗钱工作，需要及时掌握客户的有效信息，要加强与其他政府部门沟通合作，建立大数据反洗钱共享平台，实现与工商、税务、公安等相关部门反洗钱信息互联互通，以能够实时有效更新客户信息，为异常交易的识别提供基础信息，反洗钱监测系统可以通过大数据平台进行全方位、多角度的检索、汇总，把反洗钱工作的事后监控变为实时、无间断的监控，提升反洗钱的敏锐度、时效性和准确性。例如丹麦反洗钱工作注重信息共享与交流，反洗钱行政调查中心有权直接访问包括警察机关、税务机关的内部数据库在内的各种公共数据库，通过多部门、多维度信息比对引证，较大程度提升了反洗钱中心发现重点线索的能力和效率，保证了线索的有效性和准确性。（文/桂舒婷）