证券代码：002212　　证券简称：天融信

天融信科技集团股份有限公司

投资者关系活动记录表

编号：2026-007

投资者关系活动类别	□特定对象调研　□分析师会议 □媒体采访　□业绩说明会 □新闻发布会　□路演活动 □现场参观 √其他（投资者交流会）
参与单位名称及人员姓名	本次线上会议在线参会人员 36 人，详细名单信息请参阅文末附表。 因本次投资者关系活动采取进门财经网络及电话会议形式，网络端参会者已按深圳证券交易所要求签署调研承诺书，电话端参会者无法签署调研承诺书。在交流活动中，我公司严格遵守相关规定，保证信息披露真实、准确、及时、公平，没有发生未公开重大信息泄露等情况。
时间	2026 年 10 月 29 日 15:30-16:50
地点	天融信科技集团股份有限公司会议室
形式	进门财经网络及电话会议
上市公司接待人员姓名	李雪莹：董事长、总经理 孔继阳：董事、财务负责人、副总经理 吴亚飚：董事、高级副总裁 孙　嫣：董事会秘书、副总经理 雷晓锋：副总裁 马腾辉：副总裁 王　炜：副总裁

交流内容及具体问答记录	**一、公司情况介绍** **（一）经营数据说明** **1、主要经营数据** 2026 年前三季度，营业收入 8.50 亿元，同比下降 29.28%；毛利率 56.10%，同比下降 7.52 个百分点；归属于上市公司股东的净利润为-4.85 亿元，同比下降 106.01%；归属于上市公司股东的扣除非经常性损益的净利润为-5.03 亿元，同比下降 99.64%；经营活动产生的现金流量净额为-6.07 亿元，同比下降 38.33%。 **2、第三季度降幅收窄** 2026 年上半年营业收入同比下降 33.99%，第三季度同比下降 18.93%； 2026 年上半年归属于上市公司股东的净利润同比下降 321.80%，第三季度同比下降 24.26%。 **3、智算云产品收入持续增长** 智算云产品（含智算云平台与一体机）2026 年前三季度营业收入 1.44 亿元，同比增长 11.46%，保持持续增长态势；2026 年前三季度智算云产品收入占营业收入比重为 16.90%，较上年同期 10.73%占比提升。 **4、政府收入比重下降，国有企业营收比重提升** 1）政府及事业单位：2026 年前三季度营业收入为 2.84 亿元，占营业收入比重为 33.35%，较上年同期 38.31%下降明显。 2）国有企业：2026 年前三季度营业收入为 3.49 亿元，占营业收入比重为 41.06%，较上年同期 36.62%比重提升。 3）商业及其他：2026 年前三季度营业收入为 2.18 亿元，占营业收入比重为 25.58%，上年同期为 25.07%。 **5、教卫行业营收增长** 2026 年前三季度，卫生行业和教育行业增长比较突出，卫生行业同比增长 70.33%，教育行业同比增长 7.50%。 **6、受原材料价格上行等因素影响，毛利率下降** 2026 年前三季度毛利率为 56.10%，较上半年毛利率 59.35%有所下降。

7、费用总额持续下降

2026 年前三季度三项费用合计 12.01 亿元，同比下降 1.08%；扣除离职补偿金和股份支付费用影响，同比下降 3.96%。

8、团队持续优化，提质增效显著

2026 年第三季度末员工总人数 4,759 人，较 2025 年末 5,160 人下降 7.77%，在营销、技术、管理等方面人数均有下降。

（二）AI 安全行业分析

1、AI 安全市场的核心驱动力

1）政策：合规从可选变为强制

（1）2026 年 1 月新修改《网络安全法》施行，首次将人工智能安全纳入法律框架。

（2）2026 年 3 月“十五五”规划纲要发布，明确建立 AI 全生命周期风险管理制度及风险防控体系。

（3）2026 年 5 月网信办等三部门印发《智能体规范应用与创新发展实施意见》，强化智能体安全保障。

（4）2026 年 7 月全球首部智能体安全强制性国标《智能体应用安全基本要求》立项，强化 AI 应用安全治理。

（5）2026 年 8 月工信部《关于开展人工智能应用服务商培育专项行动的通知》，培育人工智能应用服务商。

（6）2026 年 9 月《人工智能安全治理框架 3.0》发布，提升人工智能安全治理共识和风险防范应对能力。

2）事件：风险从理论变为现实责任

（1）2026 年 7 月 OpenAI 的 AI 智能体在内部测试中自主入侵 Hugging Face，持续 107 小时。

（2）2026 年 9 月 Anthropic CEO 呼吁放缓前沿大模型迭代，模型能力提升速度远超安全管控能力。

（3）2026 年 9 月 IBM 发布《2026 年数据泄露成本报告》，全球单次泄露平均 499 万美元创新高，AI 驱动攻击增长 56%、单起均值 600 万美元。

（4）2026 年 10 月韩国新韩银行、KB 国民银行、韩亚银行等 7 家

	金融企业，遭到黑客攻击，多处发现同一攻击者利用 AI 实施攻击的迹象。 （5）2026 年 10 月 AI 挖出 PHP 编程语言两个严重安全漏洞，全球 70%网站面临风险。 3）技术：安全成为新增基础设施 （1）2026 年大模型竞争重心从“刷榜、堆参数”转向智能体、长流程自动执行、端云协同、工程化落地。 （2）2026 年 4 月大模型、AI 智能体迭代落地提速，Anthropic Claude Mythos 可自主挖掘零日漏洞。 （3）2026 年 9 月网安周发布 AI 赋能网络安全应用测试结果：151 家单位 251 个团队参与 8 大场景，产品加速商用验证。 （4）2026 年 9 月 IDC 首发《中国 AI 安全技术发展路线图 2026》报告，明确 AI 安全技术阶段演进方向。 （5）2026 年 10 月 Gartner 发布《2026 年人工智能安全技术成熟度曲线》《2026 年人工智能驱动网络安全技术成熟度曲线》报告，评估各类 AI 安全、AI 驱动网安技术的成熟周期。 **2、AI 安全已经进入全新发展期** 1）AI 安全的两大方向 （1）AI 赋能安全（AI-amplified security） 用大模型提升安全能力，包括威胁研判、漏洞挖掘、安全运营。 （2）AI 自身安全（Securing AI） 主要包括大模型安全、智能体安全。 2）全球 AI 安全市场（Gartner） 两大赛道同步扩容、持续高增长。 （1）AI 赋能安全：2026 年预测市场规模 485 亿美元，2030 年预测市场规模 2,044 亿美元，五年复合年均增长率 53%； （2）AI 自身安全：2026 年预测市场规模 28 亿美元，2030 年预测市场规模 164 亿美元，五年复合年均增长率 60.4%。 3）全球市场结构扩张（Gartner） AI 安全市场包含 AI 赋能安全与 AI 自身安全

	（1）2026 年 AI 安全市场规模 513 亿美元，占全球网安市场规模（2,490 亿美元）的 20.60%； （2）2030 年 AI 安全市场规模 2,208 亿美元，占全球网安市场规模（3,723 亿美元）的 59.30%。 AI 安全属于典型的“荷花效应”，增长快、确定性高、集中爆发的新赛道。 **3、国外 AI 安全市场回报已显现** 1）Palo Alto Networks： （1）AIRS 营业收入突破 1 亿美元； （2）AI 安全运营营业收入突破 7 亿美元； （3）2026 年整体营业收入 115 亿美元，增长 24%。 将 AI 深度注入全产品线，构建统一、智能的主动防御体系。 2）Fortinet： （1）2026 年第三季度硬件收入增长 37%，AI SecOps 账单增速约 23%； （2）2026 年度预计整体营收 80 亿，增长 19%。 通过 FortiGuard 实验室提供 AI 驱动的安全服务，作为产品的智能升级包。 3）CrowdStrike：AI 原生的端点安全防护 AIDR 意向订单 5,000 万美元，增长 250%。 从设计之初就将 AI 置于核心地位，利用轻量级代理和云端 AI 引擎。 4）公司与 Palo Alto、Fortinet 的底层发展逻辑高度趋同。 **4、全球 AI 安全防护主要产品技术** Gartner 重点关注的 AI 安全技术方向与产品： 1）AI 应用安全：2026 年预测市场规模 508 百万美元，2030 年预测市场规模 2,950 百万美元（占 2030 年 AI 安全防护市场规模的 17.90%），复合年均增长率 55.20%； 2）AI 使用控制：2026 年预测市场规模 433 百万美元，2030 年预测市场规模 2,917 百万美元（占 2030 年 AI 安全防护市场规模的 17.70%），复合年均增长率 61.10%；

	3）AI 治理平台：2026 年预测市场规模 275 百万美元，2030 年预测市场规模 1,435 百万美元（占 2030 年 AI 安全防护市场规模的 8.70%），复合年均增长率 51.10%； 4）AI 网关：2026 年预测市场规模 251 百万美元，2030 年预测市场规模 1,417 百万美元（占 2030 年 AI 安全防护市场规模的 8.60%），复合年均增长率 54.10%； 5）其他：2026 年预测市场规模 1,368 百万美元，2030 年预测市场规模 7,722 百万美元（占 2030 年 AI 安全防护市场规模的 47.00%），复合年均增长率 54.10% AI 安全防护市场总规模 2026 年预测 2,835 百万美元，2030 年预测 16,440 百万美元，复合年均增长率 55.20%。 **5、国内 AI 安全市场蓄势待发** 1）第一阶段：2024-2025 年 合规先行：优先备案、内容审核。满足应用上线的底线合规要求，以内容合规产品为主。 2）第二阶段：2025 后期-2026 年 模型推理安全：解决模型应用中的安全问题，大模型安全网关成为刚需，随着大模型落地普及，此需求会长期存在。 3）第三阶段：2027-2029 年 智能体安全：成为下轮增长核心驱动力，现在是布局窗口期，未来 1-3 年订单逐步兑现。 **6、结构性机会凸显，为头部安全企业提供了巨大结构性机会** 1）中国 AI 安全市场（IDC） （1）AI 赋能安全：2026 年预测市场规模 43 亿元，2030 年预测市场规模 593.50 亿元，五年复合年均增长率 106.50%； （2）AI 自身安全：2026 年预测市场规模 65 亿元，2030 年预测市场规模 340.30 亿元，五年复合年均增长率 50.50%。 2）中国市场结构扩张（IDC） （1）2026 年 AI 安全市场规模（108 亿元）占中国网安市场规模（900 亿元）的 12%；

	（2）2030 年 AI 安全市场规模（933.80 亿元）占中国网安市场规模（1,256.80 亿元）的 74.30%。 传统网络安全市场复合增长率 8%-10%。 3）AI 安全的两大方向 （1）用 AI（AI 赋能传统安全，存量市场） 预算来自传统预算，交付模式不变，围绕既有安全产品与服务进行智能化升级。 （2）护 AI（保护 AI 系统安全，增量市场） ①合规先行/综合防护 国内政企数字化 AI 业务风险：监管、数据主权、信创与关键安全需求叠加； 客户更倾向具备长期安全服务、信创适配和全栈交付能力的综合安全厂商。 ②合规是刚性门槛，安全预算确定性强。 **7、国内 AI 安全防护主要产品技术及市场需求** 1）主要产品技术 （1）数据安全层：防止核心数据被 LLM 带走/输出 （2）运行时防护层（刚需）：大模型安全网关（围栏）/AI（应用）网关等。 （3）Agent 安全层（智能体安全层）：新出现重要增量。 （4）AI 安全治理与评估层：模型资产盘点、AI 安全管理平台、大模型红队渗透测试、AI 安全评估测试、合规咨询（备案、等保）等。 2）政企客户需求状态 从智算平台、私有 LLM 到公有 LLM，不同行业有不同需求，都需要一套联动方案，包括网关（围栏）、数据安全、安全审计、安全治理，并需要信创底座，最终需要综合型安全厂商提供一体化服务。 **8、国内 AI 安全赋能产品技术及市场需求** 1）产品技术：AI 赋能安全运营、AI 赋能安全防护、AI 赋能安全评估等方向。 2）市场需求

（1）市场空间（IDC）

AI 赋能安全产品市场规模五年复合年均增长率 106.5%。AI 安全运营平台 2025 年市场规模 15 亿元，同比增长 144%。

（2）海外 AI 赋能安全营收印证

Fortinet2026 年第三季度硬件增速达到 37%；AI 数据中心建设带动防火墙收入增长；防火墙销售持续带动订阅/维保服务增长。

（3）新增市场机会：国产化替换+AI 技术应用增量双轮驱动

①Palo Alto、Fortinet 等国产化替代市场；

②党政信创产品、维保更新；

③金融、能源等关基行业国产化替代；

④公共安全、自动化渗透、漏洞挖掘等领域全新市场。

（三）面对 AI 安全全新发展期，天融信已经做好了充足准备

1、AI 安全布局早，非临时上此赛道

1）2014 年：成立 AI 研究团队，重点关注机器学习、小模型等赋能安全。

2）2016 年：推出基于 AI 的安全技术，恶意程序检测、加密流量分析、隐秘隧道检测等。

3）2017 年：推出基于 AI 的相关产品，UEBA、态势感知、大数据分析系统等。

4）2019 年：联合 IDC 发布 AI 防火墙白皮书。

5）2023 年：发布天问大模型。

6）2024 年：天问大模型通过双备案，生成式人工智能服务备案、境内深度合成服务算法备案。

7）2025 年：智算云平台，首批大模型一体机能力验证检验证书（中国软件评测中心）；大模型安全网关，首张大模型安全防护围栏产品认证（增强级）（公安部第三研究所）。

8）2026 年：持续完善 AI 安全体系，AI 安全评估系统、智能体安全评估服务、AI（应用）网关、AI 安全管理系统等。

2、天融信 AI 防火墙演进：AI 产品赋能的三次跃升

1）1.0 智能检测时代（2019 年-2021 年）

	2019 年联合 IDC 发布《融入人工智能的下一代防火墙》白皮书； 2021 年业内率先发布 AI 防火墙产品。 2）2.0 智能运营时代（2023 年-2025 年） 2023 年全面接入“天问”大模型； 2024 年构建以防火墙为核心的智能安全运营体系。 3）3.0 算力与大模型防护时代（2025 年至今） 2025 年业内率先推出专用大模型安全防护模块； 2026 年具备提示词注入防护、多轮对话语义防护、多模态内容检测等能力。 **3、已构建完整的（用 AI＋护 AI）全栈产品矩阵** 1）用 AI （1）AI 安全运营 天问安全智能体平台、态势分析与安全运营系统、AI MSS 托管服务、安全策略管理系统。 （2）AI 赋能安全防护 NGFW/APT/IDPS、自动化渗透测试系统、内容智能管控系统、数据/云/工控安全的 AI 化。 2）护 AI （1）Agent 安全 AI 安全管理系统、智能体/API 安全审计系统、智能体安全评估服务、终端安全 AI-DR。 （2）数据安全 大模型数据安全监测系统、大模型安全网关、智能体/API 安全审计系统。 （3）运行时防护 大模型安全网关、大模型数据安全监测系统、AI（应用）网关。 （4）AI 安全治理与评估 AI 安全评估系统、AI 安全管理系统、智能体安全评估服务。 **4、基于深厚的政企客户基础，已在多个行业实现 AI 安全落地** 涵盖政府、金融、电信、能源、交通、教育、卫生、企业等行业，很

	多行业已在部署应用阶段，已形成相关领域典型应用案例，未来可进行批量化复制。 **5、信创+智算+AI 安全（业内唯一）** 公司是业内唯一的三位一体（信创+智算+AI 安全）综合性厂商，可以做到算力底座+安全深度匹配，对算力安全需求有更深理解，信创生态和产品技术积累。 **6、前瞻性战略布局，目前已完成智能体安全产品布局** （1）资质能力测评：首批人工智能服务安全建设二级、首批人工智能服务安全检测二级资质能力测评。 （2）智能体安全产品：大模型安全网关、智能体/API 安全审计、AI（应用）网关、终端安全 AI-DR、智能体安全评估服务、AI 安全管理系统。 **7、AI 安全防护大单品-市场规模大** 1）AI 安全防护大单品：大模型安全网关（围栏）、AI（应用）网关、API/智能体安全审计、AI 安全评估系统、AI 安全管理系统； 2）AI 安全防护第三季度收入约 1,200 万元，前三季度累计约 2,300 万元，同比增长超过 130%。 **8、AI 赋能安全大单品-市场规模大** 1）AI 赋能安全大单品：AI 防火墙、APT 安全监测、自动化渗透测试、内容智能安全、AI 安全运营； 2）AI 赋能安全第三季度收入约 8,500 万元，前三季度累计约 1.65 亿元，同比增长超过 90%。 **9、2026 第三季度业务进展-产品** 1）发布 AI 网关、前沿虚拟补丁智能体、AI 智能体安全评估服务、分布式存储等新产品、新服务。 2）发布大模型安全网关、大模型数据安全监测、API 安全审计、大模型安全评估、智算云平台、超融合、桌面云、安全智能体一体机等产品新版本。 **10、2026 第三季度业务进展-方案** 发布智能体全域安全防护框架、具身智能安全防护框架、AI Agent 安

	全防护方案、政务 AI 一体化安全方案、金融行业智能体安全解决方案、教育行业智能体安全方案等框架和方案。 **11、2026 第三季度业务进展-资质荣誉** 1）公司级：2026 年度软件和信息技术服务竞争力百强企业、2026 年度国家人工智能安全漏洞库优秀技术支撑单位、2026 年度核心技术支撑单位和技术支撑单位（一级）、工信部六大安全漏洞专业库技术支撑单位、第六次入选北京民营企业科技创新百强。 2）产品级： （1）IDC ①超融合以 14.5%的市场份额，位列中国超融合软件及验证系统市场第二名； ②智能体安全类产品入选《中国企业级通用智能体安全解决方案市场洞察，2026：安全是 AI 应用的基石》； ③大模型安全评估系统入选《中国生成式 AI 的安全评估平台厂商评估，2026》； ④天问大模型入选《中国安全大模型一体机技术评估，2026》； ⑤大模型安全网关入选《中国大模型应用防火墙技术评估，2026》。 （2）Gartner：EDR 入选《中国端点保护（EPP/EDR）市场概述》； （3）北京网络空间安全协会：大模型数据安全监测获 2026 年度北京网络空间安全协会科学技术奖； （4）中国电子技术标准化研究院赛西实验室：AI 防火墙首批获得《人工智能防火墙产品测评》证书的产品。 （5）工信部中国软件评测中心等：获 AI 服务安全能力评定“建设+检测”双证； （6）中国信息通信研究院：API 安全智能体通过中国信通院数据安全智能体产品能力检验。 **12、AI 安全是产业确定性赛道，天融信已完成布局，具备优先承接行业订单的能力。**

	二、交流环节 **1、公司防火墙能力在国内处于领先地位，如何看待 AI 时代对防火墙的新要求和演进趋势？如何看待公司未来在 AI 防火墙领域的竞争优势？** 答：1）AI 防火墙领域，公司产品团队持续跟踪国内外最新技术进展，技术思路与 Fortinet 一致，主要在防火墙产品上叠加两方面新能力：一是通过 AI 提升原有安全防护能力，二是针对 AI 业务系统提供安全防护能力。 （1）通过 AI 提升防火墙原有安全能力。自 2014 年起，公司持续将 AI 技术应用于防火墙产品，陆续引入小模型和大模型，目前已部署多个专项模型，提升对恶意域名、恶意流量、未知威胁攻击等的防护能力。 （2）针对 AI 业务系统提供安全防护能力。大模型服务、智能体系统等的发展，为防火墙带来了新的安全需求和市场机会。公司即将发布的最新 AI 防火墙，将集成大模型围栏和算力网关两大功能。①大模型围栏能够防御针对大模型的攻击，如提示词注入、越狱指令等，对大模型的工作过程和 API 调用进行监督、审计，降低数据泄露风险，同时分析客户智能体对大模型的使用情况，监控智能体的数据流转链路。②算力网关能够为客户提供大模型访问的统一入口，支持多个模型实例、不同版本的模型及不同 GPU 卡配置，既支持客户内部私有化部署的大模型，也支持外部商用大模型，并结合客户业务需求，以及模型的权重、特长、费用和数据安全配置进行路由规划，在效率、费用和安全之间实现平衡。 2）公司在防火墙硬件、AI 领域均有深入研究和深厚技术积累，在 AI 防火墙领域将继续保持绝对竞争优势。 **2、请问公司对 AI 安全业务的发展规划及 27 年展望？** 答：1）公司 AI 安全业务发展规划：（1）产品技术侧，坚持“用 AI、护 AI”的思路，依托天问安全大模型，持续完善覆盖算力、模型、数据、智能体全生命周期的 AI 安全产品与方案，包括已发布的 8 类 AI 安全防护产品和服务，以及多款 AI 赋能安全产品的升级迭代。（2）市场侧，公司面向政务、电信、金融、能源及监管等行业，形成 AI 赋能安全和 AI

	安全防护两类方案，正在围绕重点行业打造标杆案例。 2）2027 年展望：伴随大模型和智能体应用规模化、监管要求落地，AI 安全需求有望从单点试点转向体系化建设，预计 AI 安全业务将实现高速增长，成为公司重要的增长动力。 **3、公司中报首次披露 AI 安全分项收入（AI 安全防护 1,100 多万元、增长超 130%；AI 赋能安全超 8,000 万元；合计约占安全收入 22%），请问前三季度这两部分的最新收入量级和增速？三季报提到的 AI 网关、AI 安全评估系统、智能体安全评估服务，是已有订单落地还是发布阶段？全年 AI 安全收入能否给个量级预期？** 答：1）前三季度 AI 安全收入：（1）关于 AI 安全防护业务收入，第三季度约 1,200 万元，前三季度累计约 2,300 万元，同比增长超过 130%，是公司目前增长幅度最快的业务。（2）关于 AI 赋能安全业务收入，第三季度约 8,500 万元，前三季度累计约 1.65 亿元，同比增长超过 90%。（3）整体来看，前三季度 AI 安全收入占公司网络安全收入的比例持续提升，达到约 26.9%。 2）AI 网关、AI 安全评估系统、智能体安全评估服务为公司第三季度新发布，目前主要处于客户测试阶段。 3）全年 AI 安全收入预期：预计 AI 安全防护业务、AI 赋能安全业务的全年收入同比增幅均在三位数水平。 **4、请问 2027 年信创对安全业务的影响和机会？** 答：信创对安全业务总体是确定性的正向驱动。预计 2027 年进入行业信创订单集中释放和党政行业更新替代的关键窗口期。公司优势如下： 1）公司在信创存量市场中产品占有率最高，无论客户后续购买续保订阅还是替换，公司均具备先发优势。 2）公司在 AI 赋能安全上已构建全栈产品和服务体系，客户替换 AI 赋能安全产品时，要考虑信创能力和 AI 安全能力，公司均具备。 3）信创替代中，不仅涉及安全，也涉及大模型应用和智能体化，带来超融合、智算云和分布式存储的需求。公司集智算云、AI 安全、信创

	能力于一体，帮助客户在 AI 技术发展阶段，提供“信创+算力+安全”协同交付的全栈能力。 **5、公司第三季度收入下滑情况较上半年明显收窄，请问改善原因？** 答：公司第三季度收入降幅收窄主要源于国有企业、教育、卫生行业的边际改善。其中国企部分细分行业已实现同比增长，如交通行业增幅较大；能源、运营商等占比较高的行业第三季度同比接近持平。 **6、目前网络安全行业整体仍处承压阶段，但公司第三季度收入降幅较上半年有所收敛。请结合下游行业情况，说明三季度细分行业需求是否出现边际变化？** 答：公司第三季度收入降幅收窄主要源于国有企业、教育、卫生行业的边际改善。其中国企部分细分行业已实现同比增长，如交通行业增幅较大；能源、运营商等占比较高的行业第三季度同比接近持平。从行业需求看，上述变化具有一定象征意义，但趋势性仍待后续验证。
关于本次活动是否涉及应披露重大信息的说明	本次活动不涉及应披露重大信息。
活动过程中所使用的演示文稿、提供的文档等附件（如有，可作为附件）	无

附表：参与单位及人员名单（按参与单位名称首字母排序）

序号	参与单位	人员姓名
1	北京证券有限责任公司	宋晔波
2	国信证券股份有限公司	张衡
3	国元证券股份有限公司	耿军军
4	鸿运私募基金管理（海南）有限公司	朱伟华
5	湖南潇湘资本投资管理有限公司	陈靓璇
6	华创证券有限责任公司	胡昕安
7	金鹰基金管理有限公司	吴海峰
8	开源证券股份有限公司	刘逍遥
9	凯联（北京）投资基金管理有限公司	李肇齐
10	METAPHASE FUND L.P.	张若跌
11	山西证券股份有限公司	邹昕宸
12	上海君璞投资咨询有限公司	刘欢
13	上海君璞投资咨询有限公司	高翔
14	上海联视投资管理有限公司	周申力
15	上海尚颀投资管理合伙企业（有限合伙）	宋明
16	上海天猊投资管理有限公司	曹国军
17	上海行知创业投资有限公司	周峰
18	深圳定航私募股权基金管理有限公司	袁子颖
19	深圳市凯玄投资有限公司	周里亚
20	深圳市裕晋私募证券投资基金管理有限公司	张恒
21	天风证券股份有限公司	王祺深
22	天津远望资产管理咨询有限公司	赵栋
23	无锡韩宴	焦为民
24	兴业证券股份有限公司	蒋佳霖
25	云南约牛软件科技有限公司	宋诚
26	长城证券股份有限公司	黄俊峰
27	长城证券股份有限公司	沈彻

序号	参与单位	人员姓名
28	长江证券股份有限公司	郭敬超
29	长江证券股份有限公司	牛兆川
30	中电产融私募基金管理有限公司	房海强
31	中国人寿养老保险股份有限公司	裴勇
32	中国银河证券股份有限公司	邹文倩
33	中泰证券股份有限公司	苏仪
34	中信证券股份有限公司	潘儒琛
35	中邮证券有限责任公司	孙鹏
36	中原证券股份有限公司	唐月