浦东新区企业

商业秘密保护指南

上海市市场监督管理局
上海市浦东新区市场监督管理局

2023年8月

序言

我国已进入了高质量发展的重要阶段，推进创新发展，实现科技自立自强，让创新成为引领发展的第一动力成为时代重大命题。大力发展创新型企业，突破一批关键核心技术，解决“卡脖子”问题变得十分紧迫。商业秘密作为企业的重要知识产权，是企业的核心竞争力。企业的核心技术、核心竞争力，是创新发展、高质量发展的重要推动力。而保护商业秘密就是保护企业的知识产权，就是保护企业的创新能力。

我们要深刻认识到，商业秘密保护对经济增长和创新发展的重要作用，积极探索有效保护模式，以商业秘密保护“小切口”，营造公平竞争“大环境”，为企业创新构筑起坚实的保护屏障，护航公平竞争条件下产业创新发展活动。

浦东新区于2022年7月入选国家首批商业秘密保护创新试点地区。编制《浦东新区企业商业秘密保护指南》（以下称本指南）是浦东新区今年的重点工作之一。市市场监管局和浦东市场监管局联合组建编写组，邀请法官、检察官、律师等专业人士撰稿，从事前防护、民事保护、行政保护、刑事保护、商业秘密鉴定、海外维权等维度对商业秘密保护建言献策。

目前，全国各地陆续出台了一批商业秘密保护地方性标准、指南或指引，从内容看，多系现行法律法规的简单整理汇编，体现企业急需的有关商业秘密保护的实操办法或措施并不多。为了更加贴合企业的实际需求，编写组在以下方面做了全新的探索：

——重点聚焦于企业事前保护部分，对在本区培育创建商业秘密保护示范点过程中发现企业好的经验和做法加以归纳总结；

——认真总结浦东新区司法、行政执法部门一线审判执法实践心得，以实际问题为牵引，以案例的方式导出相关解答；

——公布浦东地区维权部门的联系方式和具体地址，解决维权最后一公里的问题；

——请专业鉴定人讲授入门 ABC，揭开商业秘密神秘的面纱；

——邀请具有海外知识产权执业经验的专家介绍中外维权的差异及应对，切实回应企业“走出去”的难题。

囿于时间和水平有限，本指南还有诸多不足之处，敬请广大业者批评指正。

撰稿人（按撰稿顺序排列）：

☆上海上湖信息技术有限公司李扬、邵晓婷负责 1.1 部分的撰写

☆上海瀛泰律师事务所章煦春、许懿、劳嘉馨、杜逸文、刘扬负责 1.2—1.10 部分的撰写

☆浦东新区人民法院叶子晖负责民事保护部分的撰写

☆上海思济律师事务所代涛负责行政保护部分的撰写

☆浦东新区人民检察院季柳阴来负责刑事保护部分的撰写

☆上海科普教育技术展示中心陈琳负责商业秘密鉴定部分的撰写

☆北京汉坤律师事务所上海分所龚雅玲、严瑾丽负责涉外保护部分的撰写

☆市市场监管局郑取、杨杰和浦东市场监管局秦芳负责统稿和校对

目录

1.自我保护

1.1【保护策略】

知己知彼，方能百战不殆。商业秘密的保护，亦是如此。

只有针对公司的核心经营要素，例如技术、经营、客户信息等资产，明确保护的对象，依据这些对象所处载体的不同，如数据库、办公计算机、纸质、云服务等不同场景，方才便于设定合理的保护策略和手段。

1.1.1【商业秘密保护要素】

实现商业秘密的保护，可归纳为三要素:

a）机密性。商业秘密不被未授权的主体访问。例如，访问控制，仅高管有权查看保险箱里的文件。加密，一个核心算法被加密存储，盗窃的第三方无解密用的口令，也无权查看。

b）完整性。商业秘密不被未授权的主体篡改。例如，数字签名，与客户一笔经由网络渠道签署的合同存在争议，若合理使用数字签名技术，可由第三方公证合同的未被篡改和其有效性。

c）可用性。商业秘密可被授权主体及时可靠的访问。例如，使用备份技术，防止因勒索软件等原因，造成商业秘密信息无法访问。

1.1.2【小微企业】

小微企业需要管理的商业秘密数量较少，涉及的员工较少，但员工可能身兼数职。保护的核心思路应从可用性着手，避免因天灾人祸的事故，导致商业秘密不可用。

1.1.2.1【保密条款】

对于可能涉及商业秘密的员工，应签署保密协议，利用法律约束，进行兜底。

1.1.2.2【安全意识培训】

对所有员工，都应将安全意识培训纳入到入职试用期转正和周期性工作考核中进行。

1.1.2.3【备份】

对关键性数据进行实时备份，对于其他数据每天进行备份，可有效应对勒索病毒的威胁，保证商业秘密信息如客户信息的实时有效可

用。

1.1.2.4【杀毒软件】

确保办公计算机杀毒软件有效启用并更新，可有效应对勒索病毒的威胁。

1.1.2.5【访问控制】

确保每个员工使用独立的账号，而非共用一个账号，启用登录日志和行为日志功能。针对单一账号，仅授权其需要访问的最小资源，如客服人员仅能访问客服资源，而非核心财务系统。

1.1.2.6【云服务】

信息化是目前企业经营的核心依托之一，通过采购知名云服务提供商的产品，对于备份、访问控制等都具备较为成熟的方案。如典型的客户管理，可通过企业微信进行集中化管理，避免因员工离职、未有效交接，导致客户流失问题。

1.1.2.7【主要风险点及检查措施】

针对小微企业场景的商业秘密保护方案，其主要的风险点包括：保密协议未签署、安全意识培训不足、备份策略不完善、杀毒软件未部署完全或未启用、系统账号共享行为等。

针对上述风险点，我们可采取的检查措施包括：

a）定期对新入职员工的保密协议签署进行抽样检查，特别是关键岗位人员，查看其是否签订了有效的保密条款。

b）每次安全意识培训后保留培训材料和培训人员签到表；定期对培训材料和签到表检查，确认应覆盖人员都参加了培训；不定期组织抽检关键岗位人员进行安全意识考核。

c）定期检查公司备份机制的运行情况，包括审阅备份日志记录，抽样检查备份文件的完整性和可读性，不定期执行备份文件恢复测试。

d）如果是集中部署的防病毒软件，可以通过服务端，定期查看杀毒软件在公司设备中的部署情况，并与员工名单或资产清单进行匹配，确保相关设备都有安装；如果是单机版防病毒软件，可定期或不定期根据员工名单或资产清单进行抽检，检查是否有安装防病毒软件，并且设置为即时防护和定期扫描。

e）定期进行系统账号权限核查，并与员工名单进行匹配，确保账号数量和所有者与员工一致，严格遵循“一人一账号”原则；重点检查已离职员工账号，确认是否已经被删除或禁用。

1.1.3【中型企业】

需要管理的商业秘密数量较多，涉及的员工较多，需要独立的部门负责。保护的核心思路是全面风险识别和重点风险管控相结合。在满足小微企业的建设点以外，可考虑如下措施。

1.1.3.1【信息安全管理体系建设】

常见的如《中华人民共和国网络安全法》要求的，应进行网络安全信息等级评估，或国际上广受认可的 ISO27001 认证，亦或某些行业特有的，如 PCI-DSS 支付卡行业安全认证。可通过第三方测评机构对照完整的信息安全管理体系建设的要求，明确差距，查找不足，通过技术和管理手段，进行重点防护。

1.1.3.2【关键岗位背景调查】

对涉及较多商业秘密的岗位，如数据库管理员、研发人员等，进行入职前的背景调查，防止不法分子以合法身份入职后，伺机盗取商业秘密信息。

1.1.3.3【网络隔离】

对涉及较多商业秘密的信息系统，进行网络隔离，避免同互联网进行直接连接。如采用网络层防火墙。

1.1.3.4【统一账号管理】

应建立统一账号管理系统，如常见办公环境的微软 AD 域等，所有涉及登录的系统都纳入到此系统中。有效进行员工账号的管理，避免员工离职后账号关闭不及时不全面，导致商业秘密持续泄露风险。

1.1.3.5【双因子鉴别】

对涉及较多商业秘密的信息系统，应启用双因子鉴别，如常见的手机短信验证码、动态数字动态口令等，防止关键岗位的员工因账号被窃，导致商业秘密被第三方窃取风险。

1.1.3.6【网络准入】

因企业规模增大，人员增多，可能有不法分子企图在周围入侵企

业内部 wifi，或潜入企业内部，通过网线连接的方式，入侵内网，试图窃取商业秘密。对此，可通过部署网络准入系统的方式，限定当账号有效时，才允许进入企业网络，可为企业办公网筑起第一道防线。

1.1.3.7【堡垒机】

对涉及较多商业秘密的信息系统，应启用加强版的访问控制，针对每次访问，留存访问记录，如配置堡垒机。一方面，规范内部人员有序管理商业秘密，若遇到极端情况，如删除数据等操作，可固定证据，并依据记录，提供数据恢复的思路方案；另一方面，因企业规模增大，商业秘密数量和价值提升，堡垒机可作为有效控制点，防止不法分子的入侵。

备注：“堡垒机”是指具备监控和记录运维人员操作行为功能的网络安全设备。

1.1.3.8【应用防火墙】

部分依托商业秘密开展业务的信息系统，可能对互联网开放，此时，应部署应用防火墙，减轻因自身信息系统的漏洞（如 SQL 注入等）导致商业秘密被批量窃取的风险。

1.1.3.9【数据防泄密系统】

通过对办公计算机部署管理终端、在办公网出口部署网络探针的方式，识别和拦截含商业秘密在内的敏感数据外发行为，减轻被内部员工有意或无意的外传被第三方恶意窃取的风险。

1.1.3.10【主要风险点及检查措施】

针对中型企业场景的商业秘密保护方案，其主要风险点包括：信息安全管理体系不够完善、关键岗位候选人背景调查缺失、网络隔离策略未生效、统一账号管理不完善、双因子鉴别未启用、网络准入策略未生效、数据库异常访问、敏感数据泄露等。

针对上述风险点，企业除了采用小微企业的检查措施外，还可采取以下检查措施：

a）参与第三方机构对公司的信息安全管理体系的认证审核或复核，及时了解信息安全体系的建设情况。

b）定期对关键岗位的新入职员工进行背景调查复核，确保相关调

查执行到位。

c）保留书面的防火墙配置策略，调整策略时必须要有正式的书面申请和审批；定期审计网络防火墙生产环境配置，检查与书面策略的一致性，并审阅相关策略是否能够有效隔离内外网环境。

d）定期对域控服务器进行审计，并与员工名单进行匹配，确保所有在职员工均通过 AD 域进行统一的账号管理；同时检查基础的安全域组策略是否已经部署，如复杂口令策略、最小口令长度策略、口令强制修改策略、口令历史策略、审计策略、禁用共享策略等等。

e）定期检查双因子鉴别策略设置，确认是否已启用；同时随机抽取用户进行登录测试，查看其双因子认证是否有效。

f）定期从服务端检查终端准入软件在公司设备中的登录情况，并与员工名单或资产清单进行匹配，检查是否有未经认证的设备入网；同时不定期用非公司设备测试接入公司网络，确认终端准入限制的有效性。

g）定期检查堡垒机配置，确认公司关键生产服务器均已接入堡垒机，且堡垒机限制对生产服务器的高风险命令直接操作；同时定期对堡垒机日志进行审计，检查是否有异常的线上操作命令。

h）定期检查数据防泄漏软件在公司设备中的安装情况，与员工名单进行匹配，确保部署的完整性；同时定期审计防泄漏软件的拦截和警告日志，及时发现员工的数据传输异常操作，并对其进行追因溯源调查。

1.1.4【大型企业】

需要管理海量的商业秘密，涉及的员工数量巨大，存在一定部门墙，导致商业秘密的识别和保护存在盲点。保护的核心思路是全面风险管控。在满足以上建设点以外，可考虑如下措施。

1.1.4.1【组织保障】

企业应建立独立的部门，统筹行使商业秘密保护的职责，牵头承担商业秘密识别、保护、审计等工作。

1.1.4.2【数据分类分级】

依照国家和行业要求，建立对应的数据分类分级体系，对涵盖商

业秘密在内的数据，进行全面识别和分类，以此为依托，进行分级保护。

1.1.4.3【数据不落地】

对含商业秘密在内的敏感场景，启用云终端等方式，确保员工可用基础上，商业秘密仅可查看不可下载，无有效审批，无法批量导出，防止内外部的商业秘密窃取行为。

1.1.4.4【数字水印】

在关键应用系统上，启用数字水印技术（如明水印），警示规范员工操作，不进行截屏拍照，也可使用暗水印，在商业秘密流失后追查来源。

1.1.4.5【代理】

通过使用代理模式，以虚拟号形式进行统一外呼，防止客服人员恶意获取注册用户手机等联系方式，保护客户信息。

1.1.4.6【最小授权】

通过建立统一身份验证+安全网关+微隔离的形式，授予员工工作所需的必要最小权限，既减轻内部员工恶意嗅探和窃取商业秘密的风险，也提高第三方窃取商业秘密的难度。

1.1.4.7【主要风险点及检查措施】

针对大型企业场景的商业秘密保护方案，除了中型企业的风险外，其他风险点还包括：数据分类分级体系的缺失、未经授权的数据落地行为、数字识别技术的缺失、员工账号权限过大等。

除了采用小微企业和中型企业的检查措施外，可以额外增加以下检查措施:

a）定期检查数据分类分级体系是否根据业务的变化进行及时更新，各分类数据是否都已指定明确的所有者。

b）通过 VDI 等虚拟桌面工具限制数据落地访问；定期审查 VDI 操作日志，确保无异常的数据交互行为。

c）定期选择关键系统进行随机截屏操作，查看数字水印技术是否启用生效。

d）定期选择关键系统进行抽样检查，查看敏感信息（如用户个人

数据等）是否已脱敏。

e）根据员工岗位职能制定标准的系统权限角色，形成书面的岗位角色矩阵表；根据业务变化及时更新该矩阵表；申请岗位新增权限时需有书面审批记录；定期进行系统账号权限检查，确保员工系统权限与工作岗位相一致，额外权限均有正式申请和审批，严格遵循最小授权原则。

1.2 【组织架构】

1.2.1【商业秘密保护部门】

企业应设立商业秘密保护部门或由具备商业秘密保护职能的部门开展商业秘密管理工作。

企业的分支机构、子公司和关联企业可参照企业设置商业秘密保护部门。

1.2.2【部门职责分工】

企业应明确各部门的商业秘密保护职责，划分商业秘密保护部门与其他各部门的分工与责任界限。各部门之间应建立常态化沟通与协作机制。

1.2.3【岗位职责】

商业秘密保护部门应履行以下职责:

a）界定和管理商业秘密;

b）组织员工进行商业秘密保护培训;

c）组织制订、实施商业秘密保护措施;

d）会同各部门对相关保密制度及其落实情况进行检查、督促及整改。

e）完成商业秘密泄露的证据整理、搜集、举证、协助调查取证等工作。

1.2.4【人员保障】

企业应在商业秘密保护部门内配备专职的商业秘密管理人员，或由法务、信息安全等部门人员兼任商业秘密管理工作。

1.3【信息管理】

1.3.1【商业秘密识别】

商业秘密保护部门应评估并识别商业秘密信息，并建立商业秘密清单，确定商业秘密信息、级别、保存期限、涉密人员范围等内容。商业秘密信息包括:

a）涉密技术信息：与科学技术有关的结构、原料、组分、配方、材料、样式、工艺、方法或其步骤、算法、数据、计算机程序及其有关文档等信息;

b）涉密经营信息：与经营活动有关的创意、管理、营销、财务、计划、样本、招投标材料、数据、客户信息等，以及对特定客户的名称、地址、联系方式、交易习惯、交易内容、特定需求等信息进行整理、加工后形成的客户信息。

不同行业、不同类型的企业拥有的商业秘密不尽相同。详见第 18 页【附录】

1.3.2【不属于商业秘密的信息】

下列信息不应作为企业的商业秘密:

a）公知信息和基础理论;

b）已申请并公开的专利技术信息;

c）公众可通过反向工程等合法途径获得的信息;

d）法律、法规、规章及相关司法解释规定的其他情形。

备注：最高人民法院《关于审理侵犯商业秘密民事案件适用法律若干问题的规定》（自 2020 年 9 月 12 日起施行）

第二条当事人仅以与特定客户保持长期稳定交易关系为由，主张该特定客户属于商业秘密的，人民法院不予支持。

客户基于对员工个人的信赖而与该员工所在单位进行交易，该员工离职后，能够证明客户自愿选择与该员工或者该员工所在的新单位进行交易的，人民法院应当认定该员工没有采用不正当手段获取权利人的商业秘密。

1.3.3【分级管理】

商业秘密保护部门应将商业秘密信息进行分级管理，可按重要性

分为核心秘密、重要秘密和一般秘密三个等级，并实行定期复评、动态调整。根据商业秘密的级别，采取不同的保密措施。如企业的商业秘密同时属于国家秘密的，应按照相关国家保密法规进行管理。

1.3.4【保密期限】

商业秘密保护部门应根据密级以及商业秘密自身情况确定商业秘密的保密期限。可以确定的时限以“年”“月”“日”计，不可确定的时限应定为“长期”或“永久”。

1.3.5【权限管理】

商业秘密保护部门应根据商业秘密密级和岗位职责“最小授权”原则，确定可接触的人员范围。

1.3.6【保密措施】

商业秘密保护部门应根据商业秘密的性质、载体、密级等制定相应的保密措施。

1.3.6.1【文件管理】

商业秘密保护部门应根据秘密载体对商业秘密进行如下分类管理:

a）文件资料管理：对于纸质文件资料，应做好标识管理（如：在文件资料上注明密级、保密期限等醒目标注）、权限管理等工作。

b）电子信息管理：对于电子信息，应做好安全管理（如：及时检杀病毒、修补漏洞）、权限管理、口令管理（如：对涉密设备、数据库或账户设置密码）、存储管理（如：涉密信息应存储于企业授权的存储设备和应用系统内）等工作。

1.3.6.2【场所管理】

建议企业对涉密场所和非涉密场所进行明确区分，对涉密场所设置醒目标识、门禁、监控等物理措施，对进入涉密场所的人员范围、权限、程序、允许的范围等进行明确限制。

1.3.6.3【物品管理】

对于涉及商业秘密的物品，包括但不限于员工计算机、生产设备、样品、原材料等，企业应制定具体制度管理其存放、使用、更新及销毁的过程。

1.3.7【解秘管理】

企业的商业秘密出现下列情形时，商业秘密保护部门可通过消除密级标识、电子文档解密等方式予解密:

a）企业认为商业秘密事项已不再具有保护价值的;

b）其他特定因素导致商业秘密被公开的。

1.3.8【销毁管理】

销毁涉及商业秘密的文件（含复制文件）、资料、电子信息、载体和物品，应由商业秘密管理人员列出销毁清单，经商业秘密保护部门审批后实施。销毁过程由商业秘密保护部门全程监督。

文件、资料应粉碎成颗粒状或焚烧处置，电子信息应利用彻底删除软件永久删除。

1.4【人事管理】

1.4.1【入职管理】

1.4.1.1 建议企业通过章程、制度、员工手册以及书面通知等方式，明确保密信息的范围以及员工的保密义务。同时应确定相应的保密制度已经实际送达员工并为其所知悉，例如，通过邮件发送或要求员工书面签收，并保存相应记录。

对于新入职、转岗到涉密岗位的员工，应与其签订与岗位工作内容相适应的员工保密合同/协议。

1.4.1.2 高级管理人员、高级技术人员及其他负有保密义务的人员（如职业经理人、技术、采购、销售等涉密重点岗位人员），可与其签订竞业限制协议。

1.4.1.3 涉密重点岗位员工入职前宜做背景调查，必要时应要求其作出不侵犯他人商业秘密的承诺。

1.4.2【在职管理】

1.4.2.1 员工在职期间，应督促员工遵守企业商业秘密保护制度，做好本岗位商业秘密保护工作：涉密信息及载体应及时上报，由保密员归档统一管理；使用涉密信息应履行登记手续；涉密电子文档、数据按规定途径和要求使用、流转等；离开工作岗位前及时下线工作账户，或设置计算机锁屏等。

1.4.2.2 在录用潜在竞争性关系企业的员工后，应采取特定的措施，可能包括以下方面：审核待录用的员工与原单位之间的保密约定、保密义务、保密内容及范围，以防范该员工在本企业内部公开或使用原单位的商业秘密；提醒待录用的员工不应将原单位的商业秘密带入本企业进行使用或公开，并要求就本项内容签署保证书；定期对已入职的员工所从事的业务内容进行审核，以排除使用原单位商业秘密。

1.4.2.3 商业秘密保护培训宜列入企业年度培训计划，使在职员工对商业秘密可能泄露的异常状态及承担的法律后果保持足够警觉。

1.4.2.4 应对新入职涉密岗位的人员进行商业秘密保护培训。

1.4.2.5 可采取发放资料、集中培训、网络培训或相结合的方式开展培训，保存培训记录。

1.4.2.6 签订员工保密合同/协议的人员在培训结束后宜进行考核，保存相关考核材料。

1.4.3【**离职管理**】

1.4.3.1 涉密岗位员工离职前，企业应主动告知保密义务，以及若违反规定应承担的法律责任。告知离职员工不得有以下行为：复制、带离、损毁、篡改、拍摄涉密文件资料、物品；查阅、拷贝、篡改、发送涉密电子文档、数据；删除、更改账户；披露、使用商业秘密等。

1.4.3.2 涉密岗位员工离职前，企业应提醒离职员工主动移交一切涉密载体和物品，准备离职交接清单并安排人员确认交接完成。涉密物品包括但不限于：涉密文件资料、数据以及载体、物品；账号、密码等账户信息；工作计算机；门禁卡、钥匙等。

1.4.3.3 应在员工离职后采取适当措施进行脱敏，及时回收系统权限，并及时通知与离职员工有关的供应商、客户、合作单位等，做好业务交接。

1.4.3.4 应实际开展离职检查，检查的具体内容包括：检查工作计算机数据是否完整；检查工作账户是否有异常操作，如异常查询、下载、拷贝、修改、删除等；检查工作邮箱的邮件收发记录；离职前一定期限内的涉密文档、数据的查阅和使用情况等。

1.4.3.5 应与离职涉密重点岗位工作人员签订竞业限制协议等商

业秘密保护确认文书，竞业限制应根据自身需要进行启动或解除。

1.4.3.6 应及时掌握离职员工在竞业限制期限内的任职去向。

1.5【研发管理】

1.5.1【职务商业秘密】

职务商业秘密是指员工在劳动关系存续期间，根据劳动合同的约定或在企业指定的工作中研究或开发取得的商业秘密。

1.5.2【研发成果归属】

企业与员工就职务商业秘密的归属宜以书面形式进行明确约定，未做约定的，该商业秘密系执行企业的工作任务或主要利用企业的物质技术条件完成的，应视为归属于企业。

企业委托第三方开发完成的成果属于商业秘密的，建议对相关成果的归属以书面形式进行明确约定，未做约定的，双方均享有使用和转让的权利。

1.5.3【研发成果管理】

确定归属于企业的商业秘密，企业应按照本指南开展商业秘密管理工作。

确定归属于员工或第三方的商业秘密，且该商业秘密与企业相关的，企业应与员工或第三方签署保密协议，要求员工或第三方履行保密义务。

1.6【采购承揽】

1.6.1【委托加工管理】

涉及商业秘密的委托加工，企业应与加工方签署保密协议或保密条款。

1.6.2【第三方人员管理】

企业聘任或委托专家、顾问、翻译、律师、会计师等因工作需要可能接触涉密信息的外部人员，宜做背景调查，并签订保密协议、保密条款或保密承诺书。企业可要求前述人员使用企业提供的保密计算机并对信息进行加密，需要通过企业内部网络接入涉密计算机或设备

的，应通过堡垒机采取保密措施。

1.7【销售管理】

1.7.1【客户名单管理】

对于由客户的名称、地址、联系方式以及交易的习惯、意向、内容等区别于相关公知信息的特殊客户信息组成的客户名单，企业应按照本指南开展商业秘密管理工作。

1.7.2【产品流通管理】

对于投入市场流通且涉及技术秘密的产品，企业宜采取足以对抗不特定第三人通过反向工程获取该技术秘密的保密措施，如采取一体化结构，产品拆解后技术秘密即被破坏。

1.8【财务管理】

1.8.1 企业宜对涉及商业秘密的财务信息进行严格管理，采取以下保密措施:

a）不得在不利于保密的场合谈论涉密财务信息，不得在不利于保密的位置存放纸质涉密财务资料，不得在未经批准的情况下随身携带涉密财务资料。

b）与财务相关的重要文件、软件、报告应设置秘钥，应指定专人保管，秘钥的密码应定期更换。使用人不得泄露密码，并保证秘钥和密码的使用安全。

c）对因工作原因需要查阅重大交易记录、重要财务数据的，查阅人应提出申请并逐级审批，经商业秘密管理人员最终审批通过后，方可调阅。

1.8.2 应安排专人管理网银业务系统的交易数据，管理人员必须通过严格的资信调查。企业应定期检查，确保网银业务系统的保密性。

1.9【内控内审】

1.9.1【检查和评估】

1.9.1.1 企业应定期对商业秘密保护、管理情况进行检查和评估

并形成书面报告，检查内容应包括:

a）商业秘密保护制度的适宜性、实施情况等;

b）商业秘密管理人员的履职情况;

c）涉密人员管理情况;

d）涉密区域管理情况;

e）商业秘密事项的定密、隐密、解密、分级、流转、销毁情况;

f）涉密文件资料、计算机的管理情况;

g）涉密账户、电子信息、操作系统、办公软件的管理情况;

h）电子邮箱、聊天工具、设计软件、存储软件等工具软件使用商业秘密的情况;

i）涉密载体、物品的管理情况等。

1.9.1.2 企业应采取以下措施并保留记录或原始文件用于检查和评估:

a）重要涉密区域的出入口和内部应安装监控系统实时监控;

b）涉密网络的出、入口应实时监控;

c）涉密计算机的操作;

d）存储商业秘密信息的信息系统;

e）对外发送商业秘密信息的软件，如电子邮箱、即时通讯软件等。

1.9.1.3 企业可根据自身情况，委托第三方专业机构对企业商业秘密管理情况进行评估。

1.9.2【纠正和整改】

1.9.2.1 企业发现有泄密情况及隐患的，应及时采取纠正或预防措施。

1.9.2.2 企业应针对定期评估报告发现的管理漏洞制定改进方案、整改计划并严格执行。

1.9.2.3 企业应对商业秘密保护制度落实环节中存在的问题对相关责任人进行约谈、问责。

1.9.2.4 企业应对整改情况定期进行复查、复评。

1.10【对外合作】

1.10.1【外部人员访问管理】

1.10.1.1 外部人员进入企业应出示证件并履行登记程序，佩戴与企业内部员工不同颜色的出入卡。

1.10.1.2 外部人员访问涉密区域应经审批并进行登记，告知其禁止录音、摄影、摄像、使用便携机、移动存储介质等设备，限制手机等器材的拍摄功能，并安排专人全程陪同。

1.10.1.3 外部人员进入企业参观的，应设置专门的参观路线以避开涉密区域，参观路线上可能涉及的商业秘密信息应采取隐蔽措施。

1.10.2【项目合作管理】

1.10.2.1 在商务合作、共同研究及涉及商业秘密的交易、公证、保险等活动时，企业应与外部合作方签订保密协议，或在合同条款中规定保密要求，约定保密内容和范围、保密义务及违约责任等。

1.10.2.2 在共同或委托开发的项目合作中，企业应采取措施防止侵犯他人商业秘密，签订保密协议对涉及商业秘密等知识产权的权利归属和使用权作出约定。

1.10.2.3 涉密项目需要长期向外部合作方提供商业秘密信息的，或因维修、研发等需要经常进入涉密区域的，企业可要求外部合作方采取以下保密措施:

a）与参与项目的外部合作方员工签订个人保密协议;

b）使用企业提供的保密计算机;

c）使用企业提供的加密系统;

d）使用企业提供的加密存储介质;

e）对外部人员使用的便携机等设备进行检查。

1.10.3【会议及活动管理】

在涉及商业秘密的会议或其他活动中，企业宜采取以下保密措施:

a）选择具有保密条件的场所;

b）尽量避免使用远程视频、音频、电话会议等线上会议方式，如必须采用的，应采取会议密码、屏幕水印等保密措施;

c）根据工作需要，限定参加人员的范围，指定参与涉密事项的人员;

d）告知参加人员保密要求，必要时签订保密承诺书；

e）对涉密文件、资料进行控制，如：确定文件发放范围，做好发放登记；重要涉密文件资料应有明显保密和会后回收标识；休会或会议结束时，及时收回清点、登记。

【附录】不同行业企业需要重点保护的商业秘密信息

【科学研究和技术服务企业】

涉及到的重要商业秘密可能包括:

1.技术研发和创新：与企业科研技术、创新及产品设计制造有关的任何设计、程序、公式、产品配方、制作工艺、制作方法、研发记录、实验数据、技术诀窍、技术图纸、编程规范、计算机软件源代码、独特的数据集、软件算法、数据分析方法、数据模型、技术方案、统计算法和有关文档等信息。

2.内部运营及管理：企业内部独特的业务流程、操作方法、服务标准、人力资源管理（培训材料、员工手册、薪酬福利方案等）、商业模式、质量控制、资源分配、供应链管理、流程优化方案等。

3.品牌和市场策略：企业未公开的市场调研数据，如市场研究报告、潜在客户分析、竞争对手情报及分析、市场需求趋势分析等企业调研所得的相关数据和信息；企业未公开的商业计划、销售策略、定价策略、商标注册信息、品牌推广计划、广告策略、市场定位、公关活动方案等信息；与企业品牌和声誉有关的信息等。

4.商业合作和合作伙伴关系：合作方名单、与合作方之间的交易合同、定价策略及相关细节，如合同期限、价格、保证金、违约条款等信息。

5.客户信息：企业所拥有潜在和现有的客户信息，如客户名单、个人资料、需求偏好、消费意向、消费能力、交易细节、合同内容、客户需求和反馈、客户关系管理等信息。

6.财务信息：本企业未公开的投资成本、预计收益、利润率、财务报表等相关财务信息。

7. 保密协议和保密措施：与客户、合作伙伴和员工签署的保密协议和合同，以及企业采取的保密措施和安全控制措施等。

（2、3、4、5、6、7 项为共性信息，以下不再罗列）

【信息传输、软件和信息技术服务企业】

涉及到的重要商业秘密可能包括:

1. 软件源代码：企业开发的软件源代码，包括应用程序、算法、数据库设计等。这些源代码是企业的核心竞争力和独特价值所在，通常应被视为核心商业秘密。

2. 技术解决方案和开发流程：企业独特的技术解决方案和开发流程，包括用于开发和实施的软件系统、网络架构、数据管理等。

3. 数据安全和隐私保护措施：企业实施的数据安全和隐私保护措施，包括加密技术、访问控制、数据备份等。

4. 客户数据和业务需求：企业积累的大量客户数据和业务需求，包括业务流程、用户行为分析、市场趋势等。

【制造企业】

涉及到的重要商业秘密可能包括:

1. 产品设计和创新：企业特有的产品设计和创新，包括产品的外观、功能、技术、材料和制造流程等。

2. 生产流程和工艺：特殊的生产流程和工艺，包括制造过程中的专有方法、工艺参数、设备配置和优化等方面信息。

3. 物料供应链和采购：包括供应商的选择、采购策略、合同条款和定价等。

4. 质量控制和标准：企业独有的质量控制和标准，包括制定和执行质量控制程序、测试方法、质量标准和认证标准等。

【房地产企业】

涉及到的重要商业秘密可能包括:

1. 土地资源、交易信息：包括企业未公开的土地供应计划、用途

规划、开发潜力、开发成本、投资预测、交易合同、价格和出让方式等信息。

2.项目计划和投资决策：包括企业未公开的项目规划、用地规划、项目规模、设计方案、市场定位、建设进度、商业计划书、投资方案、资金筹集方案、财务数据和预测等。

3.建筑设计和施工技术：包括企业未公开的建筑/结构设计图纸、施工工艺、结构技术、装修材料的选择方案等。

4.内部运营及管理：包括企业未公开的运营流程、操作手册、管理制度、人力资源策略（培训材料、员工手册、薪酬福利方案等）等信息；物业管理方案、维护计划、维修和保养记录、物业运营成本和收益等内部管理信息。

【建筑企业】

涉及到的重要商业秘密可能包括:

1.设计方案：企业特有的设计理念、方法和技巧，包括设计方案、建筑外观、结构、功能布局、材料选用等。

2.技术和工艺：企业独特的建筑技术和工艺，包括新型结构系统、高效的施工方法等。

3.商业模式和运营策略：企业独有的商业模式和运营策略，包括市场定位、项目选择等。

【金融企业】

涉及到的重要商业秘密可能包括:

1.金融产品和服务设计：企业特有的金融产品和服务设计，包括银行产品、保险产品、投资组合、特定定价模型、风险评估方法和创新金融工具等。

2.风险管理和合规措施：企业的风险管理和合规措施，用于评估和管理风险，包括特定风险模型、内部控制流程、合规程序等。

3.企业处理的敏感数据，包括个人身份信息、财务信息等。

4.企业进行的各类金融分析和研究：包括市场趋势分析、股票研

究报告等，以及这些分析和报告包含的特殊见解、数据分析方法和研究成果等。

5.金融交易和交易策略：企业独有的金融交易和交易策略，包括股票交易、外汇交易、衍生品交易等，以及这些交易和策略涉及的交易模型、算法和高频交易技术。

【交通运输、仓储和邮政企业】

涉及到的重要商业秘密可能包括:

1.运输网络和路线优化：企业独特的运输网络和路线优化策略，包括仓储设施位置、运输路径选择、交通规划，以及可能涉及的整合物流资源、提升运输效率的手段等。

2.物流管理和供应链优化：企业特有的物流管理和供应链优化策略，包括货物装卸、仓储管理、订单处理、运输调度等。

3.信息技术和数据分析：企业拥有先进的信息技术和数据分析能力，用于物流追踪、库存管理、运输计划等，由此形成的内部资料。

4.安全和风险管理：企业实施的安全和风险管理策略，包括货物保险、安全检查、灾难应急预案、安全措施、风险评估等。

5.客户信息和物流需求数据：企业积累的大量客户信息和物流数据，包括货物特性、运输需求、收货人信息等。

【文化、体育和娱乐企业】

涉及到的重要商业秘密可能包括:

1.艺术作品和创作内容：企业独特的艺术作品和创作内容如音乐、电影、舞蹈、戏剧、文学作品等，包括这些作品的创作过程、创意构思、创作技巧和未发布的作品等。

2.艺术表演和演出方案：企业独特的艺术表演和演出方案，包括演出流程、节目选择、舞台设计、灯光音效等。

3.体育训练和战术：企业独特的训练方法和战术策略，用于提高运动员的竞技水平，包括训练方法、战术计划和技术指导等。

4.商业合作和版权授权：企业与其他企业或个人进行商业合作或

版权授权，包括合作协议、商业合作细节、版权授权范围和条件等。

【批发零售企业】

涉及到的重要商业秘密可能包括:

1.供应链和采购策略：企业独特的供应链管理和采购策略，包括供应商选择、采购合同、库存管理等。

2.商品选择和定位策略：企业独特的商品选择和定位策略，包括产品种类、品牌选择、定价层次等。

3.销售和市场推广策略：企业独特的销售和市场推广策略，包括促销活动、广告策略、渠道选择等，以及这些策略涉及的特定销售技巧、营销渠道、目标市场。

4.网络销售和电子商务策略：企业独特的网络销售和电子商务策略，包括在线平台、物流管理、支付系统等。

【教育培训企业】

涉及到的重要商业秘密可能包括:

1.教学课程和教材：企业自主开发的教学课程和教材，包括教学大纲、教学计划、教学方法和教材内容等。

2.教育技术和在线平台：企业自主开发在线学习平台、教育应用程序或教育技术工具，这些软件的源代码、设计原理、功能和性能等信息。

【餐饮企业】

涉及到的重要商业秘密可能包括:

1.特色菜品的制作工艺：企业特色菜品的独特调味方法、烹饪工艺等。

2.供应链管理和食材采购：企业独特的供应链管理和食材采购策略，帮助企业确保食材新鲜度和质量，包括供应商选择、采购渠道、食材质量控制等。

【水利、环境和公共设施管理企业】

涉及到的重要商业秘密可能包括:

1.环境调查和评估数据：企业在进行环境调查和评估时，可能收集大量关于土壤、水质、空气质量等方面的数据,如监测结果、采样方法、分析技术和解释等。

2.专有技术、知识及解决方案：包括企业用于处理水资源、净化水源、保护环境等方面的特殊技术、软件系统、数据分析工具、专有算法等；企业的项目方案、设计图纸、施工计划、设备选型等；企业的技术解决方案，如技术设计、工艺流程、设备改进、节能减排方案等。

【农业、林业、渔业企业】

涉及到的重要商业秘密可能包括:

1.品种选育和改良：企业经过多年选育和改良，拥有产量高、抗病虫害能力强或其他特性的农作物品种，这些农作物品种的具体参数、种植技术、选育方法、繁殖材料、培养数据等信息。

2.生产工艺和技术：企业独自开发的可用于提高农产品质量和产量的生产工艺和技术，包括种植、施肥、灌溉、病虫害防治等方面的专有知识。

3.林业种植和育苗技术：企业独特的林木种植和育苗技术，包括育种、繁殖和生长管理等技术。

4.森林病虫害防治技术：企业独特的能促使林木健康生长且提高产量的病虫害防治技术等。

5.渔具和渔船技术：企业具有特殊运用场景的渔具和渔船技术，包括渔网、钓具和船舶设计方案、设计图纸等。

6.养殖和养护技术：企业独特的用于提升渔场鱼苗质量、产量的养殖和养护技术，包括鱼苗育种、鱼苗养殖、水质管理和疾病控制、生态保护和可持续渔业管理技术等。

【相关案例】

问题：对企业经营中的电子数据类信息可以采取哪些有效的保密措施?

案例：新赛点体育公司案

来源：（2018）京73民终686号

案情简介：原告公司经营中国高尔夫网，为多家银行的高端客户提供高尔夫球增值服务。被告金某等五人曾分别在原告公司就职，其与原告公司签订的《劳动合同书》《商业秘密保密合同》《员工手册确认书》中明确约定，“乙方在甲方工作期间所获悉的商业秘密，包括但不限于公司资料、文件、信息、软件、数据库及其他公司的信息资料（包括但不限于书面资料、电子文本、照片等）；乙方从甲方获得的与项目有关或因项目产生的任何商业、营销、技术运营数据或其他性质的资料”，并列明了保密义务和例外情形。原告公司将其与高尔夫球场、银行等合作的信息通过MIS系统和21Golf管理系统进行管理，对不同部门、级别的员工根据岗位设置了不同的操作使用权限。被告从原告公司辞职后，加入被告新赛点体育公司（全称：北京新赛点体育投资股份有限公司），将原告公司与相关银行的合作信息、交易价格等披露给新赛点公司，使新赛点体育公司成功以类似价格与特定银行签约成功。法院经审理后认为，原告公司对其主张的与银行合作的信息采取了合理保护措施，该部分经营信息属于商业秘密。新赛点体育公司、金某等5人应承担侵权责任。

解读：本案中，原告公司对经营中产生的电子数据信息采取了以

下几种叠加的保密措施：第一，在相关协议中对保密信息的范围以及多样化的电子数据载体，采取“列举+兜底”的方式进行具体的约定；第二，对银行、高尔夫俱乐部等相关经营信息通过专门的信息系统进行管理，并对不同部门、级别的员工设置了不同的操作权限；第三，对上述措施做好相关记录，留存证据。在诉讼中相关证据被认定为采取了有效的保密措施，进而认定相关信息属于商业秘密，应受保护。

问题：通过发放员工手册约定的竞业限制是否有效？

案例：杭州某舞蹈培训公司诉左某竞业限制案

来源：(2012)浙杭民终字第 2913 号

案情简介：2011 年 7 月杭州某舞蹈培训公司与左某签订书面《劳动合同书》及《保密协议》，但未约定竞业限制条款。2012 年 2 月左某申请离职，于同年 5 月到另一舞蹈学校从事教学工作。杭州某舞蹈培训公司诉至法院，提交《员工手册》一份，上面约定了竞业限制的时间、地域范围、补偿金额和支付时间，但未能证明左某实际签收过该《员工手册》。法院认定原告提交的证据不能充分证明载有竞业限制条款的《员工手册》被左某签收，判决原告败诉。

解读：企业与劳动者约定竞业限制，应尽可能在《劳动合同》《保密协议》或《竞业限制协议》中，对竞业限制的范围和期限等作出明确约定，而不是仅体现在单方发放的《员工手册》中。

如果《员工手册》中对竞业限制的具体内容、时间、区域、补偿金的金额及支付进行了明确约定，而且《员工手册》有员工的书面签收确认，应视为有效，对员工具有约束力，建议企业留存相关的书面签收确认单。

问题：企业和员工约定了竞业限制条款，但没有实际支付竞业限制补偿款的，能否要求员工承担竞业限制的违约责任？

案例：A 珠宝公司诉马某、B 珠宝公司不正当竞争纠纷案

来源：（2006）苏民三终字第 0018 号

案情简介：2001 年，A 珠宝公司与马某签订协议，聘请马某为公

司的副总经理，同时约定马某因解聘、辞职、退休等原因离职起二年内，不能自行从事同类业务或受雇于与A珠宝公司同类业务的公司。2004年，马某与他人成立B珠宝公司，马某担任法定代表人。B珠宝公司与A珠宝公司经营范围均与生产销售金属首饰、工艺品相关。A珠宝公司将马某与B珠宝公司诉至法院，诉讼中，法院查明竞业限制协议中未约定补偿金，其亦未实际向马某支付补偿金。故法院认定竞业限制条款无效，马某无需承担违约责任。

解读：根据权利义务对等原则，企业应主动向员工支付竞业限制补偿金。如果竞业限制协议中未约定补偿内容（包括补偿金的计算方式、支付时间等），或虽然约定，双方劳动合同关系结束后没有实际给予劳动者竞业限制补偿金的，劳动者无需承担违反竞业限制的违约责任。

问题：企业能否以奖金、分红等代替竞业限制补偿金？

案例：A印刷公司诉薛某、B印刷公司不正当竞争纠纷案

来源：（2006）苏民三终字第0027号判决书

案情简介：薛某曾任A印刷公司技术质量部部长，并为公司的股东之一。2003年，薛某提出辞职并至某B印刷公司担任总经理助理职务。后A公司以薛某违反竞业限制约定为由诉至法院，同时A公司认为薛某在A公司任职期间所获得的奖配股、红利筹等应视为竞业限制补偿金。法院判决A公司败诉。

解读：本案中企业支付的奖配股、红利被法院认为系员工基于股东身份获得，不能视为公司对员工支付的竞业限制补偿金。建议企业对竞业限制补偿金进行明确清晰的约定并单独支付。竞业限制补偿金的金额应能体现对劳动者就业自由限制的合理补偿，如果过低其效力也可能受到质疑。

问题：企业销售环节的单个或少量客户信息能否作为商业秘密保护？

案例：上海可可庄公司案

来源：（2008）沪一中民五（知）终字第 3 号判决书

案情简介：吴某原为可可庄公司的员工，在可可庄公司工作时与某外国客户进行了长时间的联系以及业务洽谈。后吴某离职，自行出资设立公司，并与该外国客户发生了一笔交易，该交易与吴某在可可庄公司工作时与该客户业务洽谈有关。经查明，原告可可庄公司对其客户名单采取了保密措施，包括：在业务员参加广交会等各种会展后将客户的名片装订成册，同时将客户的信息整理后输入数据库中；通过公司服务器为业务员设置电子邮箱，以便于业务员与客户进行业务联系，邮箱设置时由原告法定代表人设定密码，除原告法定代表人及业务员本人外，他人无法看到业务员邮箱中的邮件内容。法院审理后认定该特定外国客户的信息构成商业秘密，吴某的行为构成商业秘密侵权。

解读：客户名单是否能作为商业秘密保护，主要取决于客户信息的深度，而非客户的数量。少量甚至单个客户的信息如果能为企业带来商业价值且采取了相应保密措施，也可以受到保护。

问题：市场流通产品贴“危险！私拆担保无效！”警示标志可否视为采取了相应的保密措施?

案例：济南思克公司与济南兰光公司侵害技术秘密纠纷案

来源：（2020）最高法知民终 538 号

案情简介：思克公司生产并在市场上销售气体透过率测试仪。该测试仪生产过程中使用了思克公司的技术秘密。思克公司向法院起诉称，被告兰光公司通过恶意发起的诉讼、利用另案的保全程序取得原告生产的测试仪，获取了原告的技术秘密，并运用在被告产品生产中，构成商业秘密侵权。原告提出，对上述技术秘密已经采取合理的保密措施，包括：原告在测试仪的特定位置贴有标签，载明“危险！私拆担保无效！”“SYSTESTER 思克品质保证撕毁无效”等内容；在与客户签订的《设备购销合同》中约定，“该气体透过率测试仪产品的转让不意味着客户公司取得该产品的任何知识产权，且客户公司需承担确保该产品技术机密信息安全以及不得将技术机密信息提供给任何第三

方的合同义务”。

法院审理后认为，原告与客户签订的合同，仅具有约束客户的效力，由于《设备购销合同》并未限制客户对所购买的产品进行处分、转让，故不特定第三人可通过市场流通取得该产品，且不受《设备购销合同》的约束。另一方面，原告在测试仪上贴的标签内容属于安全性提示与产品维修担保提示，且无法约束后续受让产品的不特定第三人，故不构成以保密为目的的保密防范措施。最终，法院认定原告未采取相应的保密措施，其主张的技术信息不构成受反不正当竞争法保护的商业秘密。

解读：对于承载了技术秘密的产品，一旦进入市场流通，就脱离了权利人的物理控制，其采取的保密措施应与始终处于权利人控制之下的技术图纸、配方文档等内部性载体相区别。我国法律规定，他人通过自行开发研制或反向工程获得被诉侵权信息的，不构成商业秘密侵权。因此，权利人对市场流通产品这类外部性载体采取的保密措施，应足以对抗不特定第三人通过拆卸、测绘、分析产品获得产品的相关技术信息（即反向工程）。比如采取一体化结构生产，拆解产品将破坏技术秘密等。仅在产品上贴“危险！私拆担保无效！”的标签，更多属于产品安全性提示，且系思克公司的单方声明，不能约束后续通过转让等途径取得产品的他人对产品进行拆解等自由处分行为，故不属于与商业秘密的性质、载体相适应的保密措施。

2.民事保护

2.1【当事人主体资格】

2.1.1【一般情形】

商业秘密的权利人及被许可使用人有权作为原告提起侵害商业秘密诉讼或申请商业秘密仲裁。其中独占许可被许可人可单独起诉，排他许可被许可人可与权利人共同起诉或在权利人不起诉情况下自行起诉，普通许可被许可人可与权利人共同起诉或经权利人书面授权单独起诉。

2.1.2【确认不侵害商业秘密之诉】

被商业秘密权利人发送侵权警告的相对方可向权利人发出诉权行使催告。若权利人未在合理期间内起诉，则该相对方有权提起确认不侵害商业秘密之诉。

2.2【主管与管辖】

2.2.1【主管】

若原、被告间存在合同关系且就商业秘密问题存在有效仲裁条款，宜向仲裁机构提起仲裁。

若原、被告间存在劳动合同关系，原告主张被告违反竞业限制协议，应适用劳动争议解决程序，不宜直接起诉。

2.2.2【管辖】

因侵害商业秘密案件属于侵权之诉，依法由侵权行为地或被告住所地法院管辖。

侵权行为地包括侵权行为实施地和侵权结果发生地，如非法获取商业秘密地、侵权产品制造地等，但不宜至原告住所地、侵权产品销售地、收货地等地法院起诉。

在本市范围内，技术秘密民事纠纷案件由上海知识产权法院管辖，但诉讼标的额在2亿元以上或者诉讼标的额在1亿元以上的涉外、涉

港澳台及当事人一方住所地不在本市的技术秘密民事纠纷案件由上海市高级人民法院管辖；经营秘密民事纠纷案件一般由各区法院按辖区管辖。也就是说，侵权行为地或被告住所地在浦东的经营秘密民事纠纷案件由浦东新区人民法院管辖。

2.3【诉讼请求、事实及理由】

2.3.1【明确秘点】

原告应在一审法庭辩论终结前明确商业秘密的具体内容即秘点。建议出具书面的秘点说明，指出哪些技术、经营或其他信息需要保护，这些信息与原告提交的信息载体间是何关系，并将其中的公有领域信息予以剔除，而非笼统地将某载体如文件、图纸、软件整体主张为商业秘密。

2.3.2【明确行为类型】

原告应明确其主张的侵权行为类型，是非法获取、披露、使用、允许他人使用还是教唆、引诱、帮助他人违反保密义务侵害商业秘密，并明确各被告是否共同侵权及是否承担连带责任。

2.3.3【明确责任承担方式】

原告应提出明确、具体、可执行的责任承担方式，包括停止侵害、赔偿损失及合理开支等。

因侵犯商业秘密受到损害的权利人的赔偿数额，按照其因被侵权所受到的实际损失确定；实际损失难以计算的，按照侵权人因侵权所获得的利益确定。权利人因被侵权所受到的实际损失、侵权人因侵权所获得的利益难以确定的，由法院根据侵权行为的情节判决给予权利人五百万元以下的赔偿。

侵权人恶意实施侵犯商业秘密行为，情节严重的，法院可在按照上述方法确定数额的一倍以上五倍以下确定赔偿数额。

合理开支系权利人为维权支出的费用，包含取证费、律师费、翻译费、侵权产品购买费、差旅费等。

案件受理费、保全费属于诉讼费，由法院依职权处理，无需作为诉请提出。诉讼过程中产生的司法鉴定费，法院根据诉讼结果决定如

何负担。

备注：根据《上海市浦东新区建立高水平知识产权保护制度若干规定》第十条规定，故意侵犯商业秘密，情节特别严重的，法院可在按照上述方法确定数额的五倍以上十倍以下确定赔偿数额。上述金额难以确定，由法院根据侵权行为的情节判决给予权利人一千万元以下的赔偿。

2.4【证据准备及证明标准】

2.4.1【原告的证明责任】

当事人对自己提出的主张应及时提供证据。原告应在法院确定的举证期限届满前提出证据，无正当理由逾期提供证据可能不被采纳或虽被采纳但受到训诫、罚款处罚。

2.4.2【权利证据】

原告可提供开发商业秘密的证据以证明所有权，例如研发报告、证人证言、客户或经营信息表格、交易合同及发票等；可提供转让、许可或授权合同等证据以证明使用权。

2.4.3【秘密性、价值性及保密性】

原告应证明其主张的商业秘密具备三个特征，即不为公众知悉、具有商业价值以及采取保密措施。对于技术信息可采用类似权利要求方式固定秘点或由第三方专业机构出具检索报告；对于经营信息应列明每个秘点的名称及内容。商业价值的证明可提供开发成本或获利的相关证据佐证。保密措施需达到在特定范围内足以达到防止泄露的合理标准，如提供协议、规章、标注、权限等形式的证据。

2.4.4【客户信息的证明标准】

对于属于经营秘密的客户信息，内容除名称、地址、联系方式外，还应满足深度信息和交易稳定性的要求，能体现出客户特别需求、交易习惯等特殊信息。

2.4.5【被告的证明责任】

若原告提供初步证据证明其主张商业秘密的具体内容、已采取的保密措施以及被侵权事实，则被告应证明原告主张不属于商业秘密或

者系合法获得。

2.4.6【侵权推定】

若原告证明被告信息与原告商业秘密相同或实质性相同，且被告有接触原告商业秘密的条件后，除非被告能证明其有合法来源，否则法院可推定被告采取不正当手段侵犯商业秘密。

2.4.7【惩罚性赔偿的证明标准】

原告主张惩罚性赔偿应证明被告恶意实施商业秘密侵权行为且情节严重。

2.5【诉讼过程中的保密措施】

2.5.1【不公开审理】

当事人可以视情况向法院申请不公开审理。

2.5.2【人员限制】

当事人可以申请法院对接触涉及商业秘密相关证据或信息的诉讼参与人员范围作出相应限制。

2.5.3【涉密证据质证】

当事人可以对证据交换和质证方式提出意见，在法庭主持下确定涉密证据的开示方式。

2.5.4【裁判文书上网屏蔽】

涉及商业秘密的裁判文书上网公开时法院会进行相应的信息屏蔽处理。

2.6【证据保全与行为保全】

2.6.1【证据保全】

在证据可能灭失或以后难以取得的情况下，当事人可以在诉讼过程中向法院申请保全证据。商业秘密侵权诉讼的证据保全主要集中在被告侵权行为及被告侵权获利两方面，常见的有被告往来邮件、合同、生产技术资料、财务账册等。原告应明确秘点并提供被告侵权及存在取证困难或证据灭失风险的初步证据，并且在举证期限届满前提出证据保全申请，否则可能不被法院准许。

原告能够自行获得或公证固定的证据，无需向法院申请证据保全，可自行至市场监管、税务、海关等部门调取。

证据保全可能需要提供担保，复杂情况会涉及鉴定或审计。

2.6.2【行为保全】

在侵权行为可能对原告合法权益造成难以弥补的损害或使案件裁决难以执行情况下，原告可向法院申请对被告采取行为保全措施。

【相关案例】

问题：违反竞业限制义务是否等于侵犯商业秘密？

案情简介：被告系原告公司员工，与原告签有竞业限制协议。离职后，被告成立与原告存在竞争关系的公司。原告以商业秘密侵权诉至法院，认为被告在公司经营中必然会使用到原告的商业秘密，但没有得到法院支持。

解读：违反竞业限制协议的行为可能同时构成违约与商业秘密侵权。但并不是所有的违反竞业限制协议的行为都能构成商业秘密侵权。如果原告不能证明自己拥有商业秘密，且被告采取了不正当手段侵犯其商业秘密，则不能主张商业秘密侵权，只能提起违反竞业限制的违约之诉。

问题：商业秘密的载体是否等同于商业秘密？

案情简介：原告诉称，被告自 2006 年 5 月起在原告处从事电脑动画和效果图制作工作，其制作的动画展示了高科技生态低碳建筑技术安装体系施工流程。被告离职后将包含上述施工流程的动画以光盘形式广为散发。原告主张该动画文件是原告的商业秘密，未得到法院支持。

解读：动画文件仅仅是原告主张商业秘密的载体。商业秘密的载体和具体内容不能等同。原告主张商业秘密，除提供商业秘密载体外，还应明确商业秘密的具体内容，仅仅载体本身不能构成商业秘密。

问题：未明确商业秘密具体内容的法律后果是什么？

案例：M 公司诉 S 公司等侵犯商业秘密纠纷案

案情简介：该案中原告主张两种产品的技术配方、技术诀窍是其技术秘密，但仅提交了说明书和产品标签，未得到法院支持。

解读：说明书和产品标签中仅有对产品配方、成分等概括性的描述记载，而无技术配方、技术诀窍的具体内容。原告主张技术配方、技术诀窍构成其商业秘密，应明确构成商业秘密的技术配方和诀窍是什么，即应明确商业秘密的具体内容。否则，法院无法判断其主张商业秘密的信息是否符合法律规定的构成要件，被告也无法针对性地提出公知技术信息等抗辩。

问题：已经公开的信息能否构成商业秘密？

败诉案例 1：被告离开公司前，将原告客户发给原告的招股说明书发送给了案外人。原告认为，客户不希望其发给原告的内容被同行所知，原告对此负有保密义务，同时该招股说明书对原告而言也是重要的商业机会，因此被告行为构成商业秘密侵权。法院经审理查明，该说明书“项目背景”部分明确标注了该方案系向国内知名管理咨询公司、IT 系统开发商公开征集。故法院没有认定该招股说明书构成商业秘密。

败诉案例 2：原告主张项目方案、合作方的时间安排、制度汇编和公司组织结构等构成经营秘密。法院经审理查明，项目方案系原告向国内公开征集，制度汇编涉及的各项管理规定多为业内公知的一般性操作规范，公司组织结构等在原告公司的自建网站上可以查阅，该四项信息均不构成商业秘密。

败诉案例 3：原告将已申请专利的技术主张商业秘密，没有得到法院支持。

解读：商业秘密应具有秘密性，已经通过网络或其他途径公开了的信息不构成商业秘密。对于专利技术而言，由于专利申请均会向社会公布，已经申请专利或正在专利申请中的技术均不宜主张商业秘密。

问题：权利人自行披露的信息能否认为他人非法获取？

案情简介：原告系案外人 D 公司的独家经销商，原告曾与 D 公司签订协议，约定在合作期间，原告的客户信息是共享的，原告会将其交易的具体信息（包括采购联系人、电话、电子邮箱、产品、价格、一年的销售额等）抄送给 D 公司，也不要求其保密。D 公司每月会与原告一起去拜访客户。被告 S 公司系 D 公司投资设立的子公司。原告认为 S 公司取得原告的客户信息系非法，构成商业秘密侵权，但未得到法院支持。

解读：D 公司取得原告的客户信息系原告自行披露，原告亦未与 D 公司签订保密协议。S 公司系 D 公司投资成立的子公司，其从 D 公司取得

原告的客户信息并不违法，具有合法的来源。

问题：仅说明客户名称能否被认定为商业秘密？

案情简介：原告系多年从事进出口业务的公司，被告以前系原告业务员。原告提交了10家客户名称，认为该10家客户名称是商业秘密，被告与其他公司串通，与原告客户交易，构成商业秘密侵权。但法院没有支持其主张。

解读：客户名称本身并不能构成商业秘密，能够作为商业秘密保护的客户名单一般是指客户的名称、地址、联系方式以及交易的习惯、意向、内容等构成的区别于相关公众信息的特殊客户信息。对于该些信息原告应进行举证或说明，否则难以认定其构成商业秘密。

问题：主张特定客户属于商业秘密是否应证明该客户与原告存在长期稳定的交易关系？

案情简介：被告曾是原告员工，在原告处工作期间成立公司并与某客户进行交易。原告认为该客户是原告的商业秘密，被告构成侵权，但原告仅提供了某年自己与该客户交易的两张总价为5000多元的凭证。法院没有认定该客户信息构成原告的商业秘密。

解读：原告要主张某特定客户信息构成其商业秘密，应证明该客户与原告存在长期稳定的交易关系，否则诉请难以得到支持。

问题：申请法院对被告侵权证据采取措施是否应提交被告侵权的初步证据？

案情简介：被告曾系原告员工，离职后成立A公司。原告听客户反映A公司与原告客户进行交易，于是向法院申请调查令，调查A公司账册。法院要求原告提供被告侵权的初步证据，但原告未能提交，法院未予签发调查令。

解读：调查令是法院授权当事人的代理律师进行调查取证的文书。当事人申请法院签发调查令调查被告侵权行为，应提供被告实施了侵权行为的初步证据，再由法院决定是否予以签发。否则，法院便代替

了一方当事人取证，有失公正。

3.行政保护

3.1【查处部门与管辖】

3.1.1【查处部门】

市场监管部门（机构改革前的相应职能部门为工商部门）为侵犯商业秘密行为的查处部门。市市场监管部门负责指导、协调本市侵犯商业秘密行为的预防和查处工作，查处本市重大、跨区等侵犯商业秘

密行为。区市场监管部门负责本行政区域内侵犯商业秘密行为的预防和查处工作。

3.1.2 【管辖】

侵犯商业秘密行为由违法行为发生地的县级以上市场监管部门管辖。违法行为发生地包括违法行为着手地、实施地、经过地、结果地。

3.2 【立案】

市场监管部门可依据监督检查职权或者通过投诉、举报、其他部门移送、上级交办等途径发现涉嫌侵犯商业秘密的违法行为线索。实践中较常见的途径是举报。

3.2.1【举报渠道】

权利人可通过以下渠道向市场监管部门举报:

a）实名注册并登录全国 1235 平台（网址：www.12315.cn）进行举报。

b）拨打上海市场监管部门投诉举报热线 021-12315 或市民热线 021-12345 进行举报。

c）向辖区内市场监管部门进行举报。

3.2.2【举报材料】

权利人请求市场监管部门查处涉嫌侵犯商业秘密行为的，应提供商业秘密的具体内容、已采取的保密措施以及被侵权事实等初步材料。权利人合理表明商业秘密被侵犯，可提供以下证据之一:

a）有证据表明涉嫌侵权人有渠道或有机会获取商业秘密，且其使用的信息与该商业秘密实质上相同;

b）有证据表明商业秘密已经被涉嫌侵权人披露、使用或有被披露、使用的风险;

c）有其他证据表明商业秘密被涉嫌侵权人侵犯。

3.2.3【核查期限】

市场监管部门自发现线索或收到材料之日起十五个工作日予以核查，并决定是否立案。特殊情况下可延长十五个工作日。检验、检疫、鉴定以及权利人辨认或者鉴别等所需时间，不计入前述期限。

权利人举报后如对主张的涉密信息进行相关鉴定的，鉴定所需时间不计入核查期限。

3.2.4【立案条件】

经核查，符合下列条件的违法线索，应立案：

a）有明确的违法嫌疑人；

b）有证据初步证明存在侵犯商业秘密行为；

c）属于本部门管辖；

d）在给予行政处罚的法定期限内。

注：《行政处罚法》第三十六条规定，违法行为在二年内未被发现的，不再给予行政处罚。

3.3 【调查】

市场监管部门调查涉嫌侵犯商业秘密行为时，可采取现场检查、询问、查询和复制资料、查封或扣押财物、查询经营者银行账户等措施。

3.3.1【现场检查】

市场监管部门执法人员进入涉嫌侵犯商业秘密的经营者经营场所进行检查，并制作现场笔录，载明时间、地点、事件等内容。

3.3.2【查封和扣押】

经权利人申请并提供初步证明，市场监管部门可将在调查过程中发现的与涉嫌侵犯商业秘密行为有关的场所、设施或财物进行查封或扣押。对涉案的合同、票据、账簿、凭证等资料，执法人员采取信息化手段或者通过影印、复印等方式能够及时有效固定证据的，不予实施查封、扣押措施。

涉嫌侵犯商业秘密行为涉及计算机存储信息的，可能需要查封、扣押相关计算机服务器、主机、硬盘等存储设备。查封、扣押后及时通过复制、镜像、摄像、截屏、数据恢复等方式固定证据。

查封、扣押应当符合《中华人民共和国行政强制法》和《市场监管领域不予实施行政强制措施清单》的规定。

3.3.3【委托鉴定】

权利人、涉嫌侵权人可以委托有法定资质的鉴定机构对权利人的信息是否为公众所知悉、涉嫌侵权人所使用的信息与权利人的信息是否实质相同等专门性事项进行鉴定。权利人、涉嫌侵权人可以就上述鉴定结论向市场监管部门提出意见并说明理由，由市场监管部门进行审查并决定是否采纳。

3.4 【行政处罚】

市场监管部门对确有依法应给予行政处罚的侵犯商业秘密行为，根据情节轻重及具体情况，作出行政处罚决定。

3.4.1【行为类型】

侵犯商业秘密行为类型主要有违法获取、违法披露、违法使用、合法获取违法使用、第三人侵权、教唆帮助类侵权等。

不得实施下列侵犯商业秘密的行为:

a）经营者以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密;

b）经营者披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密;

c）经营者违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密;

d）经营者教唆、引诱、帮助他人违反保密义务或者违反权利人有关保守商业秘密的要求，获取、披露、使用或者允许他人使用权利人的商业秘密。

e）经营者以外的其他自然人、法人和非法人组织实施前款所列违法行为的，视为侵犯商业秘密。

f）第三人明知或者应知商业秘密权利人的员工、前员工或者其他单位、个人实施 a 项所列违法行为，仍获取、披露、使用或者允许他人使用该商业秘密的，视为侵犯商业秘密。

3.4.2【违法行为认定】

权利人能证明涉嫌侵权人所使用的信息与自己主张的商业秘密实质上相同，同时能证明涉嫌侵权人有获取其商业秘密的条件，而涉嫌

侵权人不能提供或者拒不提供其所使用的信息是合法获得或者使用的证据的，市场监管部门可以根据有关证据，认定涉嫌侵权人存在侵权行为。

3.4.3 【行政责任】

市场监管部门认定当事人的行为构成侵犯商业秘密的，应当责令停止违法行为，没收违法所得，处十万元以上一百万元以下的罚款；情节严重的，处五十万元以上五百万元以下的罚款。

3.4.3.1【责令停止违法行为】

视当事人侵权行为的具体情形，市场监管部门可责令当事人返还或销毁载有商业秘密的图纸、软件或其他有关载体，不得继续披露、使用或允许他人使用商业秘密。

当事人利用权利人的商业秘密生产的产品，尚未销售的，应监督当事人销毁，但是权利人同意收购或同意当事人继续销售的除外。

3.4.3.2【没收违法所得】

国家市场监管总局《商业秘密保护规定（征求意见稿）》（2020年9月4日公告）第三十四条规定，侵犯商业秘密的违法所得是侵权人违法生产、销售商品或提供服务所获得的全部收入扣除侵权人直接用于经营活动的适当的合理支出。该规定与现行有效的《工商行政管理机关行政处罚案件违法所得认定办法》中认定违法所得的基本原则一致。

当事人没有违法所得或违法所得无法准确认定的，不做没收违法所得的处罚。

3.4.3.3【罚款】

对侵犯商业秘密行为应处以十万元以上一百万元以下的罚款；情节严重的，处以五十万元以上五百万元以下的罚款。目前尚无对“情节严重”的法律规定或有权解释，执法实践中一般适用十万元以上一百万元以下的罚款幅度。

3.4.3.4【列入严重违法失信名单】

根据《市场监督管理严重违法失信名单管理办法》规定，对侵犯商业秘密这种严重破坏公平竞争秩序的不正当竞争行为，市场监管部

门按照从重处罚原则处以罚款的，应将当事人列入严重违法失信名单，通过国家企业信用信息公示系统公示，并实施相应管理措施。

市场监管部门收到法院的生效法律文书，要求对相关经营者、人员实施严重违法失信名单管理的，参照该办法执行。

3.4.3.5【移送追究刑事责任】

市场监管部门在对当事人作出行政处罚后，认为当事人可能构成犯罪的，应移送公安机关追究刑事责任。经公安机关侦查、检察院提起公诉，法院判决当事人犯侵犯商业秘密罪并判处罚金的，市场监管部门已经给予当事人罚款的，应折抵相应罚金。

3.5 【调解和和解】

3.5.1【调解】

权利人因损害赔偿问题向市场监管部门提出调解要求的，市场监管部门可以进行调解。

3.5.2【和解】

在侵犯商业秘密行政案件查办过程中，权利人和当事人在双方自愿的基础上可以自行和解。和解不影响案件是否构成侵犯商业秘密的定性，但可作为处罚裁量的因素加以考虑。

【相关案例】

问题：主张保护的商业秘密是专利技术是否应当立案？

案例：王某某、上海 YG 公司诉上海市某区市场监管局不予立案决定案

来源：（2014）虹行初字第 217 号

案情简介：2014 年 8 月 11 日，某区市场监管局收到上海 YG 公司提交的《侵犯商业秘密处理请求书》，要求调查上海 HS 车窗厂、厦门 JL 旅行车有限公司上海分公司侵犯王某某技术秘密的行为。经初步核查，王某某主张的技术秘密系其于 1996 年申请的“铝合金防盗玻璃窗”专利技术（《实用新型专利证书》第 28**49 号）。某区市场监管局认定王某某持有的专利技术不属于商业秘密，被举

报人不存在侵犯商业秘密的违法行为，遂于2014年8月21日作出不予立案决定。王某某、上海YG公司不服，向法院起诉。法院经审理认为：被告作为行政机关，对于侵犯商业秘密的投诉、举报，具有受理并作出行政处理的法定职权，其作出不予立案决定并无不当，驳回原告的诉讼请求。

解读：任何一件侵犯商业秘密案件成立，首先是确定主张商业秘密保护的信息是否属于商业秘密。如果商业秘密不存在，那么无论寻求何种途径，都得不到法律的救济。

问题：现场检查需要取得哪些资料？

案例：某低温设备有限公司侵犯商业秘密案

来源：成工商处〔2018〕276号

案情简介：2018年7月11日，成都市某区市场监管局接举报称，四川某低温设备有限公司（以下称当事人）通过不正当手段获取了四川SJ低温设备制造股份有限公司（以下称权利人）的商业秘密（技术信息），在某地从事液氮冰淇淋机和液氮罐的生产。

经调查，当事人系由王某与陈某共同投资。在此之前，王某原为权利人的生产部经理，陈某原为权利人的营销人员。二人在职时与权利人均签有《劳动合同》《员工保密协议》和《企业商业秘密竞业保密协议》。这些协议将涉密的技术信息，包括技术方案、配方、工艺流程、图纸和技术文档确定为权利人的商业秘密。员工对此负有保密义务，且自离职之日起三年内不得从事相同职业的工作，为此权利人每月支付保密费和竞业禁止补偿费。

在当事人生产现场查获由权利人署名的72份图纸，经四川某司法鉴定所鉴定，结论是该72份用于生产液氮罐和液氮冰淇淋机的图纸属于权利人所有的技术秘密。对此鉴定意见当事人无异议，承认这些图纸是其离职前带走的。案发时，当事人处于试生产阶段，没有成品上市，尚未给权利人造成直接经济损失。

解读：本案得以顺利办结的原因之一在于有效组织实施了现场检查，取得了关键证据。该局接到举报后，并没有立即采取行动，而是

通过两天的观察，找到当事人的实际生产地址（当事人既不在其登记注册地也不在权利人举报的地址生产），避免一击不中、打草惊蛇，减少关键技术秘密被当事人销毁的风险。现场检查时重点明确，注意收集各类技术信息的载体,取得了最关键的由权利人署名的72份图纸。最后，办案人员制作现场笔录，当事人对整个检查过程予以确认。

问题：仅非法获取但未使用商业秘密是否构成侵犯商业秘密行为？

案例：郑某某侵犯商业秘密案

来源：玉市监处罚〔2021〕2021828号

案情简介：当事人郑某某于2020年4月入职XF公司，从事技术员岗位工作，主要工作是样品的图纸绘制、更改等。当事人入职后虽未与XF公司签订专门的保密合同，但在劳动合同的补充协议中规定对公司的机密性文件要绝对保密。XF公司为保护图纸不被窃取，在公司的计算机内安装了数据防泄密系统，该系统有文件自动加密功能，计算机内的所有文件包括图纸必须依托该系统打开，否则即使外泄文件也无法打开变成乱码。当事人利用工作之便，违反公司保密规定将打印好的图纸用自己的智能手机拍摄保存，另将生产车间用过的15张图纸偷拿回家，后又用虚拟打印机将图纸另存为PDF格式的方式绕过公司的数据防泄密系统，将一张排气阀图纸保存到自己的存储器中。当事人秘密窃取公司图纸后，全部保存到自己的手机中，经整理图纸多达523张。据当事人陈述其秘密窃取图纸是出于个人学习的目的，未对外出售或泄露。

办案机关依法对当事人侵犯商业秘密的行为作出行政处罚。

解读：员工离职前违规获取公司大量敏感信息（含商业秘密）是目前多发常见的现象。此种行为离追究刑事责任尚有距离，贸然提起民事诉讼又成本较高，许多企业往往以内部处理为主。对此类单纯获取但没有证据证明有泄露或使用商业秘密的行为，可尝试向市场监管部门举报以获得行政保护。

问题: 合法获取、非法使用商业秘密是否构成侵犯商业秘密行为?

案例: 南京某电子设备有限公司侵犯商业秘密案

来源: 雨市监处罚（2021）10290号

案情简介: 当事人南京某电子设备有限公司在加工承揽权利人定制的XF05C机箱产品时，获得了该产品的设计图纸。在完成与权利人之间的合同后，当事人又承揽了南京另一家公司的XF05C-JY骨架产品定制业务。经鉴定，权利人的XF05C机箱存在不为公众所知悉的技术秘点,并采取了必要的保密措施。而当事人为另一客户制作的XF05C-JY骨架上使用了与权利人相同的技术秘密。

办案机关依法对当事人侵犯商业秘密的行为作出行政处罚。

解读: 本案是加工承揽领域常见的违反保密义务侵犯商业秘密典型案件。当事人依据合同获取了权利人的技术秘密后违反保密义务，使用该技术秘密生产产品牟利，构成侵犯商业秘密行为。

问题: 当事人拒不配合的情况下，如何认定侵犯商业秘密行为成立?

案例: 上海FH智能有限公司侵犯商业秘密案

来源: 沪市监松处〔2020〕272020000100号

案情简介: 2012年11月至2017年2月期间，李某在权利人公司担任“机械工程设计师”一职，并签订了《保密协议》与《IT安全管理制度》。李某任职期间参与了木封边机产品的设计研发工作。

2016年8月1日,当事人法定代表人孙某某与李某签订《协议书》,双方约定孙某某出资200万元，李某提供直线自动木封边机技术，合作开办公司。2016年11月10日，孙某某与宋某注册成立上海FH智能设备有限公司（当事人），李某任总经理，全面负责木封边机生产、销售业务。

据鉴定机构鉴定，权利人木封边机产品使用的“涂胶单元”等属于不为公众所知悉的技术信息。当事人生产的木封边机使用的相关技术与权利人的技术信息相同。

同时，在当事人处查获的移动存储盘中保存的24张技术图纸（3D

模型）所载的技术信息与权利人木封边机的技术图纸（3D 模型）所载的技术信息实质上相同。

办案机关依法对当事人侵犯商业秘密的行为作出行政处罚。

解读：在本案查办过程中，当事人关闭公司、解散员工，以各种手段阻碍调查，并辩称相关产品技术系通过反向工程研发。办案机关先使用直接证据推翻当事人反向工程研发的辩解，后运用推定原则，认为李某某有接触权利人技术秘密的条件，且不能证明其掌握的与权利人技术秘密实质上相同的技术信息有合法来源，认定侵犯商业秘密行为成立。

问题：行政保护的作用是不是简单地一罚了之？

案例：敖某等三人侵犯商业秘密案

来源：（湖）市监经处字第〔2018〕1、2、3 号

案情简介：敖某作为湖州市某电子科技公司的工艺装备部长和原料生产线项目执行人，与公司签订企业员工保密协议和项目保密协议。协议明确约定敖某在任职期内完成与公司业务相关的发明创造、技术秘密或其他商业秘密信息均为职务成果，公司享有知识产权。敖某在该公司研发出被列为企业核心商业秘密的原料除杂加工工艺后，为了牟取私利，与该公司的原料供应商掌某合伙在江苏省连云港市建厂，并将其掌握的生产工艺秘密传授给工厂管理人员孙某，利用该项工艺生产原料。截至案发，该厂共生产成品原料 200 吨，尚未对外销售。办案机关认为，敖某违反保密义务，将其掌握的被所在公司列为商业秘密的原料生产工艺泄露给掌某和孙某，孙某利用该工艺生产原料。敖某、掌某和孙某均构成侵犯商业秘密行为。

解读：本案的一大亮点是办案机关在案件查办过程中积极斡旋，安排相关人员会见恳谈，主动调和权利人与当事人之间的矛盾，最终促成多方达成谅解协议。敖某、掌某和孙某三人承诺严格保守已获取的商业秘密，否则将承担法律责任并赔偿 300 万元。权利人将三人合办的工厂作价收购，继续利用该工艺生产原料。达成和解后，权利人商业秘密被继续泄露的风险极大降低。

4.刑事保护

4.1【侵犯商业秘密罪】

《刑法》（2020年修正）第二百一十九条规定，有下列侵犯商业秘密行为之一，情节严重的，处三年以下有期徒刑，并处或单处罚金；情节特别严重的，处三年以上十年以下有期徒刑，并处罚金：

a）以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密的；

b）披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密的；

c）违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密的。

明知前款所列行为，获取、披露、使用或者允许他人使用该商业秘密的，以侵犯商业秘密论。

备注：采取非法复制、未经授权或者超越授权使用计算机信息系统等方式窃取商业秘密的，应当认定为“盗窃”。

4.1.1【犯罪构成】

4.1.1.1 侵犯商业秘密罪的犯罪主体为一般主体，包括自然人与单位。凡年满16周岁的自然人及非完全丧失辨认与控制能力的精神病人，均可构成本罪。

4.1.1.2 本罪要求行为人在主观方面为故意，即行为人明知自己的行为侵犯了他人的商业秘密，过失行为不构成本罪。

4.1.1.3 侵犯商业秘密罪的犯罪对象为商业秘密，刑法所保护的商业秘密与《反不正当竞争法》界定的商业秘密相同。商业秘密是否成立是认定是否构成侵犯商业秘密罪的前提条件。

4.1.2【犯罪行为】

刑法中构成侵犯商业秘密罪的行为方式与《反不正当竞争法》规定的行为方式不尽相同。主要包括非法获取、非法披露、非法使用、非法允许他人使用四种类型。

4.1.3【刑事追诉标准】

《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释（三）》（2020年9月14日起施行，以下的简称《解释三》）第四条规定，实施刑法第二百一十九条规定的行为，具有下列情形之一的，应当认定为“给商业秘密的权利人造成重大损失”（情节严重）：

（一）给商业秘密的权利人造成损失数额或者因侵犯商业秘密违法所得数额在三十万元以上的;

（二）直接导致商业秘密的权利人因重大经营困难而破产、倒闭的;

（三）造成商业秘密的权利人其他重大损失的。

给商业秘密的权利人造成损失数额或者因侵犯商业秘密违法所得数额在二百五十万元以上的，应当认定为刑法第二百一十九条规定的“造成特别严重后果”（情节特别严重）。

备注：权利人是指商业秘密的所有人和经商业秘密所有人许可的商业秘密使用人。

2023年1月18日，《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释（征求意见稿）》

向社会公开征求意见，其中对属于“情节严重”的情形增加了两种，一是一年内以不正当手段获取商业秘密三次以上的；二是二年内因侵犯商业秘密行为受过行政处罚二次以上，又实施侵犯商业秘密行为的。

4.1.4【权利人损失数额认定】

商业秘密权利人的损失数额，应按照下列方式认定:

a）以不正当手段获取权利人的商业秘密，尚未披露、使用或者允许他人使用的，损失数额可根据该项商业秘密的合理使用许可费确定;

b）以不正当手段获取权利人的商业秘密后，披露、使用或者允许他人使用的，损失数额可根据权利人因被侵权造成销售利润的损失确定，但该损失数额低于商业秘密合理许可使用费的，根据合理使用许可费确定;

c）违反约定、权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密的，损失数额可根据权利人因被侵权造成销售利润的损失确定;

d）明知商业秘密是不正当手段获取或者是违反约定、权利人有关保守商业秘密的要求披露、使用、允许使用，仍获取、使用或者披露的，损失数额可根据权利人因被侵权造成销售利润的损失确定;

e）因侵犯商业秘密行为导致商业秘密已为公众所知悉或者灭失的，损失数额可根据该项商业秘密的商业价值确定。商业秘密的商业价值，可以根据该项商业秘密的研究开发成本、实施该项商业秘密的收益综合确定。

权利人因侵权造成销售利润的损失，可根据权利人因被侵权造成销售量的减少的总数乘以权利人每件产品的合理利润确定；销售数量减少的总数无法确定的，可根据侵权产品销售量乘以权利人每件产品的合理利润确定；权利人因被侵权造成销售量减少的总数和每件产品的合理利润均无法确定的，可根据侵权产品销售量乘以每件侵权产品的合理利润确定。商业秘密系用于服务等其他经营活动的，损失数额可根据权利人因被侵权而减少的合理利润确定。

商业秘密的权利人为减轻对商业运营、商业计划的损失或者重新恢复计算机信息系统安全、其他系统安全而支出的补救费用，应当计

入给商业秘密的权利人造成的损失。

4.1.5【侵权人违法所得数额认定】

侵权人的违法所得数额，应按照下列方式认定:

a）因披露或者允许他人使用商业秘密而获得的财物或者其他财产性利益的价值;

b）因使用商业秘密所获得的利润，该利润可以根据侵权产品销售量乘以每件侵权产品的合理利润确定。

4.1.6【共同犯罪】

如果明知他人实施侵犯商业秘密的犯罪行为，而为其提供贷款、资金、账号、发票、证明、许可证件，或提供生产经营场所或运输、储存、代理进出口等便利条件、帮助的，以侵犯商业秘密罪的共犯论处。

4.2【为境外窃取、刺探、收买、非法提供商业秘密罪】

《刑法》（2020 年修正）增设了第二百一十九条之一 9 为境外的机构、组织、人员窃取、刺探、收买、非法提供商业秘密的，处五年以下有期徒刑，并处或单处罚金; 情节严重的，处五年以上有期徒刑，并处罚金。

需要注意的是，本罪没有情节后果要求，行为人一经实施，即构成本罪。情节的严重程度，仅是加重处罚的考量因素，不属于本罪的犯罪构成要件。

4.3 【刑事案件管辖】

4.3.1【地域管辖】

侵犯知识产权犯罪案件由犯罪地公安机关立案侦查。必要时，可以由犯罪嫌疑人居住地公安机关立案侦查。

侵犯商业秘密犯罪案件的犯罪地，包括侵权产品制造地、储存地、运输地、销售地，销售侵权产品的网站服务器所在地、网络接入地、网站建立者或管理者所在地，权利人受到实际侵害的犯罪结果发生地。

4.3.2【级别管辖】

侵犯商业秘密罪的最高刑期为十年有期徒刑。一般而言，商业秘密刑事案件的一审法院为基层法院，基层检察院进行审查起诉，基层公安机关进行侦查。具体到浦东新区，是由区法院一审，区检察院审查起诉，区公安分局（经侦支队）进行侦查。

当然，实践中也存在商业秘密刑事案件由中级人民法院一审、高级人民法院二审的情况。

4.4【报案】

对涉嫌构成侵犯商业秘密犯罪的行为，任何单位和个人有权利也有义务向公安机关报案。

商业秘密权利人发现有自然人或者单位侵犯其商业秘密且情节严重的，可以依照管辖规定向公安机关报案。

4.4.1【报案材料】

报案人在向公安机关报案时，需要提供必要的证据材料，证明有犯罪事实的存在。根据侵犯商业秘密罪的构成特点，报案材料应尽量涵盖以下五方面:

a）商业秘密客观存在的证明。包括商业秘密的类型、名称及内容，涉案技术信息或经营信息不为公众所知悉的鉴定意见，对上述信息采取相关保密措施的规章制度、保密协议等。

b）商业秘密权属关系的证明。包括权利人的名称、住所及联系方式，商业秘密的研发、创制过程证明材料，如项目立项书、研发证明、制作人证言等。

c）侵权事实存在的证明。包括证明犯罪嫌疑人有条件获取权利人商业秘密的材料、证明犯罪嫌疑人披露或使用权利人商业秘密的材料、证明犯罪嫌疑人所侵犯的商业秘密与权利人的商业秘密实质相同的鉴定、证明权利人因侵权行为遭受重大经济损失的评估材料等。

d）犯罪嫌疑人的相关情况。报案人在能够确定嫌疑人的情况下，应尽量向公安机关提供犯罪嫌疑人的姓名、所在单位、住址等信息。

e）其他与证明案件事实有关的材料。如刑事立案前进行民事诉讼的相关判决、材料等。

报案人应尽可能提供翔实、充分的报案材料，帮助公安机关尽快锁定犯罪嫌疑人、查明案件真相、缩短侦办周期，从而减少权利人因侵权行为所遭受的损失。

4.4.2【鉴定意见】

鉴定意见是非常重要的定案证据。实践中主要涉及三类鉴定:

a）商业秘密存在的鉴定。此类鉴定帮助公安机关确定商业秘密是什么以及秘密点如何体现等基础问题。

b）商业秘密实质相同（同一性）的鉴定。此类鉴定是确定犯罪行为存在的重要依据。只有犯罪嫌疑人侵犯的商业秘密与权利人请求保护的商业秘密实质相同，才可能构成侵犯商业秘密罪。

c）权利人损失价值评估。此类评估决定了刑事案件是否构成犯罪及追诉量刑基准。

提示：在鉴定过程中秘点选取要合理。在梳理秘点时，首先要考虑侵权人有可能侵害了哪些技术信息；其次要考虑在后期比对时，对于动态的技术信息，如一些生产流程中的工艺参数，是否可能从侵权人处获得；最后要考虑秘点覆盖的范围大小、数量多少。如果秘点太多则鉴定费用高，太少又可能达不到维权目的。

4.5【立案】

公安机关接到报案后，应对报案材料进行审查，决定是否立案。

4.5.1【刑事立案条件】

符合下列条件的，应当立案侦查:

a）有犯罪事实，即已有证据证明犯罪事实已客观存在，而非毫无根据的主观臆测。

b)需要追究刑事责任,即犯罪嫌疑人的犯罪行为应受到刑事处罚。

c）有管辖权，公安机关只能管辖具有管辖权的案件，对于不属于自己管辖的案件应移送有管辖权的公安机关。

4.6【移送追究行政责任】

公安机关立案后，经侦查认为犯罪嫌疑人的行为未达到刑事追诉

标准的，应当移送同级市场监管部门追究行政责任。

4.7【取保候审】

立案后公安机关为防止犯罪嫌疑人逃避侦查，可采取取保候审的强制措施，即责令其提出保证人或交纳保证金，并出具保证书，保证随传随到，对其不予羁押。取保候审通常对犯罪较轻，不需要逮捕，但需要对其行动自由作一定限制的犯罪嫌疑人采用。

4.8【逮捕】

对有证据证明有犯罪事实，可能判处有期徒刑以上刑罚的犯罪嫌疑人，公安机关采取取保候审尚不足以防止发生下列社会危险性的，应予以逮捕:

a）可能实施新的犯罪的;

b）有危害国家安全、公共安全或社会秩序的现实危险的;

c）可能毁灭、伪造证据，干扰证人作证或串供的;

d）可能对被害人、举报人、控告人实施打击报复的;

e）企图自杀或逃跑的。

4.9【审查起诉】

检察院应对公安机关侦查终结移送起诉的案件进行审查，核实犯罪事实和证据、犯罪性质和罪名是否适当，并依法决定是否对犯罪嫌疑人提起公诉、不起诉或撤销案件。

商业秘密权利人应积极配合检察院在审查起诉期间的补充侦查、证据收集等工作，做好出庭的准备工作，保证刑事诉讼程序的顺利进行。

4.10【审理裁判】

法院作为审判机关根据检察院移送起诉的案件事实、证据材料等对案件进行全面审查，并可以补充调取庭审需要的证据材料。经开庭审理后，法院就商业秘密刑事案件的被告是否有罪、构成何罪及判处

何刑罚等实体问题作出依法判决。

商业秘密权利人应积极配合法院的刑事审判工作，涉及商业秘密的案件，当事人申请不公开审理的，可以不公开审理。

4.11【刑民交织】

商业秘密案件既涉及民事法律中的侵权问题，又涉及刑法规定的侵犯商业秘密犯罪，是典型的“刑民交织”案件。我们认为可采取“刑民并行”（刑事附带民事诉讼）为原则，以“先刑后民”或“先民后刑”为例外的思路。

4.11.1【先民后刑】

对于侵犯经营信息类商业秘密案件，权利是否存在、权利归属以及商业价值如何需要原被告双方充分举证，“先民后刑”可能更有利于查明事实。

4.11.2【先刑后民】

对于侵犯技术类商业秘密案件，较易达到刑事追诉标准又需要技术侦查手段的介入，“先刑后民”可能更利于权利保障。

4.11.3【民刑办案融合】

浦东新区检察院已设立知识产权刑事、民事、行政、公益诉讼检察职能“四合一”集中履行的派出检察院（张江检察院），浦东新区法院知识产权庭已实行知识产权刑事、民事、行政“三合一”的审判机制，为本区商业秘密案件刑民交织问题的解决提供了现实途径。

【相关案例】

问题：游戏代码是否属于商业秘密？

案例：陆某甲、陆某乙侵犯商业秘密案

来源：（2020）沪0110刑初869号

案情简介：2018年9月起，被告陆某甲成立上海A网络科技有限公司（以下简称A公司），后违反与原工作单位上海B信息科技有限公司（以下简称B公司）签订的保密协议，使用B公司研发的《龙珠传奇》游戏的前端代码，开发《龙珠Z战士》游戏并上线运营。期间，被告陆某乙明知上述前端代码为原工作单位B公司开发且签订过保密协议，仍帮助陆某甲在A公司的上述游戏中予以使用。经统计，A公司通过《龙珠Z战士》在各个平台的发行，违法所得近150万元。2020年11月，法院判处被告陆某甲、陆某乙构成侵犯商业秘密罪。

解读：游戏软件涉及重要玩法、游戏框架等影响游戏运行的关键程序代码可以构成商业秘密。这些关键程序代码关乎向玩家正常呈现游戏的效果，其商业价值毋庸置疑，因此A公司将这些代码存储在源代码版本控制系统中，并采用不同开发人员、不同账号密码管理的保密措施。而行为人违反约定，利用这些核心代码开发了新的手机游戏，并对外销售牟利，属于侵犯商业秘密的行为。在商业秘密刑事案件中要严格界定商业秘密范围，如侵权软件与权利人软件代码构成实质性相同，且系核心、不可分割的秘点，应认定侵权软件侵犯了权利人的完整商业秘密。

检察机关在办理本案过程中，发现权利单位有三处管理疏漏导致行为人轻易获得代码：（1）保密教育不到位。权利单位虽与行为人签订保密协议，但并不知晓商业秘密的范围及保密措施情况。（2）保密

措施不到位。权利单位除与员工签订保密协议、在服务器上为项目组成员设置账号和密码以及员工离职后回收计算机外，并未采取其他更有效的保护措施，且服务器只保存上传记录，无下载记录。（3）监督管理不到位。行为人在公司期间可以自由下载相关代码，既无下载记录留存，也无下载介质限制，更无人员予以监管。

问题：侵犯客户名单等经营信息是否构成侵犯商业秘密罪？

案例：施某侵犯商业秘密案

来源：（2019）沪 0109 刑初 991 号

案情简介：2015 年 9 月，被告施某入职上海某管理咨询有限公司（原公司），并与该公司签订劳动合同及相关保密协议。后被告施某在公司担任项目经理期间，于 2017 年 10 月私自设立上海 SY 管理咨询有限公司，从事与原公司性质相同的业务，并违反保密约定，使用其所掌握的原公司的客户名单，与原公司的客户开展业务。经审计，SY 公司使用被告施某所掌握的原公司的客户名单开展经营活动，违法所得 100 余万元。

2020 年 1 月，法院判决被告施某犯侵犯商业秘密罪，判处有期徒刑一年，缓刑一年，并处罚金十万元。

解读：单纯的客户名称、地址、电话等简单经营信息，因缺乏需求类型、交易习惯、购买频率、经营规律、价格承受能力等深度信息，不符合商业秘密的认定标准，不属于商业秘密。但符合商业秘密特性的经营信息仍是商业秘密的重要组成部分。倘若权利人付出一定的商业努力，使经营信息具备不为公众所知悉的深度内容，能为权利人带来现实的或潜在的经济利益或竞争优势，应认定为商业秘密。本案中，法院认为被告施某违反约定及权利人有关保守商业秘密的要求，使用其所掌握的商业秘密，给商业秘密的权利人造成重大损失，其行为已构成侵犯商业秘密罪。

问题：因侵权造成的权利人销售利润损失难以计算时如何认定？

案例：万超公司、于某某、贾某某侵犯商业秘密案

来源：（2018）沪 0107 刑初 1289 号

案情简介：2012 年 4 月至 2014 年 2 月，被告于某某在权利人恩坦华公司担任高级产品工程师，曾接触恩坦华公司汽车天窗机械组、汽车天窗遮阳帘驱动系统等一系列技术信息。2014 年 3 月，于某某从恩坦华公司离职，随即受被告贾某某经营的被告单位万超公司聘用，负责汽车全景天窗研发工作。于某某违反与恩坦华公司保密约定，将恩坦华公司技术信息披露并用于万超公司相关天窗产品的研发。万超公司法定代表人贾某某明知于某某可能存在非法披露他人技术秘密的情况，仍将相关数据资料用于万超公司汽车天窗产品的研发及生产销售。后贾某某、于某某又以共同发明人身份，对部分技术申请专利。经鉴定，万超公司的部分汽车天窗产品、相关专利及计算机内部分电子数据，与恩坦华公司技术信息实质相同。2015 年 9 月至 2018 年 6 月期间，万超公司销售相关产品净利润达 1200 万余元。

2020 年 1 月，法院认定各被告构成侵犯商业秘密罪，判处万超公司罚金四百万元；判处于某某有期徒刑五年，并处罚金五十万元；判处贾某某有期徒刑三年缓刑三年，并处罚金三十五万元。

解读：当权利人因侵权造成的销售利润损失难以计算时，可以参考侵权人的销售获利认定权利人损失数额。《解释三》规定以商业秘密的合理许可使用费及权利人因被侵权造成的销售利润损失计算损失数额，但基于商业秘密的类型不同、侵权行为多样、有关损失的证据难以收集等情况，需要结合个案具体分析，按照最合适的计算方式来确认权利人损失数额。从行为逻辑来看，侵权人的巨大获利通常使得权利人通过正常交易行为获得的收益减少，而侵犯商业秘密罪保护的法益是有关知识产权交易的市场经济秩序，其中必然包含权利人因商业秘密可获得的收益，因此损失的认定可以参考侵权人的获利数额。

5.商业秘密鉴定

商业秘密鉴定是商业秘密维权、司法执法活动中证明事实的重要手段。

5.1【含义】

商业秘密鉴定是指鉴定机构运用科学技术或专门知识对涉案技术信息或经营信息的相关专业性技术问题进行鉴别和判断，并出具鉴定意见的活动。

5.2【鉴定种类】

商业秘密维权和司法执法活动中常用的鉴定包括非公知性鉴定、同一性鉴定和商业秘密侵权损失鉴定等。

5.2.1【非公知性鉴定】

非公知性鉴定，是对商业秘密权利人所主张的技术信息或经营信息是否属于“不为公众所知悉”的鉴定。

5.2.1.1 “不为公众所知悉”是商业秘密构成的首要条件。不具有秘密性的信息，即使对企业具有商业价值也采取了保密措施，也不可能构成商业秘密。秘密性要求有关信息不为所属领域的相关人员普遍知悉和容易获得，一般是指特定信息在本行业内不是众所周知，而不是绝对无人知悉。只要存在“普遍知悉”或“容易获得”一种情况就不满足秘密性的要求

5.2.1.2 非公知性的判定，实务中可从以下几个方面进行综合分析:

a）该信息在所属领域是否属于一般常识或行业惯例;

b）进入市场后相关公众是否可以通过观察产品直接获得;

c）是否无需付出一定的代价而容易获得。

5.2.1.3 技术信息的非公知性鉴定涉及的领域非常广泛，包括计算机软件、机械、化工、生物医药等各方面，技术性越强的商业信息对

鉴定机构的专业要求越高，因此在选择鉴定机构时，要注重待鉴定密点的具体内容与鉴定机构、鉴定人员的专业领域是否匹配。

5.2.1.3 技术查新报告可作为鉴定参考资料。技术查新报告一般在专利审查中运用，是查新机构根据查新项目的查新点与所查数据库等范围内的文献信息进行比较分析，对查新点作出新颖性判别。虽然商业秘密的非公知性与专利的新颖性要求并不相同，但是在文献检索方法上可以相互借鉴。技术信息的非公知性鉴定报告中经常涉及对近似文献的检索，既可以由鉴定机构自行进行近似文献检索，也可以委托其他检索机构出具检索报告。

司法或行政机关通过比较检索报告与鉴定报告的分析过程和结论，可以增强对密点技术特征的全面认识，同时要注意审查检索报告中关键词的选取和数量与密点的技术特点是否匹配、查新日期是否在案发之前、查新数据库是否涵盖主要数据库及密点关联技术领域、涉外密点是否检索相关外文数据库等。

5.2.1.4 在进行非公知性鉴定时，除了利用文献数据库进行检索以外，还应当通过互联网检索类似技术、浏览相关行业期刊出版物、收集相关展会资料等方式进行排查，并将检索过程和结论在鉴定报告中予以体现。

5.2.1.5 实践中可能存在产品技术秘密因使用或者销售公开的情况。在刑事案件办理过程中，为进一步排除公开的可能性，检察机关可能需要组织侦查机关、鉴定人员实地进行设备拆卸勘测，确定通过一般测绘和观察无法准确获取密点信息。

5.2.2【同一性鉴定】

同一性鉴定，是指通过对检材与样本所示的技术信息进行比较，从而认定二者是否相同或者实质相同。

5.2.2.1【检验项目选择】

分析检材和样本，根据检材和样本的内容选择以下一项或多项内容进行检验:

a）结构间的比对样本所示的技术参数与检材所示的技术参数一一比较，对于存在相同或实质相同的技术参数需要进行说明。

b）成份间的比对样本所示的配方成份或者其含量与检材所示的配方成份或者其含量一一比较，对于存在相同或实质相同的配方成份或者其含量需要进行说明。

c）生产工艺、方法间的比对样本所示的生产工艺、方法与检材所示的生产工艺、方法一一比较（一般需要生产设备运行过程中进行检测），对于存在相同或实质相同的生产工艺、方法需要进行说明。

d）软件间的比对。参照《软件相似性鉴定实施规范》（SF/ZJD0403001-2014）。

5.2.2.2【比对结果】

鉴定意见应分别列出检材与样本技术信息是否相同、实质相同、相似及不同，并对存在相同或者实质相同的部分进行说明。

5.2.2.3【知识产权鉴定机构】

非公知性鉴定和同一性鉴定都属于技术性鉴定。鉴定机构可通过人民法院诉讼资产网（https://www.rmfysszc.gov.cn）自主查询选择。

查询步骤如下:1.登陆人民法院诉讼资产网；2.点击“司法技术”；3.点击左侧“专业机构”；4.在“专业类别”一栏勾选“知识产权”并点击确定；5.点击搜索。

上海市目前共有 9 家知识产权鉴定机构可供选择,其中浦东新区 3 家。（查询日期：2023 年 7 月 11 日）

5.2.3【商业秘密侵权损失鉴定】

被害人的损失金额以及被告的违法所得是侵犯商业秘密犯罪案件中重要的入罪标准，也是关系到被告定罪量刑的重要标准。对被害方而言，被害人要收集证据向公安机关报案，需要对损失的金额进行审计或评估，证实其损失金额达到该罪的入罪标准。在商业秘密侵权的民事诉讼中，法院也需要依据权利人的损失数额或者侵权人的违法所得数额来确定判决赔偿的数额。

商业秘密诉讼中损害赔偿额的认定，实际上就是将无形的商业秘密用具体的经济数值来替换，与知识产权资产评估之间存在较大的重合性。资产评估是确定商业秘密价值的重要手段。资产评估在商业秘密诉讼中的适用，既为立法所认可，也已在司法审判中有了一定的实

践基础。

5.2.3.1【资产评估】

评估需要由专门的资产评估机构进行评估。资产评估机构可通过人民法院诉讼资产网（https://www.rmfysszc.gov.cn）自主查询选择。

查询步骤如下:1.登录人民法院诉讼资产网；2.点击“司法技术”；3.点击左侧“专业机构”；4.在“专业类别”一栏勾选“资产评估”并点击确定；5.点击搜索。

上海市目前共有 7 家资产评估机构可供选择，其中浦东新区 1 家。（查询日期：2023 年 7 月 11 日）

5.2.3.2【会计审计】

审计是由有司法会计资格的会计师事务所来进行审计。会计审计机构可通过人民法院诉讼资产网（https://www.rmfysszc.gov.cn）自主查询选择。

查询步骤如下:1.登录人民法院诉讼资产网；2.点击“司法技术”；3.点击左侧“专业机构”；4.在“专业类别”一栏勾选“会计审计”并点击确定；5.点击搜索。

上海市目前共有 8 家会计审计机构可供选择，其中浦东新区 1 家。（查询日期：2023 年 7 月 11 日）

5.2.3.3【选择合适的鉴定方式】

案件究竟是选择评估，还是选择审计？计算损失的方式不同应采用不同的鉴定方式。

a）假定某技术信息被公开披露，失去秘密性了，此种情形宜以该技术的商业价值来计算损失，通常来说就是以研发费用来计算，此时需要评估机构对这一项技术的价值进行评估。

b)如果侵权人采取了不正当手段获取技术信息，但未披露和使用，或虽使用了但侵权产品尚未上市，此种情形宜按该项技术的合理许可费来计算损失，通常按照普通技术许可计算许可费，此时也需评估机构进行评估。

c）假如侵权人已经使用或已经允许他人使用了技术信息，侵权产品已投放市场，此种情形应以权利人减少的销售量，或者侵权人销售

侵权产品的销售量，以司法审计的方式，委托会计师事务所进行审计。

5.3【鉴定程序】

5.3.1【委托主体】

5.3.1.1【刑事民事案件委托主体】

侵犯商业秘密刑事案件和民事案件中涉及的知识产权鉴定属于司法鉴定。司法鉴定机构应统一受理办案机关的司法鉴定委托。公安机关、检察机关和法院根据需要可以委托鉴定机构进行鉴定。很多商业秘密案件的权利人在报案之前，已经自行委托鉴定机构进行鉴定，并将鉴定意见作为报案的重要证据之一。办案机关依据报案材料决定立案后，应另行委托鉴定。

5.3.1.2【行政案件委托主体】

商业秘密权利人向市场监管部门举报的，可以自行委托鉴定机构出具鉴定意见。市场监管部门对鉴定意见进行审查，并经被举报侵权人认可的，可以采纳作为定案证据。被举报侵权人对权利人提供的鉴定意见不予认可且有合理理由的，市场监管部门根据需要可以委托鉴定机构（权利人委托鉴定机构以外的其他鉴定机构）鉴定。

5.3.2【委托形式要求】

鉴定机构决定受理鉴定委托的，应当与委托人签订鉴定委托书。鉴定委托书应当载明委托人名称、鉴定机构名称、委托鉴定事项、鉴定用途、鉴定材料的提供和退还、鉴定风险，以及双方商定的鉴定时限、鉴定费用及收取方式、双方权利义务等其他需要载明的事项。

5.3.3【选定专家、查新检索和检测机构】

鉴定机构根据委托事项和要求，推荐相关专业技术领域的查新检索机构、检测机构或鉴定专家，并经委托人确认后确定。

5.3.4【回避制度与保密义务】

委托人认为查新检索机构、检测机构、鉴定专家与刑事民事案件当事人有利害关系，需要回避的情形，经委托人确认，鉴定机构可以另行选定。

查新检索机构、检测机构、鉴定专家应恪守保密义务，不得擅自

留存、泄露受委托鉴定的技术信息。

5.3.5【鉴定方式】

技术鉴定一般采用检测鉴定、专家评议鉴定的方式。

5.3.5.1 凡通过检测机构测试、检验能达到鉴定要求的技术鉴定，应采用检测鉴定。检测机构对检测结果出具书面检测报告。

5.3.5.2 专家评议鉴定，一般由两名以上专家组成鉴定组，按鉴定程序进行鉴定，对鉴定结果出具书面鉴定意见。

5.3.6【技术听证及现场勘验】

鉴定机构根据需要可启动技术听证程序，就技术问题听取权利人和涉嫌侵权人对涉案技术信息的分析和意见、组织现场勘验，并邀请委托人一同参与听证、勘验过程。

5.3.7【出具鉴定意见】

承担任务的查新检索机构、检测机构、鉴定专家应当在鉴定机构的鉴定意见上签名、盖章。鉴定机构对出具的鉴定意见承担相应法律责任。

5.3.8【鉴定意见的专家质证】

法院根据案件事实查明需要，可以通知鉴定机构派员出庭接受质询，鉴定人也应当出庭接受当事人质询。鉴定意见要经过庭审双方当事人质证才能作为定案证据。

【相关案例】

问题：如何证明技术图纸上载明的技术信息属于非公知性信息？

案情简介：某公司多年来生产并销售其自主研发并自行生产的某

种先进设备。任职于该公司多年的核心技术人员离职后，带走了该公司保密的技术图纸，在他处设立新厂生产销售相同的设备。该公司向公安机关报案该离职技术人员涉嫌侵犯其商业秘密。公安机关需要确认涉案技术信息是否属于技术秘密，委托某鉴定机构就技术信息是否属于非公知性信息出具鉴定意见。

鉴定机构出具以下意见：该公司研发的垃圾处理焚烧工艺、设计计算方法、组装调整方法及组装手册、成套 CAD 机械图及其图纸中所涉及的机械零部件尺寸公差等技术要求、与装配和结构位置关联的其他技术要求等工艺参数信息，是该公司在其产品运行实践中，通过长期的经验积累和根据客户反馈信息作出相应改进调整后逐渐形成的，也是其设备运用的关键信息，不会对外公开此类自主研发产生的技术信息和产品的生产技术图纸。涉案技术信息不为该专业领域的普通技术人员普遍了解和掌握，不可能通过公开渠道直接、容易获得。

公安机关采纳了鉴定机构的意见，认为报案人的技术信息是不为公众所知悉的信息，具有秘密性。

解读：公安机关委托鉴定机构对涉案技术信息进行非公知性鉴定，得到涉案技术信息不为该专业领域的普通技术人员普遍了解和掌握、也不可能通过公开渠道直接、容易获得的鉴定结论。除非涉嫌侵权人能够作出反证，公安机关可以依据该鉴定意见认定涉案技术信息具有秘密性。

案例：吴某侵犯商业秘密案

来源：沪浦检刑诉（2012）4086 号起诉书

案情简介：2010 年 9、10 月间，吴某利用其在上海某公司担任合成研究员的工作便利，先后数次采用拆换其他研究人员办公用保密电脑硬盘的方法，窃取上海某公司为其他公司研发的资料，其中包括化合物结构式及其合成信息。2011 年 3 月至 6 月间，吴某为虚假宣传个人研发能力，将窃取的新型化合物结构式中的 89 个在互联网公开披露，除第 56 号结构式外的其余 88 个结构式与辉瑞公司的相应结构式具有同一性。

吴某的披露行为导致该些结构式不能申请专利，使得被害单位辉瑞公司及上海某公司的研发失去意义，导致上海某公司直接经济损失人民币 268 万余元。

2013 年 10 月 22 日上海市浦东新区人民法院判决：吴某犯侵犯商业秘密罪，判处有期徒刑三年六个月，并处罚金人民币十万元。判决宣告后，吴某提出上诉。2014 年 7 月 24 日上海市第一中级人民法院终审裁定：驳回上诉，维持原判。

解读：实践中，商业案件委托就相关专业技术问题进行鉴定对象一般为其技术信息是否为非公知技术，若判定是不为公众所知悉的技术信息，随后就权利人所拥有的技术信息与侵权人所披露使用的技术信息进行比对分析是否相同或相似。由于本案中控辩双方对于结构式的同一性问题认定存在较大争议，所以法院先行判定其是否具有同一性，然后再确认其是否构成商业秘密，这种判定方法具有一定的灵活性，也说明商业秘密案件的判定的先后次序并无严格约定。

鉴定意见结论中，关于化合物的同一性认为，从有机化学的专业角度，用结构式表示有机化合物的结构时，为了书写简便，除完整的结构式外，还可以使用结构简式表述。也就是说同一个有机化合物可以使用几种符合规则的不同结构型式来表示。因此，化合物的同一性反应在化学结构式上，是指化学结构式的一致性，或化学结构式的等同性（虽然化学结构式的表示方式不同，但其书写符合有机化合物结构式的基本规则,运用命名规则具有相同的化学名称，包括手性碳的绝对构型，因此也是相同的结构）。由此，本案中涉及含手性中心化合物、互变异构体、化合物外消旋体的同一性鉴定，最终鉴定结论认为：被告人披露的结构具有同一性。

法院最终认为，对于有争议的结构式是否具有同一性的认定，进过庭审对鉴定意见的充分质证后采信了公安机关委托的鉴定机构所做出的判定，除一个结构式不同外，其余结构式与被害单位的相应结构式具有同一性。

问题：如何认定权利人因侵权遭受的损失？涉案技术信息不为该

专业领域的普通技术人员普遍了解和掌握，不可能通过公开渠道直接、容易获得。

案例：富某公司、方某某等 7 人侵犯商业秘密案

案源：上海三中院、上海市检三分院 2022 年侵犯知产犯罪十大典型案例

案情简介：瑞某公司主要从事一次性卫生用品生产设备生产线的研发、制造和销售。平某（另案处理）原系瑞某公司机械设计部经理，于 2013 年 6 月离职后加入同样从事卫生用品生产设备经营的被告单位富某公司担任技术指导。后平某将其从瑞某公司获取的若干技术秘密非法披露给富某公司经营人被告人方某某，并交由被告人龚某某、胡某某等 6 人（均从瑞某公司离职加入富某公司）使用。方某某明知上述技术信息系瑞某公司商业秘密，仍指使龚某某等人将其中部分技术秘密用于并销售给江苏、杭州等地客户，还指使胡某某等人将另外部分技术秘密以富某公司名义申请专利并公开披露。

经审计，富某公司销售侵犯商业秘密的设备，造成瑞某公司损失数额达 1220 余万元；经评估，富某公司申请并公开的商业秘密商业价值合计 2019 万余元。

2021 年 12 月，上海市人民检察院第三分院以富某公司、方某某等 7 人涉嫌侵犯商业秘密罪提起公诉。2022 年 3 月，上海市第三中级人民法院以侵犯商业秘密罪判处被告单位富某公司罚金 1000 万元，7 名被告人被判处有期徒刑三年至一年不等，并处罚金 800 万元至 30 万元不等，适用缓刑。被告单位及被告人未提出上诉，判决已生效。

解读：本案中，被告单位富某公司通过两种方式侵犯瑞某公司的商业秘密。针对富某公司以不正当手段获取并使用商业秘密的行为，法院根据权利人因被侵权造成销售量减少的总数乘以权利人每件产品的合理利润，得出权利人的损失数额。针对富某公司将部分以上述手段获取并使用的商业秘密，通过申请专利的形式对外披露的行为，因侵犯商业秘密行为导致商业秘密被公众所知悉，通过委托专门的资产评估机构根据商业秘密的研发成本、实施该项商业秘密的收益等综合确定商业秘密的商业价值。两者所得总和即为权利人的损失数额。法

院据此判决富某公司构成侵权商业秘密罪并处罚金。权利人后继可以再提起民事诉讼，要求富某公司赔偿损失。

6.涉外保护

中国企业在海外经营或国际贸易中应高度关注与重视商业秘密纠纷风险，了解各国商业秘密保护环境，实施相应的商业秘密保护措施，做好风险防控，并制定维权策略。

6.1【美国商业秘密保护】

6.1.1【立法】

6.1.1.1【统一商业秘密法】

1979 年，美国颁布《统一商业秘密法》，是首部对商业秘密的专项立法，系统确立了商业秘密的保护范围以及侵犯商业秘密的行为方式。根据《统一商业秘密法》的定义，商业秘密是指任何有独立的实际或潜在的经济价值，并且通过正常的途径无法获知，有必要采取措施保持其秘密性的信息，包括配方、模式、汇编、程序、设备、方法、技术或流程等等。因此商业秘密的三大特性是价值性、非公开性和秘密性。

6.1.1.2【经济间谍法】

1996 年，美国颁布《经济间谍法》，首次将盗窃或侵犯商业秘密的行为规定为刑事犯罪。《经济间谍法》规定了经济间谍罪和一般商业秘密盗窃罪，两者的区别在于如果盗窃商业秘密的犯罪行为是为了使任何的外国政府、外国机构或外国代理人受益，则以经济间谍罪论处。

根据 2013 年修订后的《经济间谍法》，犯一般商业秘密盗窃罪，个人最高会被处以十年监禁，公司犯罪最高会被处以五百万美元的罚金。犯经济间谍罪，个人最高会被处以五百万美元罚金并处以最高十五年监禁，公司犯罪最高会被处以一千万美元或被盗商业秘密价值三倍中较高者的罚金，法院还可没收非法所得。

6.1.1.3【保护商业秘密法】

2016 年，美国颁布《保护商业秘密法》，对盗窃商业秘密案件的联邦管辖权、案件执行、境外案件报告、国会相关共识以及行为规范、责任豁免等进行详细规定。

该法改变商业秘密案件原由各州管辖的原则，将商业秘密案件提升到联邦层面，首创有关商业秘密的民事诉讼案由。《保护商业秘密法》为起诉侵犯商业秘密案件、获得民事救济提供统一的联邦法律依据，同时建立起商业秘密保护的统一标准。侵犯商业秘密的行为方式包括：明知或应知通过不正当手段（偷窃、贿赂、虚假陈述、违反或诱使违反保密义务、通过电子侵入或其他手段进行的间谍活动）获得他人商业秘密；在未获得明示或默示同意的情况下，披露或使用他人的商业秘密。

提示：美国关于商业秘密定义和侵权行为类型的法律规定与我国大体相似。对于有涉美业务的国内企业而言，应采取实际措施确保自身信息的秘密性和安全性，同时避免侵犯美国企业的商业秘密。

6.1.2【救济途径】

在美国，当权利人商业秘密被侵犯时，可选择三种救济途径，分别是民事诉讼、刑事程序以及申请美国国际贸易委员会发起337调查。

6.1.2.1【民事诉讼】

商业秘密权利人对侵犯其商业秘密的行为人可提起民事诉讼。权利人可以获得的救济包括禁令救济、损害赔偿金、律师费补偿等。

法院可以向被告发布禁止侵害的禁令，包括临时禁令、预备性禁令和长期性禁令，其期限和适用条件也有所不同。

损害赔偿金在美国可以单独请求，也可以同禁令一起主张。赔偿数额按照实际损失、不当得利以及许可收费损失的先后顺序确定。在恶意侵犯商业秘密的情形下，法院可判决被告按前述赔偿数额两倍以内支付惩罚性赔偿。法院还会判决给予胜诉方合理的律师费补偿。

6.1.2.2【刑事程序】

美国司法部可向法院提起侵犯商业秘密的刑事指控。在刑事程序中，司法部要承担举证责任，证明被告实施侵犯商业秘密的犯罪行为，并且具有恶意的作案动机。

因盗窃商业秘密被刑事起诉的案例，包括可口可乐公司前全球研究首席工程师游晓蓉博士，被控犯盗窃商业秘密罪、经济间谍罪和电信诈骗罪，最终被判处14年监禁和20万美元罚金；俄克拉荷马石油公司科学家谭宏进，被控犯盗窃商业秘密罪，最终被判处2年监禁和15万美元罚金。

6.1.2.3【337调查】

337调查指依据美国《1930年关税法》第337节的有关规定，如果进口贸易中存在侵犯知识产权或者其他不正当竞争行为，当事人可以向美国国际贸易委员会（United States International Trade Commission，以下简称ITC）申请启动行政调查。ITC也可自行决定开展行政调查。

337 调查大多涉及与知识产权保护有关的指控。相较于漫长的司法程序，337 调查可速战速决，通常在一年半左右审结，已成为美国知识产权保护的利器。自 1986 年中国企业首次接受 337 调查以来，一直是 337 调查的主要对象。

337 调查的主要程序包括：申请、立案、应诉、听证前会议、取证、听证会、行政法官初裁、委员会复议并终裁、总统审议。如果任何一方当事人对 ITC 的裁决结果不服，可以向美国联邦巡回上诉法院提起上诉。

排除令（Exclusion Order）是 337 调查中 ITC 最具杀伤力的处罚措施，由美国海关执行，它将直接导致外国企业相关产品无法进入美国市场。

6.1.3【长臂管辖】

美国通过立法和法院判例扩大其管辖权，为司法和执法部门的域外管辖行为提供法律依据，以实现其长臂管辖的目的。依据美国《保护商业秘密法》及《经济间谍法》，如果侵害地在美国，商业秘密是在美国未经授权获得、披露或使用的，则无论侵权人的原籍国在何地，都可能被判向美国公司负担损害赔偿甚至惩罚性赔偿。

6.2【其他发达国家商业秘密保护】

6.2.1【德国商业秘密保护】

6.2.1.1【立法】

2019 年 4 月 26 日，《德国商业秘密法案》生效，开启了德国以单行法保护商业秘密的新篇章。在此之前，德国的商业秘密侵害主要通过反不正当竞争法和刑法来规制。

《德国商业秘密法案》是对欧盟商业秘密保护指令（第 2016/943 号欧盟指令）的具体实施。商业秘密获得保护的前提是商业秘密的合法持有人已经根据具体情况采取了适当的保密措施对其进行保密。《德国商业秘密法案》为保护商业秘密提供了新的民法基础，还同时规定了刑法条款，意味着侵犯商业秘密将会受到刑事处罚。

6.2.1.2【救济途径】

根据《德国商业秘密法案》，商业秘密权利人可以申请对侵权人采取临时禁令，有权要求销毁或归还包含商业秘密的文件或物件，并要求召回、下架、移除或销毁侵权商品。

商业秘密权利人可以申请损害赔偿。关于赔偿金额，权利人可以在“权利人的利润损失”“虚拟但合理的许可费用”以及“侵权人获得的利益”这三种计算方法中选择一种对自己最有利的计算方法。

6.2.2【日本商业秘密保护】

6.2.2.1【立法】

日本主要通过《不正当竞争防止法》来规制侵犯商业秘密的行为，将其作为典型的不正当竞争行为。《不正当竞争防止法》第二条规定，商业秘密是指作为秘密进行管理，尚未众所周知的生产方法、销售方法及其他经营活动中实用的技术上或经营上的情报。

日本现行刑法中没有直接针对侵犯商业秘密行为的条款。但司法实践中可以适用背信罪、泄露秘密罪和贿赂犯罪等罪名对商业秘密进行间接保护。

6.2.2.2【救济途径】

如果商业秘密被侵害，权利人可以通过民事救济途径向法院申请禁令，并可以要求赔偿损失。

如果侵权行为涉嫌构成犯罪，权利人可以向警方报案，要求追究刑事责任。相关刑事制裁包括对个人最高十年监禁和最高 3000 万日元的罚金，对公司最高 10 亿日元的罚金。此外，法院可以没收侵权人因非法披露或使用商业秘密而获得的收入。

自 2015 年《不正当竞争防止法》修订以来，检察官不需要商业秘密权利人的指控，也可以独立提起诉讼。但实践中，检察官仍然需要商业秘密权利人的合作，以便在刑事诉讼中收集足够的证据来证明所指控的行为。

6.3【中国企业的应对】

商业秘密纠纷的复杂性强，涉及的司法程序耗时长，非常耗费精力。企业一旦成为被告，可能会面临市场份额减少、利润损失、经营

能力削弱的不利局面。即便最终被法院认定不构成犯罪，企业也要应对高额的诉讼费用和复杂的涉外司法程序，企业信誉也会受到质疑。

参与国际竞争的中国企业应尽早做好准备，包括了解各国法律、定期自查评估、审慎进行招聘等。若受到指控，建议聘请专业律师，积极应诉。

6.3.1【了解各国法律】

对于一些正在走出国门的中国企业来说，即使企业主要的生产经营活动仍在国内，只要企业已经有开拓海外市场的初步计划，就应将海外涉诉的风险纳入考量，从而有意识地学习了解对应国家的法律，了解哪些信息可能构成受法律保护的商业秘密，以及如何处理这些信息才能够达到合规标准。

6.3.2【实施自查评估】

如果中国企业在国外法院被提起侵犯商业秘密的指控，中国企业应首先明确涉及的信息是否符合商业秘密的法定条件。如果能证明以下事实，将有利于后续应对:

a）不具有秘密性。如果涉及信息在被指控的行为发生时已经是众所周知的信息，那么就不构成商业秘密。比如在互联网、学术期刊可以公开检索到的信息就不具有秘密性。企业还可以尝试证明对方没有对涉及信息采取保密措施，或是涉及信息不具有商业价值。

b）有合法来源。如果中国企业可以证明自己是通过合法途径取得的信息，比如从第三方善意取得或通过自行研发、反向工程取得，就可以证明侵权行为不存在。

6.3.3【聘请专业律师】

聘请具有涉外应诉能力和经验的律师，显得尤为重要。律师可以帮助企业分析起诉状、制定整体应对策略。企业应成立内部专项小组，包括法务部门、业务部门及其他相关部门的成员，配合律师开展应诉工作。律师受保密义务的约束，企业不必过于担心商业秘密会被泄露，对律师需要了解的事实应当如实告知。

6.3.4【审慎招聘】

企业在招聘曾就职于外国企业的员工时，应当持审慎态度。要先

确定该员工没有竞业限制或其他约束，也不会携带前公司的商业秘密加入公司。

6.3.4.1【详尽背景调查】

在招聘过程中，企业应对候选人进行详尽的背景调查，了解其履历的真实性、从原单位离职的原因、是否和原单位签订过保密协议和竞业限制协议，并了解候选人是否有因涉嫌窃取商业秘密等不当行为被调查、起诉的记录。

6.3.4.2【关注来自于竞争对手的员工】

如果企业决定从国内外的竞争对手公司招聘员工，尤其是可能持有对方保密信息的员工，更需要审慎考虑、排除风险。企业在劳动协议中要明确约定，员工在公司工作期间不得违反与任何第三方的保密协议，要求员工承担前雇主要求的保密义务，不得向现雇主泄露其知晓的商业秘密。

6.3.5【寻求外部支持】

企业在接到国外法院或者执法机构的应诉或配合调查的通知后，可以联系负有支持经济发展职责的有关行政机关或者社会团体共同应对。我国的商务部（贸易救济调查局）、地方商务部门、行会商会等可能为企业提供必要的支持。

【相关案例】

案例：美国 PPG 集团诉江苏铁锚公司侵犯商业秘密案（PPG Industries Inc v. Jiangsu Tie Mao Glass Co Ltd）

案件号：2：15-CV-00965

案情简介：2015 年 7 月，美国 PPG 集团在宾夕法尼亚西区联邦地区法院起诉江苏铁锚公司，指控被告雇佣了原告的前雇员 Thomas Rukavina，并通过该雇员获取了原告的 Opticor 相关技术。原告并没有向法院提供证据以证明其实际损失，而主张被告通过侵犯商业秘密获得不当得利。

2021 年 6 月，法院将原告 Opticor 相关技术的研发费用作为评估被告不当得利的基准，认定原告的实际研发费用为约 880 万美元，判决被告向原告支付约 880 万美元的补偿性赔偿和约 1800 万美元的惩戒性赔偿，共计约 2600 万美元。

解读：诉讼中美国法院根据权利人的实际研发费用确定补偿性赔

偿数额。中国企业败诉后还被判支付高昂的惩戒性赔偿。这一案例再次给中国企业敲响警钟，应在招聘国际人才时严格审慎，避免侵犯他人商业秘密。

案例：美国钢铁公司向 ITC 申请针对商业秘密侵权对中国宝钢公司发起 337 调查

案件号：337-TA-1002

案情简介：2016 年 5 月 26 日，美国钢铁公司（U.S. Steel Corporation）向 ITC 申请，对中国输美碳钢及合金钢产品发起 337 调查。原告就被告中国宝钢公司依靠中国钢铁协会合谋操纵产品价格和出口量、标记虚假原产地以规避美国双反税令以及被告通过黑客攻击原告三个诉点提出控诉，请求 ITC 发布普遍排除令及禁止令。2017 年 2 月 22 日，ITC 行政法官裁定，终止关于被告商业秘密诉点的调查。这也是美国 337 调查历史上，中国企业首次获得商业秘密类案件的胜诉。

解读：近年来，中国钢铁产品在国际市场上具有较强的竞争优势，因而遭到美国、欧洲等多个国家和地区的抵制。此次宝钢在 337 调查中获胜意义重大。面对 337 调查，中国企业要善于利用美国当地的法律以及相关国际规则，研究、搜集证据，确定抗辩策略，积极应对此类调查。同时，中国企业也要注重日常的知识产权保护工作，加强数据和证据的留存，这样才能在面对调查时好整以暇，拿出充分证据，取得对自身有利的裁决结果。

案例：摩托罗拉诉海能达盗窃商业秘密案（Motorola Solutions, Inc. v. Hytera Commc’ns Corp）

案件号：1: 17-cv-01973

案情简介:中国海能达通信股份有限公司于 2000 年进入美国市场，四年后成立美国子公司，此后市场布局遍布全球。2017 年 3 月，海能达的竞争对手美国摩托罗拉公司在美国联邦法院对海能达提起盗窃商业秘密的指控。

海能达雇佣了曾任职于摩托罗拉的3名工程师，法院认定他们的侵权责任可以推定至他们的现任雇主海能达。2020年2月15日，美国法院作出一审裁决，认定海能达及其在美子公司侵犯了摩托罗拉的多项商业秘密及著作权，应向摩托罗拉支付损害赔偿3.46亿美元及惩罚性赔偿4.19亿美元，合计约人民币53亿元。海能达将寻求上诉。

解读：在本案中，即使海能达可能存在的相关侵权行为全部发生在美国境外，但美国法院认定海能达在美国的产品销售、广告、维修等行为是在美国境外侵犯商业秘密行为的延伸，并以此确定了美国法院的长臂管辖权。这一点需要中国企业警醒。

案例：美国超导诉华锐风电盗窃商业秘密案（AMSC v. Sinovel Wind Group LLC）

案件号：0578 3: 13CR00084-001

案情简介：美国超导公司和中国华锐风电公司于2005年开始合作，美国超导向华锐风电提供风机设计和技术服务，同时为数千台风机提供电控核心部件和控制软件。2011年合作终止。美国超导随后发现，华锐风电的两名高管说服美国超导的一名负责人加入华锐风电并秘密下载源代码，窃取美国超导的知识产权。2011年6月，美国超导在华锐风电生产的涡轮机中发现了美国超导软件的复制版本。2018年1月，华锐风电和前述三名员工在美国地区法院被判犯有盗窃商业秘密罪和电汇欺诈罪。

解读：这一案件反映出部分中国企业商业秘密保护意识的淡薄。本案中，被告两名高管与原告前员工之间的互联网聊天记录和电子邮件被原告获取并作为证据提交，起到关键性的作用。原告不但在美国提起诉讼，还在中国发布了多起针对华锐风电的诉讼。商业秘密作为一种极具价值的无形财产，对企业发展、国家发展的重要性不言而喻。中国企业不仅要为应对商业秘密涉外纠纷做好准备，也要保护好自己的商业秘密，维护自己在海外市场的合法权益。勇于面对，敢于维权。

附件 1

浦东新区商业秘密侵权投诉举报受理点

序号	受理机构	地址	联系人	固定电话
1	浦东新区 投诉举报中心	洋泾街道杨高中路 2900 号 2 号门		12315/12345
2	陆家嘴市场 监督管理所	陆家嘴街道乳山路 235 弄 2 号	阮迪	58312017
3	洋泾市场 监督管理所	洋泾街道栖山路 171 号	陈晖	58511383
4	花木市场 监督管理所	花木街道牡丹路 185 号	张赢	50451101
5	潍坊市场 监督管理所	潍坊街道潍坊路 131 弄 2 号	束方庆	50938202
6	塘桥市场 监督管理所	塘桥街道南泉路 1325 号	康友维	50942073

7	上钢市场监督管理所	上钢新村街道成山路 200 号	陈晨	20255727
8	金杨市场监督管理所	金杨新村街道栖山路 1025 号	施振欣	68536013
9	沪东市场监督管理所	沪东新村街道利津路 255 号	赵琳	58710105
10	浦兴市场监督管理所	浦兴路街道五莲路 1336 号	陈为庆	58592278
11	东明市场监督管理所	东明路街道灵岩南路 1313 号 4 楼	徐文杰	50187301
12	南码头市场监督管理所	南码头路街道临沂路 128 号一、二层	刘畅	50837857
13	周家渡市场监督管理所	周家渡街道昌里东路 210 号	王永	68700511
14	惠南市场监督管理所	惠南镇北门大街 168 号	邬海华	58000623
15	周浦市场监督管理所	周浦镇周祝公路 1378 号	倪振青	58151337
16	康桥市场监督管理所	康桥镇秀浦路 2388 号 9 号楼	顾洋舟	61182321-205
17	金桥市场监督管理所	金桥镇永建路 102 号 309 室	龙金林	50312565
18	北蔡市场监督管理所	北蔡镇五星路 677 弄 17 号楼	王志军	58432703
19	航头市场监督管理所	航头镇航头路 1198 号	许姚	58229122
20	三林市场监督管理所	三林镇三林路 85 号	张昊	58493404
21	唐镇市场监督管理所	唐镇南曹路 470 号	顾晓斌	58582187
22	高桥市场监督管理所	高桥镇和龙路 338 号	徐昊	58670511

23	张江市场监督管理所	张江镇建中路 1 号	许益	58959046
24	祝桥市场监督管理所	祝桥镇卫亭路 1029 号	沈幸军	58102650
25	新场市场监督管理所	新场镇新环西路 1185 弄 1173 号	甘焊堃	68090737
26	泥城市场监督管理所	泥城镇泥城路 101 号	张明圣	58072621
27	高东市场监督管理所	高东镇赵高公路 1295 号	叶军	68480229
28	曹路市场监督管理所	曹路镇金钻路 62 号	邓悦人	58631253
29	高行市场监督管理所	高行镇东靖路 1831 号	汤恒南	58309353
30	万祥市场监督管理所	万祥镇宏祥北路 83 弄 32 幢	于士	58043292
31	老港市场监督管理所	老港镇良欣路 456 号	顾庆旦	58051454
32	大团市场监督管理所	大团镇南团公路 3030 号	闫少文	58081093-8205
33	合庆市场监督管理所	合庆镇前哨路 200 号	胡剑	58975729
34	宣桥市场监督管理所	宣桥镇沪南公路 8666 弄 11 号楼 4 楼	苗春雨	68009942
35	书院市场监督管理所	书院镇万松路 319 弄 3 幢	李杰	58040075
36	川沙市场监督管理所	川沙新镇华夏东路 2378 号 206	丁戟	68404288
37	南汇新城市场监督管理所	南汇新城镇环湖西三路 869 号二楼	帅银平	20936502-8036
38	保税区分局	华申路 80 号 3 幢 6 层	王政强	50193525

39	度假区分局	申迪北路 700 号 4 号楼	杨正元	20991761

附件 2

上海市商业秘密侵权纠纷民事案件管辖法院

序号	法院名称	地址	联系电话
1	上海知识产权法院	上海市浦东新区张衡路 988 号	021-58951988
2	上海市浦东新区人民法院	上海市浦东新区丁香路 611 号	021-38794518
3	上海市闵行区人民法院	上海市闵行区莘庄镇雅致路 99 号	021-64120000
4	上海市徐汇区人民法院	上海市徐汇区龙漕路 128 号	021-34168168
5	上海市长宁区人民法院	上海市长宁区虹桥路 1133 号	021-52574999
6	上海市金山区人民法院	上海市金山区金山大道 2288 号	021-67965888
7	上海市奉贤区人民法院	上海市奉贤区解放东路 199 号	021-37190666

8	上海市松江区人民法院	上海市松江区南青路 701 号	021-67735555
9	上海市杨浦区人民法院	上海市杨浦区河间路 29 号	021-31372000
10	上海市虹口区人民法院	上海市虹口区北宝兴路 531 号	021-36123300
11	上海市黄浦区人民法院	上海市黄浦区延安东路 1234 号	021-53584777
12	上海市静安区人民法院	上海市静安区共和新路 3009 号	021-26120000
13	上海市普陀区人民法院	上海市普陀区铜川路 1433 号	021-22273333
14	上海市宝山区人民法院	上海市宝山区友谊路 989 号	021-26078989
15	上海市嘉定区人民法院	上海市嘉定区德富路 1221 号	021-59521000
16	上海市青浦区人民法院	上海市青浦区城中北路 555 号	021-69201478
17	上海市崇明区人民法院	上海市崇明区崇明大道 7600 号	021-59611568

附件 3

浦东新区检察机关、公安机关联系表

对外接待机构	办公地点	办公时间	联系方式
上海市浦东新区人民检察院 12309 检察服务中心	上海市浦东新区蔡伦路 68 号	工作日上午 9:00-11:00 下午 13:30-16:30 （周五下午 13:30-16:30）	021-50137200
上海市公安局浦东分局经侦支队	上海市浦东新区康桥路 1710 号	工作日上午 9:00-11:30 下午 13:30-17:00	021-22041240

附件 4

人民法院诉讼资产网备案的知识产权鉴定机构

（查询日期：2023 年 7 月 11 日）

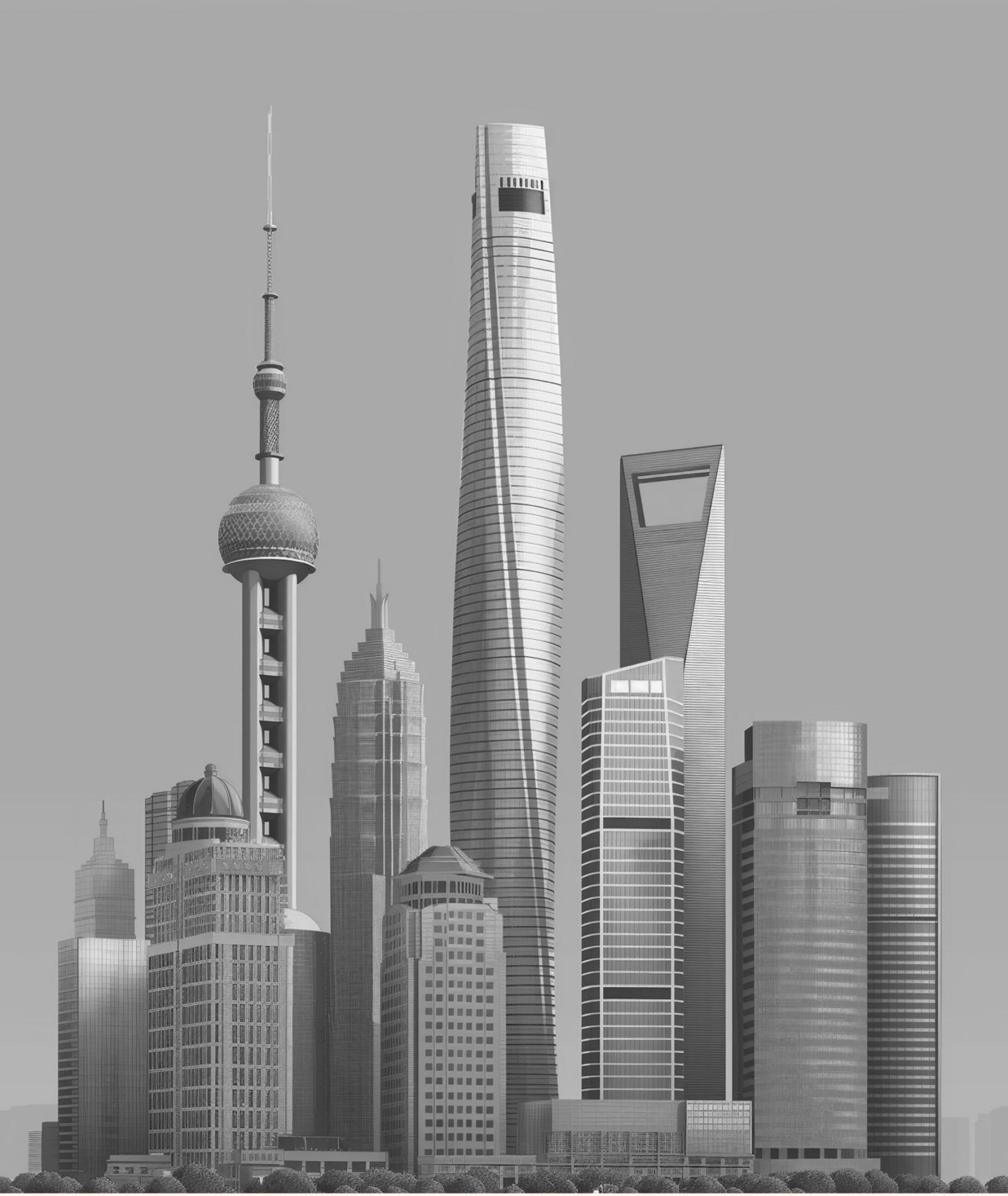
序号	机构名称	地址	联系人	联系电话
1	上海辰星电子数据司法鉴定中心	上海市浦东新区张江高科技园毕昇路 339 号	孙杨	021-68571333
2	上海汉光知识产权数据科技有限公司	中国（上海）自由贸易试验区蔡伦路 333 号 5 幢 609 室	胡惠	021-52666106
3	上海科际知识产权服务中心（有限合伙）	中国（上海）自由贸易试验区新片区环湖西二路 888 号 C 楼	赵婉明	021-53863703
4	上海市知识产权服务中心	上海市徐汇区漕宝路 650 号东幢 2 楼	董黎	021-52287963
5	上海技术交易所有限公司	上海市杨浦区国权北路 1688 弄 68 号 101 室	宋毅	021-65682551
6	上海公沁扬知识产权服务有限责任公司	上海市长宁区凤岗路 500-5 临	陆昱	021-52736778
7	上海硅知识产权交易中心有限公司	上海市徐汇区宜山路 333 号 1 幢 1705 室	徐步陆	021-61154610
8	上海洁湛知识产权服务有限公司	上海市静安区南京西路 1486 号 3102-04 室（实际楼层 27 层）	蒋坡	021-52821776

9	上海科鉴知识产权服务有限公司	上海市松江区新桥镇新站路 361 号	叶枝灿	021-54979833
10	中国电子信息产业发展研究院	北京市海淀区紫竹院路 66 号	吕如婷	010-68209275
11	中国信息通信研究院	北京市海淀区学院路 52 号	闫坤	010-62304259
12	国家工业信息安全发展研究中心	北京市石景山区鲁谷路 35 号	潘妍	010-88686227
13	北京国威知识产权鉴定评估中心有限责任公司	北京市海淀区高粱桥斜街 11 号 7 层 702-2，702-3，702-6	黄俊杰	010-61073453
14	北京菲沃德知识产权咨询有限公司	北京市海淀区西四环北路 125 号 1 幢六层 6043	李克	010-88589011
15	北京国创鼎诚知识产权应用技术研究院	北京市东城区胜古中路 1 号蓝宝商务大厦 A 座 321 号	武斌	010-84670710
16	北京京州知识产权服务中心有限公司	北京市海淀区海淀南路甲 21 号一层 102 号	张旗	010-66175475
17	中国版权保护中心	北京市东城区安定门东大街 28 号雍和大厦 2 号楼 313 室	刘雅琳	010-68003887-5127
18	首都知识产权服务业协会	北京市海淀区海淀南路甲 21 号中关村知识产权大厦 A 座 3 层	高永懿	010-66139027
19	浙江省知识产权研究与服务中心	浙江省杭州市滨江区丹枫路 399 号知识产权大厦	唐灵	0571-88917569

20	浙江省机电产品质量检测所有限公司	浙江省杭州市滨江区庙后王路 125 号 1 幢 1-4 层	吴云舸	0571-88014128
21	浙江省版权协会	浙江省杭州市拱墅区大关路 189 号万通中心 5 幢 303 室	胡伟林	0571-88135633
22	杭州中知鉴证科技有限公司	浙江省杭州市拱墅区东新路 240 号兔狗创新大厦附楼 3A 层	黎艳枝	0571-86385122
23	杭州索图知识产权服务有限公司	浙江省杭州市拱墅区东新路 533 号蔚蓝国际大厦 1 号楼 2007 室	张得明	0571-88015657
24	杭州市知识产权保护中心	浙江省杭州市滨江区丹枫路 399 号知识产权大厦 1 号楼 10 楼	潘伟祥	0571-87075161
2627	浙江现代智慧城市研究院	浙江省杭州市西湖区文三路 498 号天苑花园 3 号楼 21 层 2102 室	张韧佳	0571-85293681
28	浙江方圆检测集团股份有限公司	浙江省杭州市杭州经济开发区下沙区 300 号	陈勇	0571-81387885
29	浙江华证知识产权服务有限公司	浙江省丽水市莲都区花园路 422 号兴业大厦 254 室	杨晓波	0578-2117659
30	宁波科集技术服务有限公司	浙江省宁波市高新区扬帆路 999 弄 5 号 508-10 室	周佳	0574-87919769
31	江苏省科协企业创新服务中心	江苏省南京市建邺区梦都大街 50 号	王晓忠 周辉	025-84407703 025-84411967
32	江苏省知识产权保护中心	江苏省南京市建邺区汉中门大街 145 号省政府服务中心二期 6 楼	刘迷迷	025-83236255

33	山东知识产权司法鉴定中心	山东省济南市历城区舜华路 2020 号	刘洁	0531-88198563
34	山东知鉴知识产权司法鉴定有限公司	山东省济南市历城区舜华路 2020 号	刘洁	0531-68792110
35	山东国润资产评估有限公司	山东省济南市市中区顺河东街 66 号银座晶都国际广场 2-1806	乔守朋	0531-82377950
36	华知鉴（山东）知识产权咨询服务有限公司	山东省济南市历下区经十路 15982 号第一大道 1701 室	王怡然	0531-86920987
37	山东天德汇资产评估有限公司	山东省济南市历城区华龙路 1110 号三威大厦 804 室	窦希文	0531-88035658
38	广东省知识产权保护中心	广东省广州市越秀区先烈中路 100 号大院 60 栋 9 楼	梅颖娟	020-87681613
39	中科检测技术服务（广州）股份有限公司	广东省广州市天河区兴科路 368 号实验楼 A 房	宋泽安	020-88526904
40	深圳市公标知识产权鉴定评估中心	广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室	邓光昀	82666050
41	四川汇西知识产权鉴定评估有限公司	四川省成都市高新区天府五街 200 号 7 号楼 5 层 504 号	田晓玲	028-85969739
42	四川西部知识产权鉴定评估有限公司	四川省成都市金牛区马家花园路 2 号第 9 层 908-909 号	张锋	028-87656123
43	江西清析知识产权服务有限公司	江西省南昌市青云谱区新溪桥东二路 99 号	许文友	17775205527

44	江西原因质检鉴定中心有限公司	江西省上饶市信州区滨江西路 66 号 1、2、3、5 幢 3#704	秦立生	18198989098
45	西知鉴知识产权鉴定评估（重庆）有限公司	重庆市渝北区回兴街道宝圣大道 209 号西正街 A 座 18-8	曾得国	023-67258340
46	昆明鸿润资产评估有限公司	云南省昆明市青年路 145 号盛迪大厦二楼	李俊	0871-63137751
47	湖南湘鉴知识产权鉴定评估中心有限公司	湖南省长沙市岳麓区潇湘中路 113 号	鲁鹏	0731-85417803



浦东新区企业商业秘密保护指南