二零二零年十月十八日

100820
北京市西城区三里河东路 8 号
国家市场监督管理总局价格监督检查和反不正当竞争局

电子邮件信箱：fbzdjzc@vip.126.com

主题：《商业秘密保护规定（征求意见稿）》

致国家市场监督管理总局：

美国知识产权所有人协会（下称“IPO 协会”）感谢有机会对 2020 年 9 月 4 日发布的《商业秘密保护规定（征求意见稿）》（下称“《规定》”）提交意见。

IPO 协会是一家代表各行业、各技术领域内拥有知识产权或相关权益的公司和个人的国际性行业协会。它拥有一百七十五家公司会员以及大约一万两千名个人会员。这些个人会员有些从属于公司会员或律所成员，有些是发明人、作者或律师会员。IPO 协会的会员遍及三十多个国家。

IPO 协会提倡有效和实惠的知识产权，为会员提供广泛的服务，包括支持会员在立法和国际事务中的利益、分析当前知识产权问题、提供教育和信息服务、以及向公众传播知识产权的重要性。

IPO 协会感谢《规定》中提出的目标，包括加强对企业商业秘密的保护，制止与《反不正当竞争法》有关的不正当竞争和对商业秘密的侵害。我们注意到《规定》似乎反映了中美两国最近签订的第一阶段经济与贸易协议（“第一阶段协议”）中与商业秘密相关的某些规定。IPO 协会认为此次公开征求意见是对“第一阶段协议”第 1.4 条记载的两国加强在商业秘密保护方面合作的协议的重要且有益的落实。我们希望我们的意见将在《规定》的定稿过程中提供帮助，并为商业秘密保护的未来发展提供信息。

1501 M Street, NW, Suite 1150 ● Washington, DC 20005
T: 202-507-4500 ● F: 202-507-4501 ● E: info@ipo.org ● W: www.ipo.org

总体意见

《规定》考虑使行政机关在商业秘密执法方面发挥更广泛的作用。我们赞赏这可以提高解决侵犯商业秘密问题的速度和效率，使权利人受益。但是，我们谨提出，在促进使用行政机构和信任行政机构解决商业秘密纠纷方面，与人民法院相比，这种促进和信任需要为相关方提供与经由司法审查相同程度的一致性、可预期性、透明度、监督和程序保障。

例如，在透明度方面，IPO 协会欢迎公开行政措施和决定，以及定期报告执法统计数据，例如启动和结案的案件数量，所涉当事人的身份以及结果。就侵犯商业秘密的行政执法和刑事执法之间的机制和相互作用方面提供更多指导也将是有益的。

在一致性和可预期性方面，我们认为，公众将受益于行政程序（例如，如《规定》中所明确的）与法院（例如，在最高人民法院关于 2020 年 9 月 10 日发布的《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》中所述的）在《反不正当竞争法》的适用和解释方面的一致性。与司法途径相比，行政程序的解释或适用可能存在不一致之处，我们欢迎国家层面的指导意见，例如国务院可能出台的条例。

第三条

IPO 协会关注第三条涉及的两个方面。首先，第三条似乎旨在使《规定》仅适用于中国实体而非外国实体拥有的商业秘密。《规定》所管理的是对外国实体具有重大意义的问题（正如“第一阶段贸易协议”中有关商业秘密的条款所表明的那样），因此这一区别是不合适的，而且是与没有此限制的《反不正当竞争法》不一致的。

其次，“提供帮助”一词含义广泛，可能给许多提供商品和服务的无辜当事人带来责任。例如，U 盘经常被用于商业秘密侵害活动中 - 我们认为《规定》并非意在让 U 盘制造商对他人的侵权活动负责。扫描仪和打印机的制造商以及云存储和电子邮件服务的提供商也存在同样的问题。就此而言，对于对他人的侵权行为承担责任的情形，应该有一个“知道或应当知道”的心理状态要求。当一个实体故意无视明显的侵权证据时，可以认定该实体“应当知道”侵权。因此，IPO 建议以下修改：

> **第三条【适用范围】**任何自然人、法人或非法人组织实施了侵犯**中国**商业秘密权利人的商业秘密的行为或**在知道或应当知道侵权的情况下**为其实施侵犯商业秘密行为提供帮助的行为，均适用本规定。

第五条

《规定》第五条对“技术信息”、“经营信息”和“商业秘密”等术语进行了定义。“方案”一词用于界定“技术信息”，就此类信息的目的、范围或完整性而言是误导性的。我们建议对此定义不使用“方案”：

> 本规定所称技术信息是指利用科学技术知识、信息和经验获得的技术**性信息方案**，包括但不限于设计、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、计算机软件源代码和有关文档等信息。

第六条

《规定》第六条涉及属于“不为公众所知悉”和不属于“不为公众所知悉”的信息类型，即秘密信息或非秘密信息。根据第六条，如果信息不为其所属领域的相关人员普遍知悉或者不能从公开渠道容易获得，则认为该信息不为公众所知悉。

对于这一判定而言，重要的是如何解释“领域”一词的范围。在澄清该用语时，我们谨建议根据《与贸易有关的知识产权协议》（以下简称“TRIPS”）第七节第三十九条对该第六条进行修正，其中当信息不为“通常处理所涉信息范围内的人”所普遍知道，或不易被他们获得时，该信息被视为秘密。我们还注意到，当作为整体考虑时，可公开获得的信息也可能属于“不为公众所知悉”的信息。更具体地，作品的个别部分可能是众所周知的，但这并不排除对秘密组合的保护。在确定信息是否不为公众所知悉时，必须着眼于整个作品（例如，汇编），而不是其个别部分。整体来看不为公众所知悉的信息示例包括（但不限于）客户联系名单和客户线索数据。

第六条还涉及信息不属于“不为公众所知悉”的五种情形，我们建议修改情形（二）、删除情形（四）并修改情形（五）。

更具体地说，情形（二）涵盖了在国内外“公开使用”的信息。由于公开使用的信息通常隐藏在公开使用的产品中，因此这种情况往往难以觉察和识别。情形（二）还规定了超出 TRIPS 商业秘密要求（即第七节第三十九条）的条件。根据TRIPS，秘密性不会因信息被公开使用而丧失。而是，当信息是普遍知道的或容易获得时，秘密性丧失。因此，我们建议对情形（二）进行修改，以涵盖普遍知悉或容易获得的信息，而不是涵盖公开使用的信息。

情形（四）涵盖无需付出一定的代价而容易获得或者从其他公开渠道可以获得的信息。这种情形相当模糊。这就产生了一些问题，例如：什么样的代价才使信息不再被视为“不为公众所知悉”？这种“一定的代价”是否应随时间变化？付出一定的代价而不再“容易”获得信息的情形有哪些？鉴于难以确定何时满足情形（四），我们谨建议删除该情形。

情形（五）仅涉及产品尺寸、结构、部件的简单组合等内容信息，进入公开领域后相关公众可通过观察、测绘、拆卸等简单方法获得。我们建议将这一情形扩大以包括进入公开领域后相关公众可通过观察、测绘、拆卸等简单方法获得的任何信息。

第六条还允许在质疑信息不为公众所知悉的推定时提供证据。我们谨强烈要求，在推翻这一推定之前，必须提供足够清楚的相反证据。

鉴于上述情况，我们建议对第六条进行如下修改：

第六条【不为公众所知悉】本规定所称不为公众所知悉，是指该信息**作为整体**不为**其所属领域的通常处理所涉信息范围内的**相关人员普遍知悉或者**不易被其获得不能从公开渠道容易获得。**

具有**包括但不限于**下列情形之一的，可以认定有关信息不构成“不为公众所知悉”：

（一）该信息已经在国内外公开出版物或者其他**公开**媒体上公开披露或者已经通过公开的报告会、展览等方式公开**披露**；
（二）该信息已经在国内外**普遍知悉或容易获得公开使用**；
（三）该信息为其所属领域的相关人员普遍掌握的常识或者行业惯例；
~~**（四）该信息无需付出一定的代价而容易获得或者从其他公开渠道可以获得；**~~
~~**（五）仅涉及产品尺寸、结构、部件的简单组合等内容信息，**~~**（四）**进入公开领域后相关公众可通过观察、测绘、拆卸等简单方法获得**的信息。**

例如但不限于申请人提交的技术查新报告、检索报告、公开渠道查询商业信息的资料等**信息**与涉案信息不构成实质上相同的，可以推定该信息“不为公众所知悉”，但有**足够清楚的**相反证据证明的除外。

第八条

第八条列举了商业秘密权利人为防止信息泄漏而采取的八类“相应保密措施”。我们注意到，商业秘密权利人采取的保密措施是否“合理”取决于对权利人业务的独特情况的考虑。因此，八类具体措施中的任何一项是否可能“足以”防止某些泄密并不能决定所采取的措施总体上是否合理。我们建议这八项措施仅仅是对于行为的说明性而非限制性示例，而不是规定对其中某项措施的满足是决定性的；由此，结合背景考虑，该等行为可能会支持相应的保密措施是合理的这一结论。此外，是否可以独立获取或开发商业秘密，不应作为判断权利人是否已采取适当的保密措施来保护自己的商业秘密的因素。因此，我们谨建议进行以下修改：

> **第八条【相应保密措施】**本规定所称权利人采取相应保密措施，是指权利人为防止信息泄露所采取的与商业秘密的商业价值~~、独立获取难度~~等因素相适应、合理且具有针对性的保密措施。
>
> ~~**具有下列情形之一，足以防止涉密信息泄漏的，可以认定**~~**在认定**权利人**是否**采取了“相应保密措施”**时应考虑下列非限制性情形**：

第十条

《规定》第十条涉及自然人为了法人或非法人组织所研究或开发的商业秘密的所有权问题。在这方面，我们谨建议对第十条进行修改而体现当事人之间的协议对商业秘密所有权的控制，而无论该商业秘密是否在法人或非法人组织的实际或预期业务范围之内或之外。我们还建议，应根据法人或非法人组织的实际或预期业务来确定商业秘密的所有权，而不是根据分配给自然人的工作任务来确定。这样，就自然人进行的研究或开发工作而言，自然人与法人或非法人组织之间则不太可能就此发生冲突。通过采用这种方法，可以避免涉及有关任务是在该自然人的工作安排范围之内还是之外的争议。

第十条还涉及自然人创造商业秘密利用了法人或非法人组织的物质技术条件或经验的情况。尽管自然人将拥有商业秘密的所有权，但我们谨提出，利用法人或非法人组织资源的对价应当是，在法人或非法人组织的业务范围内使用商业秘密而无需向自然人支付报酬的权利。也就是说，从公平和公正的角度来讲，法人或非法人组织有权使用该商业秘密，而无需向该自然人支付额外的费用。

鉴于上述情况，我们建议对第十条进行如下修改：

> **第十条【权利归属】**自然人为了**完成**法人或者非法人组织**工作任务的实际或预期业务、或者在实际或预期业务范围之内**所研究或开发的商业秘密，归法人或者非法人组织所有，但当事人另有约定的，从其约定。**此外，除当事人另有约定外，**自然人在法人或者非法人组织**实际或预期业务工作任务**以外所研究或开发的商业秘密，归该自然人所有。

但其商业秘密系利用法人或者非法人组织的物质技术条件或经验的，法人或者非法人组织有权**在支付合理报酬后，**~~，~~于其业务范围内使用该商业秘密。

第十一条

根据《反不正当竞争法》的规定，我们建议“侵权人”还包括那些在知道或应当知道违反《规定》的情况下允许或协助他人违反《规定》获取、披露和/或使用商业秘密的人。如下所示：

第十一条【侵权人】本规定所称侵权人，是指违反本规定获取、披露**和/或**~~、~~使用商业秘密的自然人、法人或者非法人组织**，或者在自然人、法人或非法人组织知道或应当知道违反本规定的情况下，允许或协助他人获取、披露和/或使用商业秘密**。

第十二条

第十二条列举了构成“非法获取”商业秘密的示例。首先，我们谨寻求澄清第（二）项中所述的“设计陷阱”的含义。

此外，我们建议在与电子信息系统有关的第（三）项中添加“数据抓取”。数据抓取是一种技术，其中计算机程序从在线数据库的输出中提取数据，而提取的方式往往并不是该目标在线数据库的管理员所能合理预想的。在线数据库的操作员通常会将这种数据抓取视为不受欢迎的行为，这是因为，除了丧失控制和增加系统负荷可能阻却用户之外，还有诸如窃取数据库中受保护的内容（“非法获取”商业秘密）等原因。为了澄清，将数据抓取与更无害的“解析”区分开，在“解析”的情况下，“被抓取”的输出仅用于显示给最终用户，而不是作为另一个程序的输入（在数据抓取的情况下）。因此，我们建议对第（三）项进行以下修改：

（三）未经授权或超出授权范围进入权利人的电子信息系统获取商业秘密或者植入电脑病毒破坏其商业秘密的，**包括但不限于未经授权的数据抓取，**其中，电子信息系统是指所有存储权利人商业秘密的电子载体，包括数字化办公系统、服务器、邮箱、云盘、应用账户等；

我们进一步建议增加另外的第（六）项，该条款涉及解雇后未经授权保留雇主的商业秘密材料：

（六）在终止雇佣关系后未经许可保留雇主的商业秘密材料。

第十三条

与对第三条讨论的原则类似，我们关注的是，对于那些提供了商品和服务而被用于侵害商业秘密的情况，在提供者（例如，相机制造商）不知道且没有理由知道侵权的情况下而被设定了承担责任。因此，我们建议承担责任应满足“知道或应当知道”的心理状态要求。

此外，一项行为是否构成“披露”，不应该取决于第十三条第二款所要求的其是否“足以破坏权利人的竞争优势或损害其经济利益”。对竞争优势和经济利益的评价更适合用于认定“商业秘密”和/或损失程度，而不是针对商业秘密是否被不当“披露”。

第十三条第三款将“使用”定义为将商业秘密应用于产品设计、产品制造、市场营销及其改进工作、研究分析等。这种“使用”的内涵似乎过于狭隘，应当定义为任何使权利人受损或使侵权人受益的、对商业秘密信息的利用。例如，这包括为产品或服务的开发或供给提供信息、帮助或使其加快。因此，我们建议以下修改：

> **第十三条【披露、使用】在经营者知道或者应当知道商业秘密是以不正当手段获取的情况下，**经营者不得披露、使用或者允许他人使用以不正当手段获取的权利人的商业秘密。
>
> 本条所称“披露”，是指将权利人的商业秘密公开~~，足以破坏权利人的竞争优势或损害其经济利益的行为~~。
>
> 本条所称“使用”，是指**任何使权利人受损或者使侵权人受益的、对于**将权利人的商业秘密**的**利用于**，包括但不限于为**产品设计、产品制造、市场营销及其改进工作、研究分析等**的开发或者供给提供信息、帮助或使其加快**。

第十四条

如第三条和第十三条所述，我们关注的是，对于那些提供了商品和服务而被用于侵害商业秘密的情况，在提供者（例如，相机制造商）不知道且没有理由知道侵权的情况下而被设定了承担责任。因此，我们建议承担责任应满足“知道或应当知道”的心理状态要求，如下所示：

> **第十四条【保密义务和权利人有关保守商业秘密的要求】在经营者知道或者应当知道会构成违反保密义务的情况下，**经营者不得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。

第十五条

第十五条第二款规定："员工或前员工在工作过程中所形成的自身知识、经验、技能除外"。这是有问题的，因为这可以被解释为，赋予了记忆力好的员工使用商业秘密并将其透露给第三方的权利。我们建议删除此句。我们还建议对该条进行修改，以明确其适用于经双方同意的限制，而与协议类型无关：

本条所称"限制性使用商业秘密"，包括但不限于**~~在保密协议、劳动合同、合作协议、合同等中与权利人订立的~~对商业秘密使用的**法定**限制**或**当事人之间**约定的**对商业秘密的**限制**使用**。**~~员工或前员工在工作过程中所形成的自身知识、经验、技能除外。~~**

第十六条

如第三条、第十三条和第十四条所述，我们建议承担责任应满足"知道或应当知道"的心理状态要求，如下所示：

第十六条【教唆、引诱、帮助侵犯商业秘密】在经营者知道或者应当知道会构成违反保密义务或违反权利人要求的情况下，经营者不得教唆、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。

第十八条

第十八条涉及某些客户名单的保护。本条例对客户名单的描述非常具体，我们认为这导致涵盖范围太窄，无法为本应在《反不正当竞争法》下受到的保护客户名单提供足够的保护。因此，我们建议做出澄清，即，第十八条中的描述仅仅是示例性的，并不排除应作为商业秘密加以保护的其他类型的客户名单。

我们还注意到，第十八条规定了"不正当手段"的例外，即客户"自愿"选择与前员工进行交易。我们担心的是，在前员工利用雇主的客户名单招揽雇主客户并与之进行交易的情况下，同意交易的客户很可能会声称交易是"自愿"进行的。关于是否使用"不正当手段"的决定性因素应该是前员工在该过程中是否招揽了客户或使用了权利人的保密信息，而不是看客户的意愿。因此，我们建议以下修改：

第十八条【客户名单】权利人经过商业成本的付出，形成了在一定期间内相对固定的且具有独特交易习惯等内容的客户名单，可以获得商

业秘密保护。**根据《反不正当竞争法》，本条例未规定的其他类型的客户名单也可以作为商业秘密。**

前款所称的客户名单，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知信息的特殊客户信息，包括汇集众多客户的客户名册，以及保持长期稳定交易关系的特定客户。客户基于对职工个人的信赖而与职工所在单位进行市场交易，该职工离职后，能够证明客户**未经员工的招揽或使用权利人的保密信息而自愿**选择与自己或者其新单位进行市场交易的，应当认定没有采用不正当手段。

第十九条

第十九条涉及侵犯商业秘密的例外。通过增加对于做出发现或进行研发时产生的书面记录的要求，例外（一）将提供更加一致和可预测的结果。例外（四）涉及两种不同情况：公共政策例外和举报人保护。我们建议将例外（四）分为以下两部分，以便更容易理解。如下所示，针对公共利益或国家利益修订的例外（四）侧重于环境、健康和安全方面的问题，而新的例外（五）规定了向政府当局举报不法行为的准则（举报人例外）。

关于“反向工程”，“接触、了解权利人或持有人技术秘密的人员通过回忆、拆解终端产品获取权利人技术秘密的行为”是否是“反向工程”的例外，还是已经被例外（二）（“通过不正当手段获得”或“或违反保密义务”）所涵盖。与第十五条类似，残留或记忆的清晰性对评估员工行为很重要。我们建议删除此内容，为了清楚起见，在例外（二）中添加“合同义务”。

此外，IPO 认为举报人保护是有益的，但是根据如《规定》作为行政要求似乎不适合。

第十九条【侵犯商业秘密行为的例外】下列行为不属于侵犯商业秘密行为：

（一）**有同期书面记录证明的**独立发现或者自行研发；

（二）通过反向工程等类似方式获得商业秘密的，但商业秘密或者产品系通过不正当手段获得、或违反保密义务**或合同义务**的反向工程除外；

（三）股东依法行使知情权而获取公司商业秘密的，但不得进一步分享或利用公司商业秘密牟取利益；

（四）~~商业秘密权利人或持有人的员工、前员工或合作方基于环境保护、公共卫生、公共安全、揭露违法犯罪行为等公共利益或国家利益需要，而必须披露商业秘密的。~~依法需要披露商业秘密，但仅限于为公共利益或国家利益而需要披露的、与环境保护、公共卫生和公共安全有关的信息，且权利人有机会就披露的依据是否合理向有关部门提出异议；

（五）商业秘密权利人或持有人的员工、前员工或合作方为举报违法和/或犯罪活动而向有关部门秘密披露商业秘密；

前款所称反向工程，是指通过技术手段对从公开渠道取得的产品进行拆卸、测绘、分析等而获得该产品的有关技术信息~~，但是接触、了解权利人或持有人技术秘密的人员通过回忆、拆解终端产品获取权利人技术秘密的行为，不构成反向工程~~。

披露人在向有关国家行政机关、司法机关及其工作人员举报前述违法犯罪行为时，须以保密方式提交包含商业秘密的文件或法律文书。

~~商业秘密权利人或持有人应在其与员工、合作者、顾问等签订的管控商业秘密或其他保密信息使用的任何合同或协议中，向后者提供举报豁免和反报复条款。合同或协议的形式包括但不限于劳动合同、独立承包商协议、咨询协议、分离和解除索赔协议、遣散协议、竞业禁止协议、保密和所有权协议、员工手册等~~。

第二十条

第二十条赋予县级部门认定查处侵犯商业秘密行为的权力。第十九条赋予执法机关很大的自由裁量权，可以将某些商业秘密排除在保护范围之外。同样，第三十一条赋予这些机关以自由裁量权，可以将某些违反商业秘密的行为认定为情节严重，并可能触发罚款和其他补救措施。IPO 协会认为，在这种情况下，为更一致和更可预期的执法，将这些责任赋予具有更广泛的地理范围覆盖的部门是更可取的。因此，我们建议将对侵权的调查和认定提高到省级：

第二十条【执法机关】侵犯商业秘密行为由**省级县级**以上市场监督管理部门认定查处。

第二十二条

第二十二条涉及在商业秘密认定中鉴定的使用。本条中所涉及的第三方实体，即鉴定机构和有专门知识的人，应要求其独立于各方，以确保其可信度。此外，应该要求这些实体将其收到的信息作为保密信息加以保护，以维持有关信息的保密状态。因此，IPO 协会建议进行以下修改：

第二十二条【委托鉴定】权利人、涉嫌侵权人可以委托有法定资质且**独立的**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。**鉴定机构应当对其收到的信息保密。**

权利人、涉嫌侵权人可以委托**独立的且**有专门知识的人对权利人的信息是否为公众所知悉等专门性事项提出意见。**有专门知识的人应当对其收到的信息保密。**

第二十三条

第二十三条针对涉及计算机软件程序的侵犯商业秘密的认定。应当明确的是，侵权人不能仅仅因为涉案软件代码（包括源代码）与涉案商业秘密不同而免于侵权责任。因此，我们建议采用“相同或实质相似”的标准，如下所示：

第二十三条【涉及计算机软件程序的证据认定】侵犯商业秘密行为涉及计算机软件程序的，可以从该商业秘密的软件文档、**源代码或**目标程序与被控侵权行为涉及的软件是否相同**或实质相似**，或者被控侵权行为涉及的计算机软件**源代码或**目标程序中是否存在权利人主张商业秘密的计算机软件特有内容**（包括配置参数，数据库结构等）**，或者在软件结果（包括软件界面、运行参数**、数据库结构**等）方面与该商业秘密是否相同**或实质相似**等方面进行判断，认定二者是否构成实质上相同。

第二十五条

第二十五条规定，侵犯商业秘密行为涉及计算机技术的，应当扣押相关计算机服务器、主机、硬盘等存储设备。鉴于只有在非常情况下才应准予扣押，谨此提出，除通常不可弥补的损害和权益平衡之外，只有在有证据清楚表明涉嫌侵权人（一）不会遵守任何其他形式的命令、（二）实际拥有包含商业秘密的特定财产、（三）盗用了商业秘密或与他人合谋这样做（这不包括无辜的第三方，例如云提供商或互联网服务提供商），且（四）如果给与通知，将销毁、移动、隐藏或以其他方式使该秘密无法接触时，才可以进行扣押。

我们还建议采取以下额外的保护措施：（一）提供调查结果和结论，以证明扣押的合理性；（二）限制为针对必要财产的最低程度扣押；（三）禁止权利人接触或复制信息；（四）明确执法部门的扣押条件；（五）在很短的时间内安排审理，例如七天；（六）要求权利人缴纳担保金。此外，我们建议将所有扣押的材料存放在市场监管部门，并在已告知的审理结束前予以保密。最好在市场监督管理部门内指定专人将商业秘密信息与其他财产分开，以使其他财产及时归还给涉嫌侵权人。鉴于上述情况，我们建议在第二十五条末尾增加以下内容：

尽管有上述规定，但仅在非常情况下才可授权这种扣押行为，除通常不可弥补的损害和权益平衡之外，只有在有证据清楚表明涉嫌侵权人（一）将逃避、回避或不遵守任何其他形式的命令；（二）实际拥有包含商业秘密的特定财产、（三）盗用了商业秘密或与他人合谋这样做（这不包括无辜的第三方，例如云提供商或互联网服务提供商），且（四）如果给与通知，将销毁、移动、隐藏或以其他方式使该秘密无法接触时，才可以进行扣押。

扣押令必须（一）包括调查结果和结论；（二）规定对必要财产的最低程度扣押；（三）禁止权利人接触或复制信息；（四）明确执法部门的扣押条件；（五）在很短的时间内安排审理；和（六）要求权利人缴纳担保金。所有扣押的材料存放在市场监管部门，并在已告知的审理结束前予以保密。在市场监督管理部门内指定专人将商业秘密信息与其他财产分开，以使其他财产及时归还给涉嫌侵权人。

第三十一条

第三十一条涉及《反不正当竞争法》第二十一条所称的“情节严重”。在评估商业秘密侵害的经济影响方面，我们注意到，第三十一条基于权利人的损失或侵权

人的获利设定了五十万元的门槛。根据中国最高人民法院、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”的解释（三）》（法释【2020】10号，自2020年9月14日起施行），商业秘密刑事责任的入罪数额已经降低至三十万元。

IPO协会建议，将权利人的损失、侵权人的违法所得和合理的使用费的总和计入三十万元的门槛，前提是合并后的损失不存在对同一损害的重复计算。

IPO协会建议使用三种普遍适用的方法来评估因侵害商业秘密而造成的总损失，以确定是否“情节严重”：（一）实际损失（利润损失，以及价格或市场侵蚀）；（二）违法所得（不当得利），包括非法收入，侵权人获得的不正当利益，例如但不限于加快开发时间和避免开发成本；（三）合理的使用费。上述每一种方法都可以与其他方法结合使用，前提是合并后的损失不存在对同一损害的重复计算。如果总额超过三十万元的门槛，则符合《反不正当竞争法》第二十一条所称的“情节严重”。

我们特别提出加快开发这一概念，即允许尽早进入市场（这使商业秘密权利人丧失了其全部“先发”优势）。此外，我们建议在确定侵权人的违法所得和/或商业秘密权利人的损失时，应考虑其他可能的侵权方面，例如随同销售。这是因为，在侵犯商业秘密的案件中，被告不仅可能从与受商业秘密保护的产品相关的销售中不正当地获利，而且可能从与受商业秘密保护的产品一起销售的附赠或附属产品的销售中不正当地获利。同样，商业秘密权利人的损失可能不限于受商业秘密保护的产品，还可能是由随同销售产品造成的。

关于情形（三）（“造成权利人破产的”），我们注意到许多互不相关的商业因素可能成为企业破产的部分或全部原因。我们担心的是，如果有人指控商业秘密侵害导致破产，那么如果没有来自原告的证据开示，被告将很难证明破产是出于无关的原因。我们还认为，权利人的损失、侵权人的违法所得和合理的使用费（无同一损害的重复计算）三者一起构成更合适的标准。因此，我们建议将作为《反不正当竞争法》中“情节严重”的一个独立原因的“造成权利人破产的”的情形（三）删除。

关于情行（六）（“造成国家、社会重大经济损失，或具有恶劣社会影响的”）和情行（七）（“其他情节严重的行为”），我们认为这些规定旨在作为对第三十一条未列举的其他严重行为的总括性条款。但是，由于这些规定含糊不清且可能非常广泛，因此，我们希望进一步澄清其范围和适用性。

第三十一条【情节严重】符合以下情形之一的，可以认定为《反不正当竞争法》第二十一条所称的情节严重：

（一）因侵害商业秘密造成**的**权利人损失**（包括随同销售）、侵权人违法所得（包括加快开发和随同销售）以及合理使用费的合计**超

过**三五**十万元的**，前提是合并后的金额不存在对同一损害的重复计算**；

~~**（二）因侵害商业秘密获利超过五十万元的；**~~

~~**（三）造成权利人破产的；**~~

（四）拒不赔偿权利人的损失的；

（五）电子侵入方式造成权利人办公系统网络和电脑数据被严重损坏的；

（六）造成国家、社会重大经济损失，或具有恶劣社会影响的；

（七）其他情节严重的行为。

第三十三条

第三十三条涉及针对商业秘密主张的“合法来源”抗辩。但是，支持这种抗辩的证据应与合理注意义务相联系，而合理注意义务与生产经营规模和实践相关。鉴于难以评估商业秘密的价值，商业秘密使用的“合理对价”也极难评估。因此，我们谨建议对第三十三条进行以下修改：

第三十三条【善意侵权】为生产经营目的使用不知道是未经商业秘密权利人许可的商业秘密，且能举证证明该商业秘密**是基于合理注意义务合法**来源**合法**的，应责令侵权人停止上述使用行为~~，**但商业秘密的使用者能举证证明其已支付合理对价的除外**~~。

第三十四条

第三十四条涉及侵犯商业秘密违法所得的计算。该条第二款提到计算违法所得可以考虑的证据类型。如前所述，侵权人的违法所得还应包括加快开发和随同销售。此外，权利人提供与调查有关的证据时，也应考虑这些证据。因此，我们建议进行以下修改：

第三十四条【违法所得的计算】《反不正当竞争法》第二十一条所称违法所得是指，以侵权人违法生产、销售商品或者提供服务**（包括随同销售）**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，以及**因加快开发而获得的收益**。

市场监督管理部门可以综合参考商业秘密侵权人的会计账簿、生产记录、销售记录、转让协议等资料**以及权利人提供的其他证据**，计算违法所得的数额。

我们还建议提供其他证据（例如，权利人提交的证据）的示例，据此确定损失金额。具体来说，此类示例可包含以下信息：

- 侵权人关于销售或商业活动的公开声明，
- 侵权人在商店或其他渠道中的产品定价，
- 市场调查，
- 向政府机构提交的监管文件中的声明，
- 通过首次公开募股（IPO）公开的信息，
- 客户的收据，
- 第三方的零售销售信息，以及
- 其它有关侵权活动规模和范围的信息。

第三十五条

第三十五条涉及计算权利人损害的几种方法。如果难以确定因侵权所造成的权利人销售量减少的数量（如第一种计算方法）或涉嫌侵权人销售的每件侵权产品的合理利润（如第二种计算方法），谨建议使用另外方法。在这种另外的方法下，将根据所销售的侵权产品总数乘以权利人的与每件侵权产品有关的合理利润所得之积来确定损害。

关于涉及商业秘密许可他人使用的价款的方法，我们建议明确该价款是由权利人设定的。

如前所述，我们还建议在计算损害时，即确定权利人受到的实际损失和侵权人获得的利益时，包括随同销售。更具体地说，商业秘密权利人的损失可能不限于受商业秘密保护的产品，还可能来源于随同销售（即与受商业秘密保护的产品一起销售的附赠或附属产品的销售）。同样，侵权人可能会从侵权产品和相关随同产品的销售中获得不正当利益。

鉴于上述情况，我们建议对第三十五条进行以下修改：

第三十五条【造成权利人损害的计算】市场监督管理部门调查侵犯商业秘密行为造成权利人的损害的，应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。在计算“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”的时候，可以参照下列计算方法：

（一）权利人的产品因侵权所造成销售量减少的总数乘以每件产品的合理利润所得之积；

（二）权利人销售量减少的总数难以确定的，侵权产品在市场上销售的总数乘以每件产品的合理利润所得之积；

（三）第（一）项或者第（二）项难以确定的，侵权产品在市场上销售的总数乘以涉及商业秘密的权利人的每件产品的合理利润所得之积；

（四） ~~**（三）**~~按照通常情形权利人可得的预期利润，减去被侵害后使用同一信息的产品所得利益之差额；

（五） ~~**（四）由**~~**权利人设定的**商业秘密许可他人使用的价款；

（六） ~~**（五）**~~根据商业秘密研究开发成本、实施的收益、可得利益、可保持竞争优势的时间等因素确定商业秘密的价值，并以该价值的一定比例确定“权利人因被侵权所受到的实际损失”或者“侵权人因侵权所获得的利益”。

（七）对于权利人受到的实际损失和侵权人获得的利益，均需考虑随同销售。

第三十七条

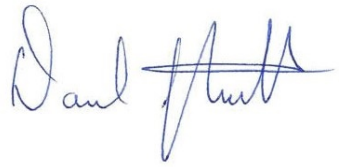
第三十七条第二款规定：“违反法律、法规，损害国家利益、社会公共利益，违背诚实信用原则的商业秘密，不在本规定保护范围。”

我们关切的是，该条款给予了相当大的灵活性，可以将商业秘密排除在《规定》的保护范围之外，我们希望能对其范围和适用性进行澄清。例如，我们希望得到这样的指导，即这一表述是否意味着某些商业秘密根本不适合保护，或者是否意在将读者指引向其他法律（例如，《反不正当竞争法》）以寻求保护。

我们感谢国家市场监督管理总局给予提交意见的机会，我们也非常愿意与国家市场监督管理总局进行进一步的交流或能有机会提供更多的信息。

随信附上本信的翻译版本。

此致



Daniel J. Staudt
美国知识产权所有人协会主席

附件：IP0 协会对《商业秘密保护规定（征求意见稿）》的反馈意见 （英文版）

18 October 2020

Price Supervision and Competition Bureau
State Administration of Market Supervision
No. 8 Sanlihe East Road
Xicheng District
Beijing, People's Republic of China
100820

Via Email: fbzdjzc@vip.126.com

Re: Rules on Trade Secret Protection (Draft for Solicitation of Comments)

Dear State Administration of Market Supervision:

The Intellectual Property Owners Association (IPO) appreciates the opportunity to respond to the request for comments on the draft entitled *Rules on Trade Secret Protection (Draft for Solicitation of Comments)* ("Draft Rules") published on 4 September 2020.

IPO is an international trade association representing companies and individuals in all industries and fields of technology who own, or are interested in, intellectual property rights. IPO's membership includes 175 companies and close to 12,000 individuals who are involved in the association either through their companies or as inventor, author, law firm, or attorney members. IPO membership spans over 30 countries.

IPO advocates for effective and affordable IP ownership rights and offers a wide array of services, including supporting member interests relating to legislative and international issues; analyzing current IP issues; providing information and educational services; and disseminating information to the public on the importance of IP rights.

IPO appreciates the objectives stated in the Draft Rules including to strengthen the protection of enterprise trade secrets and to stop unfair competition and infringement of trade secrets in connection with the *Anti-Unfair Competition Law* ("AUCL"). We note that Draft Rules appear to be a recognition of certain trade secret-related provisions of the recent Phase One Economic and Trade Agreement between the United States of America and the People's Republic of China ("Phase One Agreement"). IPO views this invitation for comments as an important and useful implementation of the two countries' agreement to strengthen their cooperation regarding trade secret protection, as memorialized in Article 1.4 of the Phase One Agreement. We hope that our comments will be helpful during the process of finalizing the Draft Rules, as well as informing future developments in trade secret protection.

General Comments

The Draft Rules contemplate an expansive role for administrative authorities in connection with trade secret enforcement. We appreciate that this may enhance the speed and efficiency in the resolution of trade secret infringement matters for the benefit of rights holders. However, we respectfully note that in promoting use of and confidence in the administrative agencies for trade secret dispute resolution, as compared with the people's courts, such promotion and confidence should require the same degree of uniformity, predictability, transparency, oversight, and procedural protections that are provided to the affected parties through judicial review.

Regarding transparency, for example, IPO welcomes the publication of administrative actions and decisions, and periodic reporting of enforcement statistics such as the number of cases initiated and concluded, identity of the parties involved, and outcome. Additional guidance on mechanisms and interplay between administrative and criminal enforcement of trade secret infringement will also be beneficial.

In regard to uniformity and predictability, we believe that the public will benefit from consistency in application of and interpretation under the AUCL between administrative procedures (e.g., as articulated in the Draft Rules) and the courts (such as stated in the Supreme People's Court's *Interpretations on Several Issues Concerning the Application of Law in the Trial of Civil Cases of Trade Secret Infringement Disputes*, published on 10 September 2020). To the extent there may be inconsistency in interpretation or application in administrative compared to judicial avenues, we welcome guidance at the national level such as in the form of proposed Regulations from the State Council.

Article 3

There are two aspects of Article 3 that are of concern to IPO. First, it seems that this article intends for the Draft Rules to apply only to trade secrets owned by Chinese entities and not foreign entities. This discrepancy is inapt for the Draft Rules which govern an issue of vast significance to foreign entities (as demonstrated by the provisions of the Phase One Trade Agreement that relate to trade secret protection) and is inconsistent with the AUCL (which has no such limitation).

Second, the term "providing assistance" is broad and could create liability for many innocent parties that are providers of goods and services. For example, USB sticks are often used in trade secret infringement activity – we do not think that the Draft Rules intend for USB stick manufacturers to be held liable for infringement activity conducted by others. The same concern applies to manufacturers of scanners and printers, and providers of cloud storage and email services. We respectfully suggest that there should be a "know or should have known" mental state requirement in order for there to be liability for the infringing acts of others. When an entity intentionally disregards clear evidence of infringement, it can be determined that such an entity "should have known" of the infringement. Thus, IPO proposes the following revision:

> ***Article 3 [Scope of Application]*** *This regulation shall apply to any natural person, legal person or unincorporated*

> *organization that infringes on the trade secrets of* ~~***China's***~~ *trade secret rights holders or provides assistance for the infringement of trade secrets* ***when they know or should have known of the infringement****.*

Article 5

Article 5 defines terms such as "technical information," "business information" and "trade secret(s)" under the Draft Rules. The word "plans" used to define the term "technical information" is misleading, with regard to the purpose, scope or completeness of such information. We recommend not using "plans" for this definition:

> *The term "technical information" used in the Rules refers to* ***information of a*** *technical* ~~***plans***~~ ***nature*** *obtained through utilizing knowledge of science and technology, information and experience. Technical information includes but is not limited to designs, programs, formulas,* ~~***product***~~ *ingredients,* ~~***production***~~ *processes,* ~~***production***~~ *methods, records of R&D,* ~~***lab***~~ *data,* ~~***technical***~~ *know-how,* ~~***technical***~~ *drawings, coding styles, source codes of computer software and relevant documents and other information.*

Article 6

Article 6 of the Draft Rules addresses the type of information that falls within and outside of being "unknown to the public," that is, information that is or is not secret. Under Article 6, information is considered to be unknown to the public if it is not generally known to relevant personnel in the field to which it belongs or cannot be easily obtained from public channels.

Crucial to this determination is how broadly the term "field" is to be construed. In clarifying this term, we respectfully suggest that Article 6 be amended based on Section 7, Article 39 of The Agreement on Trade-Related Aspects of Intellectual Property Rights (hereinafter referred to as "TRIPS") wherein information is considered secret when the information is not generally known among or readily accessible "to persons within the circles that normally deal with the kind of information in question." We also note that publicly available information, when taken in its entirety, may also fall within information that is "unknown to the public." More particularly, individual portions of a work may be well known but that should not preclude protection for a secret combination. One must look to the entire work (*e.g.*, a compilation) and not its individual parts in determining whether the information is unknown to the public. Examples of information, taken in its entirety, that may be unknown to the public include, but are not limited to, customer contact lists and customer lead data.

Article 6 also addresses five circumstances where information falls outside of "not known to the public." We recommend that circumstance (2) be amended, circumstance (4) be deleted, and circumstance (5) be amended.

More particularly, circumstance (2) covers information that has been "publicly used" at home and abroad. This circumstance is often challenging to detect and identify because publicly used information is often hidden within publicly used products. Circumstance (2)

also sets forth conditions that are beyond the trade secret requirements of TRIPS (*i.e.*, Section 7, Article 39). Under TRIPS, secrecy is not lost by information being publicly used. Rather, secrecy is lost when it is generally known or readily accessible. We therefore recommend that the circumstance (2) be amended to cover information that is generally known or readily accessible rather than to cover information that is publicly used.

Circumstance (4) covers information that is easily obtained without paying a certain price or can be obtained from other public channels. This circumstance is rather vague. Questions arise such as: At what price should information be viewed as no longer being "unknown to the public"? Should such "certain price" vary over time? When are circumstances no longer "easy" in obtaining the information at a certain price? In view of the difficulty in determining when the conditions of circumstance (4) are met, we respectfully submit that this circumstance be deleted.

Circumstance (5) is directed to only relevant content information such as product size, structure, simple combination of components, etc. that can be obtained by the relevant public through simple methods such as observation, surveying, and disassembly after entering the public domain. We recommend that this circumstance be broadened so as to capture any information that can be obtained by the relevant public through simple methods such as observation, surveying, and disassembly after entering the public domain.

Article 6 also allows for evidence to be presented in contesting the presumption that the information is not known to the public. We respectfully urge that in overcoming this presumption the evidence to be presented must be sufficiently clear to the contrary.

In view of the foregoing, we recommend that Article 6 be amended as follows:

> ***Article 6 [Unknown to the public]*** *The term "unknown to the public" mentioned in these regulations means that the information* ***, taken in its entirety,*** *is not generally known to* ***or otherwise not easy to obtain by*** *the relevant personnel* ***within the circles that normally deal with the kind of information in question*** *~~in the field to which it belongs or cannot be easily obtained from public channels~~. ~~Under~~* ***Including, but not limited to, any*** *one of the following circumstances, it can be determined that the relevant information does not constitute "not known to the public":*
>
> *(1) The information has been publicly disclosed in public publications or other* ***public*** *media at home and abroad or has been* ***publicly*** *disclosed through public reports, exhibitions, etc.;*
>
> *(2) The information has been ~~publicly used~~* ***generally known to or readily accessible*** *at home and abroad;*
>
> *(3) The information is common sense or industry practice generally mastered by relevant personnel in the field;*
>
> ***~~(4) The information is easily obtained without paying a certain price or can be obtained from other public channels;~~***
>
> ***~~(5)~~Only relevant content*** ***(4) The*** *information* ***~~such as product size, structure, simple combination of components, etc.~~*** *can be obtained by the relevant public through simple methods such as observation, surveying, and disassembly after entering the public domain.*

*If **information such as, but not limited to,** the technical novelty report, search report, public channel inquiring about commercial information, etc. submitted by the applicant does not constitute substantially the same information as the information involved, it can be presumed that the information is "not known to the public" unless there is evidence **that is sufficiently clear** to the contrary.*

Article 8

Article 8 lists eight types of "corresponding confidentiality measures" taken by the trade secret holder to prevent information leakage. We note that whether a trade secret holder's measures to maintain confidentiality are "reasonable" depends on consideration of the unique circumstances of the holder's business. Therefore, whether any one of the eight specified actions might be "sufficient" to prevent some leakage does not determine the answer to the larger question of whether the measures taken as a whole are reasonable. Instead of providing that the sufficiency of one of these actions may be determinative, we recommend that these eight are merely illustrative, non-limiting examples of actions that, considered in context, may support a conclusion that corresponding confidentiality measures are reasonable. In addition, whether a trade secret can be independently acquired or developed should not factor into whether the right holder has taken the appropriate confidentiality measures to protect its own trade secret. We therefore recommend the following revisions:

***Article 8 [Corresponding Confidentiality Measures]** The corresponding confidentiality measures taken by the right holder in these regulations refer to the measures taken by the right holder to prevent information leakage that are compatible with the commercial value of the trade secret**~~, the difficulty of independent acquisition,~~** and other factors that are reasonable and targeted confidentiality measures.*

***The ~~If one of the~~** following **non-limiting** circumstances **~~is sufficient to prevent the leakage of confidential information, it can be determined that~~ should be taken into account to determine whether** the right holder has taken "corresponding confidentiality measures":*

Article 10

Article 10 of the Draft Rules addresses the ownership rights of a trade secret researched or developed by a natural person for a legal person or unincorporated organization. In this regard, we respectfully suggest that Article 10 be amended to reflect that an agreement between the parties controls the ownership of the trade secret, whether or not the trade secret is within or outside of the actual or contemplated business of the legal person or unincorporated organization. It is also respectfully suggested that ownership of a trade secret be determined based on the actual or contemplated business of the legal person or unincorporated organization, rather than based on the task assigned to the natural person. In this way, it is far less likely that the natural person and the legal person or unincorporated organization will be placed into conflict with each other regarding the research or development work performed by the natural person. By adopting this approach,

conflicts as to whether a task is within or outside of the natural person's work assignment can be avoided.

Article 10 also addresses where a trade secret created by a natural person uses the material and technical conditions or experience of a legal person or unincorporated organization. Although the natural person will own the trade secret, it is respectfully submitted that the *quid pro quo* for use of a legal person's or unincorporated organization's resources is the right to use the trade secret within a legal person's or unincorporated organization's scope of business without remuneration to the natural person. That is, equity and fairness entitle the legal person or unincorporated organization to the use of the trade secret without further payment to the natural person.

In view of the foregoing, we recommend that Article 10 be amended as follows:

> ***Article 10 [Ownership of Rights]*** *Trade secrets researched or developed by natural persons* ***for and within the actual or contemplated business*** ~~***for the purpose of completing the tasks***~~ *of a legal person or unincorporated organization shall belong to the legal person or unincorporated organization, but if the parties have agreed otherwise, the agreement shall prevail.* ~~***Commercial***~~ ***Furthermore, unless the parties have agreed otherwise, trade*** *secrets researched or developed by a natural person outside of the* ~~***tasks***~~ ***actual or contemplated business*** *of a legal person or unincorporated organization shall belong to the natural person. However, if its trade secrets use the material and technical conditions or experience of a legal person or unincorporated organization, the legal person or unincorporated organization has the right to use the trade secret within its business scope* ~~***after paying reasonable remuneration***~~.

Article 11

Consistent with the principles of the AUCL, we recommend that an "infringer" also include those that allow or assist another to obtain, disclose, and/or use trade secrets in violation of the Draft Rules when they know or should have known of the violation, as shown below:

> ***Article 11 [Infringer]*** *The infringer mentioned in these regulations refers to natural persons, legal persons or unincorporated organizations that have obtained, disclosed,* ***and/or*** *used trade secrets in violation of these rules,* ***or allowed or assisted another to obtain, disclose, and/or use trade secrets when the natural persons, legal persons or unincorporated organizations know or should have known of the violation of these rules****.*

Article 12

Article 12 lists examples of what constitutes "illegal obtaining" of trade secrets. First, we respectfully request clarification as to what constitutes "designing traps" as contemplated in clause (2).

In addition, we propose adding "data scraping" to clause (3) pertaining to electronic information systems. Data scraping is a technique where a computer program extracts data from output coming from an on-line database, often in a manner not reasonably intended by the administrator of that targeted, on-line database. The operator of the on-line database will often see this data-scraping as an unwanted act, due to reasons such as pilfering of the protected content of the database ("illegal obtaining" of trade secrets), in addition to loss of control and increased system load which could deter intended users. For clarification, data scraping is distinguished from the more innocuous "parsing" where the output being "scraped" is only intended for display to an end-user, rather than as input to another program (in the case of data scraping). Thus, we proposed the following edit in clause 3:

> *(3) Entering the electronic information system of the right holder without authorization or beyond the scope of authorization* ***including, but not limited to, unauthorized data scraping,*** *to obtain trade secrets or planting computer viruses to destroy their trade secrets. Among them, the electronic information system refers to all electronic carriers that store the right holder's trade secrets, including digitalization Office systems, servers, mailboxes, cloud disks, application accounts, etc.*

We further suggest the below additional clause 6, which pertains to the unauthorized retention of trade secret materials of an employer after termination:

> ***(6) Retaining, without permission, the trade secret materials of an employer after termination of employment.***

Article 13

Similar to the principle discussed in reference to Article 3, we are concerned about creating liability for providing goods and services that are used for trade secret infringement where the provider (*e.g.*, a camera manufacturer) does not know and has no reason to know of the infringement. We therefore propose a "know or should have known" mental state requirement for liability.

In addition, whether an act constitutes "disclosure" should not depend on whether it is "sufficient to undermine the right holder's competitive advantage or harm its economic interests" as required in the second paragraph of Article 13. Assessment of competitive advantage and economic interest is more appropriately directed to determination of a "trade secret" and/or the extent of loss, not whether a trade secret is improperly "disclosed."

The third paragraph of Article 13 defines "use" as the application of the trade secret information to product design, manufacturing, marketing and improvement, research and analysis. This formulation of "use" seems too narrow, and should instead be defined as any application of the trade secret information that harms the holder or benefits the infringer. This includes for example to inform, assist, or accelerate the development or provision of a product or service. We therefore propose the following revisions:

> ***Article 13 [Disclosure, Use]*** *Operator shall not disclose, use or allow others to use the trade secrets of the right holder obtained by improper*

means ***when the operator knows or should have known that the trade secrets were obtained by improper means****.*

*The "disclosure" mentioned in this article refers to the act of disclosing the right holder's business secrets****, which is sufficient to undermine the right holder's competitive advantage or harm its economic interests****.*

The "use" mentioned in this article refers to ***the*** ***any*** *application of the right holder's trade secrets* ***that harms the right holder or benefits the infringer, including without limitation*** *to* ***inform, assist, or accelerate the development or provision of*** *product design, product manufacturing, marketing and improvement, research and analysis, etc.*

Article 14

As mentioned in reference to Articles 3 and 13, we are concerned about creating liability for providing goods and services that are used for trade secret infringement where the provider (*e.g.*, email software providers) does not know and has no reason to know of the infringement. We therefore propose a "know or should have known" mental state requirement for liability, as shown below:

Article 14 [Confidentiality Obligation and Obligee's Requirements for Keeping Trade Secrets] *Operators may not violate the confidentiality obligation or the obligee's requirements for keeping business secrets by disclosing, using or allowing others to use the business secrets they have* ***when the operator knows or should have known that it would constitute a violation of the confidentiality obligations****.*

Article 15

Article 15, paragraph 2, states, "[s]elf-knowledge, experience and skills of an employee or a former employee formed in the process of work are excluded." This is problematic as it could be interpreted as giving an employee with a good memory the right to use trade secrets and reveal them to third parties. We recommend deleting this statement. We also suggest revising the article to make clear it applies to the restrictions agreed to by the parties regardless of the type of agreement:

The term "restricted use of a trade secret" used in this Article includes but is not limited to the legal ***restrictions,*** *or* ***agreed*** *restrictions* ***as agreed between the parties,*** *on the use of a trade secret****, concluded with a right holder in a non-disclosure agreement, labor contract, cooperation agreement and other contracts. Self-knowledge, experience and skills of an employee or a former employee formed in the process of work are excluded.***

Article 16

As with Articles 3, 13 and 14, we propose a "know or should have known" mental state requirement for liability, as shown in the proposed revision to this article below:

> ***Article 16 [Instigate, induce, or assist in the infringement of trade secrets]*** *Operators shall not instigate, induce, or assist others in breaching confidentiality obligations or violating the right holder's requirements for keeping business secrets, obtaining, disclosing, using or allowing others to use the right holder's business secret****, when the operator knows or should have known that it would constitute a breach of confidentiality or violation of the right holder's requirements.***

Article 18

Article 18 relates to protection of certain customer lists. The description of customer lists under this article is very specific, and we believe it is too narrow to provide adequate protection of customer lists that would otherwise be protectable under the AUCL. Thus, we recommend a clarification that the description in Article 18 is illustrative only, and does not preclude other types of customer lists that should be protected as trade secrets.

We also note that Article 18 provides an exception to "improper means" where a client "voluntarily" chooses to conduct transactions with a former employee. We are concerned that in situations where a former employee uses the customer lists of the employer to solicit and transact with the employer's client, a client who agrees to the transaction will most likely claim that the transaction is done "voluntarily." Rather than looking at the willingness of a client, the determinative factor as to whether "improper means" is used should be whether the former employee has solicited the client or used the right holder's confidential information in the process. We therefore propose the following revisions:

> ***Article 18 [Customer List]*** *After paying commercial costs, where the right holder has formed a relatively fixed customer list with unique transaction habits and other content within a certain period of time, it can be protected as trade secret protection.* ***Other types of customer lists not specified in this article may also qualify as trade secrets pursuant to the Anti-Unfair Competition Law.***
>
> *The customer list mentioned in the preceding paragraph generally refers to the customer's name, address, contact information, and transaction habits, intentions, content and other special customer information that is different from the relevant publicly known information, including the customer list of many customers, and maintenance, specific customers with long-term stable trading relationships. If a client conducts market transactions with the employee's unit based on the individual's trust in the employee, and after the employee resigns, it can prove that the client****, ~~voluntarily~~ without solicitation or use of the right holder's confidential information by the employee,*** *chooses to conduct market transactions*

with him or his new unit, it shall be determined that no improper means have been used.

Article 19

Article 19 addresses exceptions to infringement of trade secrets. Exception (1) would provide more consistent and predictable results by adding a requirement for written records generated at the time the discovery was made or research and development was conducted. Exception (4) addresses two different situations: public policy exceptions and whistle-blower protections. We recommend that exception (4) could be more easily understood by separating it into two sections as shown in the proposal below. As shown below, the revised exception (4) directed to public interest or national interest focuses on environmental, health and safety concerns, and the new exception (5) sets out the guidelines for reporting wrongdoing to the government authorities (whistleblower exception).

With regard to "reverse engineering," it is not clear whether "*the act of the personnel who have access to or known about the technical secret of a right holder or holder, obtaining the technical secret of a right holder through their memories and dismantling of the end product*" is an exception of "reverse engineering" or has already been covered by exception (2) (either as "through improper means" or "violates confidentiality obligations"). Similar to Article 15, the clarity around residuals or memories is important to evaluate employee behaviors. We recommend deleting this, then adding "contractual obligation" into exception (2) for clarity.

Further, while IPO recognizes the merits of whistleblower protection, it does not seem like an appropriate requirement in administrative rules such as these Draft Rules.

Article 19 [Exceptions for Infringements of Trade Secrets] *The following acts are not infringements of commercial secrets:*

(1) Independent discovery or independent research and development ***as demonstrated by contemporaneous written records thereof****;*

(2) Where trade secrets are obtained through reverse engineering or similar methods, except that trade secrets or products are obtained through improper means, or reverse engineering that violates confidentiality ***or contractual*** *obligations;*

(3) Shareholders obtain company trade secrets by exercising their right to know according to law ***provided company trade secrets are not further shared or used for gain****;*

(4) ~~***The employees, former employees or partners of the owners or holders of trade secrets must disclose***~~ ***Where*** *trade secrets* ***are required by law to be disclosed, provided that such disclosure is limited to information that is needed to serve*** ~~***based on***~~ *the needs of public interest or national interest* ~~***such as***~~ ***regarding*** *environmental protection, public health*~~***,***~~ ***and*** *public safety****, with the right holder having an opportunity to contest the grounds for such disclosure, if appropriate, to the relevant authorities; and*~~***disclosure of illegal and criminal activities***~~*.*

(5) Where the trade secrets are disclosed in confidence to the authorities by employees, former employees or partners of the owners or holders of trade secrets for purposes of reporting illegal and/or criminal activities.

*The term "reverse engineering" used in the preceding paragraph, refers to the act of using technical means to acquire relevant technical information of a product, method or process obtained from public channels through dismantling, mapping, analyzing, etc.**, ~~but the act of the personnel who have access to or known about the technical secret of a right holder or holder, obtaining the technical secret of a right holder through their memories and dismantling of the end product, does not constitute reverse engineering~~***.

The disclosing party shall, when reporting the afore-mentioned illegal and criminal acts to the relevant state administrative organs, judicial organs and their functionaries, submit documents or legal documents containing trade secrets in a confidential manner.

~~A right owner or right holder of a trade secret shall provide clauses on immunity granted to whistle-blowers and anti-retaliation in any contract or agreement signed with an employee, partner or consultant to manage and control the use of a trade secret or other confidential information. The form of a contract or agreement includes, but is not limited to, a labor contract, an independent contractor agreement, a consulting agreement, a separation and claim termination agreement, a severance agreement, a non-compete agreement, a confidentiality and ownership agreement, an employee handbook, etc.~~

Article 20

Article 20 grants authority to a county-level department to investigate and determine trade secret violations. Article 19 grants the enforcement authorities significant discretion to exclude certain trade secrets from protection. Similarly, Article 31 grants those authorities discretion to identify certain trade secret violations as serious, potentially triggering fines and other remedies. IPO believes that, under these circumstances, giving these responsibilities to departments with a broader geographic scope would be preferable for more consistent and predictable enforcement. We therefore propose that investigations and determinations of violations be elevated to the provincial level:

Article 20 [Law Enforcement Organs] *Violations of trade secrets shall be determined and investigated by the market supervision and management department at or above the* ***~~county~~ provincial*** *level.*

Article 22

Article 22 relates to the use of appraisals in a trade secret determination. The third-party entities referred to in this article, *i.e.*, appraisal agencies and persons with specialized knowledge, should be required to be independent from the parties in order to ensure their credibility. Moreover, those entities should be required to protect the information they

receive as confidential, in order to preserve the confidential status of the information at issue. IPO therefore proposes revising this article as shown below:

> ***Article 22 [Entrusted Appraisal]*** *Rights holders and suspected infringers may entrust a legally qualified* ***and independent*** *appraisal agency to check whether the right holder's information is known to the public, whether the information used by the suspected infringer is substantially the same as the right holder's information, etc. Specialized matters are identified.* ***The appraisal agency shall be required to keep the information they receive confidential.***
>
> *Rights holders and suspected infringers may entrust* ***independent*** *persons with specialized knowledge to comment on specialized matters such as whether the right holder's information is known to the public.* ***The person with specialized knowledge shall be required to keep the information they receive confidential.***

Article 23

Article 23 relates to determination of trade secret infringement involving computer software programs. It should be made clear that an infringer cannot avoid infringement liability simply because the software code (including source codes) at issue is not identical to the trade secret at issue. Thus, we propose that a "same or substantially similar" standard be applied, as shown below:

> ***Article 23 [Determination of Evidence Involving Computer Software Programs]*** *Where a trade secret infringement involves a computer software program, to determine whether the two are substantially the same, the determination can be whether the software document****, source codes or*** *target program of the trade secret are the same as* ***or substantially similar to*** *the software involved in the alleged infringement, whether the computer software* ***source codes or*** *target program involved in the act contains specific computer software content claimed by the right holder as a trade secret* ***(including configuration parameters, database structure, etc.)****, or whether the software results (including software interface, operating parameters, ~~database structure~~, etc.) are the same as* ***or substantially similar to*** *the trade secret, etc.*

Article 25

Article 25 authorizes the seizure of relevant computer servers, mainframes, hard disks and other storage devices when the trade secret infringement involves computer technology. Inasmuch as seizure should be granted only in extraordinary circumstances, it is respectfully submitted that such seizure be available only when the evidence clearly shows, in addition to the usual irreparable harm and balance of equities, that the suspected infringer (1) will not comply with any alternative form of order, (2) actually has possession of the specific property containing the trade secret, (3) either misappropriated the trade secret or conspired with someone else to do so (this excludes innocent third parties such as

cloud providers or internet service providers); and (4) will destroy, move, hide, or otherwise make the secret inaccessible if given notice.

We also suggest that additional safeguards be put in place as follows: (1) providing findings and conclusions justifying the seizure; (2) limiting to the narrowest seizure of property necessary; (3) prohibiting access by the right holder or copying of the information; (4) specifying the seizure conditions for law enforcement; (5) setting a hearing within a very short time frame (for example, seven days); and (6) requiring a bond be posted by the right holder. Furthermore, we recommend that all seized materials be deposited with the market and supervision department and maintained in confidence until after the noticed hearing. Preferably, a person within the market supervision and management department should be appointed to separate trade secret information from other property and to facilitate the return of the latter to the suspected infringer. In view of the foregoing, we respectfully recommend that the following be added to the end of Article 25:

> ***Notwithstanding the foregoing, such seizure is granted only in extraordinary circumstances and is available only when the evidence clearly shows, in addition to the usual irreparable harm and balance of equities, that the suspected infringer (1) would evade, avoid, or otherwise not comply with any alternative form of order; (2) has actual possession of specific property containing a trade secret; (3) either misappropriated it or conspired with someone else to do so (this excludes innocent third parties such as cloud providers or internet service providers); and (4) would destroy, move, hide, or otherwise make the secret inaccessible if given notice.***
>
> ***A seizure order must (1) include findings and conclusions; (2) provide for the narrowest seizure of property necessary; (3) prohibit access by the right holder or copying of the information; (4) specify the seizure conditions for law enforcement; (5) set a hearing within a very short time frame; and (6) require a bond be posted by the right holder. All seized materials must be deposited with the market and supervision department and maintained in confidence until after the noticed hearing. A person within the market supervision and management department may be appointed to separate trade secret information from other property and to facilitate the return of the latter to the suspected infringer.***

Article 31

Article 31 addresses what constitutes "circumstances are serious" under Article 21 of the AUCL. In regard to assessing the financial impact of trade secret infringement, we note that Article 31 sets a 500,000 RMB threshold based on the loss of the right holder, or the profits gained by the infringer. According to the Supreme People's Court and Supreme People's Procuratorate latest interpretation on *Several Issues Concerning the Specific Application of Law in Handling of Criminal Cases of Intellectual Property Infringement (III)* (Fa Shi [2020] No. 10 effective on 14 September 2020), the threshold for trade secret criminal liability has been lowered to 300,000 RMB.

IPO recommends that the total sum of: the loss by the right holder, illegal gain by the infringer, and reasonable royalty, be counted towards the 300,000 RMB threshold, provided the combined losses are not duplicative for the same harm.

IPO recommends that three generally available methods be utilized in assessing total loss due to trade secret infringement for purposes of determining whether "circumstances are serious": (1) actual loss (e.g., lost profits, price or market erosion); (2) illegal gains (unjust enrichment), which include illegal income, unfair benefits to the infringer such as, but not limited to, acceleration of development time and avoided development costs; and (3) reasonable royalty. Each of these methods may be used in combination with others, provided the combined losses are not duplicative for the same harm. Where the total amount exceeds the threshold of 300,000 RMB, then the "circumstances are serious" is met under Article 21 of the AUCL.

We propose a specific reference to the notion of acceleration of development that allows early entry into a market (which deprives the trade secret owner of its full "head start" advantage). Moreover, we recommend that other possible aspects of infringement, such as convoyed sales, be considered in determining illegal gain to the infringer and/or loss to the trade secret owner. This is because, in a trade secret infringement case, a defendant may unfairly benefit not only from sales associated with a product protected by the trade secret, but also from sales of complementary or ancillary products sold together with the product protected by the trade secret. Likewise, the trade secret owner's losses may not be limited to the product protected by the trade secret, but also arise from convoyed products.

Turning to circumstance (3) ("Causes the obligee to go bankrupt"), we note that many unrelated business factors can be a partial or complete cause of bankruptcy of a business. We are concerned that, where there is an accusation of trade secret infringement leading to bankruptcy, it will be very difficult for the defendant, without discovery from the accuser, to prove that the cause of the bankruptcy was for unrelated reasons. We also believe that the combination of loss to the owner, illegal gains to the infringer, and reasonable royalty (without duplicative damages) constitutes more appropriate criteria. Thus, we recommend deleting the circumstance (3) of "causes the obligee to go bankrupt" as a stand-alone cause for "circumstances are serious" under the AUCL.

Regarding circumstance (6) ("Causing major economic losses to the country or society, or having a bad social impact"), and (7) ("Other serious acts"), we recognize that these are intended to be catch-call provisions for other serious acts not enumerated in Article 31. However, because these references are vague and potentially very broad, we welcome further clarification on their scope and applicability.

> ***Article 31 [Serious Circumstances]*** *If one of the following circumstances is met, it can be determined that the circumstances mentioned in Article 21 of the Anti-Unfair Competition Law are serious:*
>
> *(1) The* ***combined loss by the*** *right holder* ***(including convoyed sales), illegal gain by the infringer (including acceleration of development and convoyed sales), and reasonable royalty is*** ~~*loses*~~ *more than* ~~***500,000***~~ ***300,000*** *yuan due to infringement of trade secrets****, provided that the combined amount is not duplicative in damages for the same harm****;*

~~(2) Profits exceeding 500,000 yuan due to infringement of trade secrets ;~~

~~(3) Causes the obligee to go bankrupt ;~~

(4) Refusing to compensate the right holder for the losses;

(5) The electronic intrusion method causes serious damage to the right holder's office system network and computer data;

(6) Causing major economic losses to the country or society, or having a bad social impact;

(7) Other serious acts.

Article 33

Article 33 addresses the "legitimate source" defense against a trade secret claim. However, the evidence to support such defense shall be connected with the reasonable duty of care in accordance with the manufacturing and operation scale and practices. The "reasonable consideration" for a trade secret use is also extremely hard to evaluate, given the difficulty to evaluate the value of the trade secret. In view of the foregoing, we respectfully recommend the following changes to Article 33:

Article 33 [Misappropriation Out of Goodwill] *When an infringer uses a trade secret for the purpose of manufacturing and operation, without knowing that this use of the trade secret has not gained the approval from the right holder of the trade secret, where this infringer can provide evidence of the legitimate sources of this trade secret* ***in accordance with the reasonable duty of care****, this infringer shall be ordered to stop the aforementioned acts****~~, unless the user of the trade secret can prove that he or she has paid reasonable consideration~~****.*

Article 34

Article 34 addresses calculation of illegal income from trade secret infringement. The second paragraph of this article references the types of evidence that may be considered to calculate illegal gains. As mentioned earlier, illegal income by the infringer should also include acceleration of development and convoyed sales. In addition, where the right holder provides evidence relevant to the inquiry, such evidence should also be taken into consideration. Therefore, we recommend the following revisions:

Article 34 [Calculation of Illegal Income] *The "Illegal Income" mentioned in Article 21 of the Anti-Unfair Competition Law refers to the total income obtained by the infringer's illegal production, sale of goods or services* ***(including convoyed sales)*** *after deduction of appropriate and reasonable expenditures for business activities from the infringer's direct income****, and gains due to acceleration of development****.*

The market supervision and management department may comprehensively refer to the accounting books, production records, sales records, and transfer agreements of the trade secret infringer ***and***

<u>other evidence provided by the right holder</u> *to calculate the amount of illegal gains.*

We also recommend providing examples of other evidence (*e.g.*, submitted by the rights owner) from which to determine the amount of loss. Specifically, such examples may include information such as:

- Public statements of the infringer about sales or commercial activity
- Pricing of the infringer's products in stores or other venues
- Market surveys
- Statements in regulatory submissions to government agencies
- Information made public through Initial Public Offerings (IPOs)
- Receipts from customers
- Retail sales information from third parties and
- Other such information probative of the size and scope of the infringing activity.

<u>Article 35</u>

Article 35 addresses several methods for calculating a right holder's damages. In the event that it is difficult to determine either the number of the right holder's reduced sales caused by the infringement (as set forth under the first calculation method) or the suspected infringer's reasonable profit of each infringing product sold (as set forth in the second calculation method), it is respectfully suggested that an additional method be employed. Under this additional method, damages would be determined based on the product of the total number of infringing products sold multiplied by the right holder's reasonable profit associated with each infringing product.

Regarding the method covering the price at which the trade secret is permitted to be used by others, we suggest clarifying that the price is set by the right holder.

As previously mentioned, we also recommend that convoyed sales be included in the damage calculations, that is, in determining the actual loss suffered by the right holder and the benefits gained by the infringer. More particularly, a trade secret owner's losses may not be limited to the product protected by the trade secret, but also arise from convoyed sales (*i.e.*, sales of complementary or ancillary products that would be sold together with the product protected by the trade secret). Similarly, the infringer may be unfairly benefitting from both sales of the infringing product and associated convoyed products.

In view of the foregoing, we respectfully recommend the following amendments to Article 35:

Article 35 [Calculation of damage to the right holder] *If the market supervision and management department investigates the infringement of trade secrets and causes the damage to the right holder, it shall be determined according to the actual loss suffered by the right holder; if the actual loss is difficult to calculate, it shall be determined according the benefits obtained by the infringer. When calculating "the actual loss*

suffered by the right holder due to the infringement" and the "benefits gained by the infringer due to the infringement", the following calculation methods can be referred to:

(1) The product of the total number of sales reductions caused by infringement of the right holder's products multiplied by the reasonable profit of each product;

(2) Where it is difficult to determine the total number of sales reductions by the right holder, the product of the total number of infringing products sold on the market multiplied by the reasonable profit of each product of the suspected infringer;

(3) Where it is difficult to determine either (1) or (2), the product of the total number of infringing products sold on the market multiplied by the reasonable profit relating to the trade secret by the right holder of each infringing product;

(4) According to the expected profit that the right holder can obtain under normal circumstances, minus the difference of the profit from the product that uses the same information after being infringed;

(5) The price ***set by the right holder*** *at which the trade secret* ***is permitted*** *to be used by third parties ~~permits others to use~~;*

(6) Determine the value of trade secrets based on factors such as trade secret research and development costs, implementation benefits, available benefits, and time to maintain a competitive advantage, and use a certain percentage of the value to determine "the actual "Loss" or "Benefits gained by the infringer from the infringement"

(7) Taking into account convoyed sales for both actual losses suffered by the right holder and benefits gained by the infringer.

Article 37

Article 37 states in the second paragraph that "[t]rade secrets that violate laws and regulations, harm national interests, social public interests, and violate the principle of good faith, are not covered by these rules."

We are concerned that this provision allows considerable flexibility to exclude trade secrets from protection under the Draft Rules, and we seek clarification as to its scope and application. For example, we would appreciate guidance as to whether this language means that certain trade secrets are not suitable for protection at all or whether it intends to refer the reader to other laws, such as the AUCL, for protection.

We thank the State Administration of Market Supervision for this opportunity to comment, and we welcome further dialogue and opportunity to provide additional comments.

We have enclosed this letter as translated herewith.

Sincerely,

Daniel J. Staudt
President

Attachment