中国国际金融股份有限公司关于上海证券交易所

对青岛天华院化学工程股份有限公司问询函的回复

上海证券交易所：

青岛天华院化学工程股份有限公司（以下简称“天华院”、“上市公司”）于 2018 年 12 月 24 日收到上海证券交易所《关于对青岛天华院化学工程股份有限公司有关重大资产重组标的资产网络受攻击事项的问询函》（上证公函【2018】2752 号），中国国际金融股份有限公司（以下简称“中金公司”、“独立财务顾问”）对问询函的相关事项回复如下：

1、KM 集团收到 IT 系统受到网络攻击的具体时间，上市公司获悉上述事项的具体时间，并结合上述情况，说明公司信息披露是否存在延迟。

回复：

经 KM 集团管理团队确认，2018 年 11 月 13 日 KM 集团遭到首次黑客入侵，随后恶意软件在系统内潜伏并扩散，2018 年 11 月 21 日入侵的恶意软件对 KM 集团 IT 系统内的文件进行加密，从而确认受到了网络攻击。网络攻击得到确认之后，KM 集团立即开展紧急应对工作，采取了一系列措施阻止情况进一步恶化。由于网络攻击具有较强的专业性和隐蔽性，同时，KM 集团全球化的生产经营管理信息化程度较高、IT 系统较为复杂，需要一定时间确认网络攻击的来源、机制和具体影响，并在上述工作的基础上制定应对方案。

2018 年 12 月 12 日，KM 集团管理团队告知上市公司及独立财务顾问关于网络攻击的具体过程及 KM 集团 2018 年 11 月经营业绩概算。根据重大资产重组实施过程中发生重大事项的信息披露要求，为保证披露信息的真实、准确、完整，独立财务顾问和德勤会计师协助上市公司就 KM 网络攻击事件的过程和可能产生的损失向 KM 集团管理团队进行进一步核实论证。

经上述核实论证，上市公司在 2018 年 12 月 21 日收到相关反馈后，于当日

发布了《青岛天华院化学工程股份有限公司关于 KM 集团网络攻击事件的公告》（公告编号：2018-071），及时履行信息披露义务。

综上所述，独立财务顾问认为，KM 集团于 2018 年 11 月 21 日确认受到网络攻击，在确认相关影响后于 2018 年 12 月 12 日告知上市公司及独立财务顾问。上市公司及相关中介机构根据《上市公司重大资产重组管理办法》关于重大资产重组实施过程中发生重大事项的有关规定，为保证披露信息的真实、准确、完整，对本次网络攻击事件履行相关尽职调查，包括要求标的公司提供网络攻击证据、与标的公司 IT 人员进行访谈、与会计师进行交流等，从而确定该事项的具体影响及性质。2018 年 12 月 21 日，上市公司获得相关信息的核实确认并于当日就本次网络攻击事件发布了公告，符合信息披露及时性的要求。

2.公司于 2018 年 12 月 4 日获得证监会对本次重大资产重组事项的核准。请公司说明是否在 IT 系统受到攻击后及时报告证监会，若无，请说明原因。

回复：

在 2018 年 12 月 12 日，KM 集团管理团队就 KM 集团 2018 年 11 月管理层报表以及关于网络攻击情况的具体影响告知上市公司及独立财务顾问之后，为保证获取信息的真实、准确、完整，上市公司、独立财务顾问及德勤按照重大资产重组实施过程中发生重大事项的有关规定就该事项向 KM 集团管理团队进行了核实论证。2018 年 12 月 21 日，上市公司获得相关信息的核实确认并于当日就本次网络攻击事件向证监会及其派出机构、交易所进行了报告，同时发布了公告。

独立财务顾问认为，上市公司于 2018 年 12 月 21 日网络攻击的具体事项得到确认后及时向证监会及其派出机构、交易所进行了报告，同时发布了公告，及时履行了《上市公司重大资产重组管理办法》规定的相关信息披露义务和证监会下发的《关于核准青岛天华院化学工程股份有限公司向 CNCE Global Holdings (Hong Kong) Co., Limited 等发行股份购买资产并募集配套资金的批复》（证监许可[2018]1980 号）第七款规定的报告义务。

3.请结合 KM 集团 IT 系统本次和历史上受到攻击的情况以及对生产经营的影响，说明 KM 集团 IT 系统的稳定性及潜在风险。此外，说明是否就此事项在重组报告书中进行了充分的风险提示。

回复：

经 KM 集团管理团队确认，本次网络攻击总计入侵了 349 个基于 windows 系统的 IT 管理系统，同时，备份服务器也遭到清除。本次网络攻击导致 KM 集团子公司 KMT 慕尼黑工厂及其他五个相关生产组装点的工程加工、组装交付能力受到一定影响。产生影响的因素包括：①注塑设备板块的配件备件加工环节部分重要数据被加密；②由于服务器系统关闭，组件生产环节无法及时完成新订单信息和生产参数信息的下载，进而影响调试安装进度；③在调试安装环节，无法安装设备操作软件，进而影响产品交付进度。

网络攻击事件发生后，KM 集团迅速做出反应，主要采取了包括切断恶意程序传播路径、清除 KM 集团 IT 系统中可能留存的其他木马工具或休眠工具、聘请专业 IT 安全顾问等应对措施。针对网络攻击事件 KM 集团正在积极采取措施恢复生产并提升生产经营系统安全性，核心系统预计将会在 2019 年 1 月初全部恢复，其余系统在 2019 年 1 月至 2 月全部恢复完成。KM 集团 IT 团队和安全顾问公司就被加密的数据进行恢复，同时采取措施提升备份数据服务器的安全性。伴随 IT 相关生产管理系统和数据的逐步恢复，KM 集团将采取积极有效的措施增加生产班次进行生产，加快组装调试和产品交付。

经 KM 集团管理团队确认，在其 180 年的经营历史中，未曾发生对生产经营产生显著影响的 IT 安全事件。KM 集团是一个跨国公司，每年在 IT 项目上的投入约 1,500 万欧元，其 IT 基础设施拥有最新的技术进行病毒和恶意软件检测清除，具备较强的稳定性。

由于 KM 集团经营历史较长，此前从未发生过类似网络攻击事件，同时，KM 集团非互联网等 IT 类企业，其经营风险主要集中于生产、销售、外汇等环节。基于 KM 集团的业务性质及历史上从未发生过类似 IT 安全事件的事实，结合重要性程度未在本次重大资产重组的《重组报告书》中就网络安全威胁的风险做出专项风险提示。

综上所述，独立财务顾问认为，KM 集团经营历史较长，未曾发生类似网络攻击事件。KM 集团作为跨国经营的先进制造企业，拥有、维持并运营符合其业务经营需要的 IT 基础设施，包括 IT 安全保护系统，具备较强的稳定性。本次专业、有组织的网络攻击行为具备一定特殊性和偶然性，并不必然表示其 IT 系统存在显著的潜在风险。基于 KM 集团的业务性质及历史上从未发生过类似 IT 安全事件的事实，结合重要性程度未在本次重大资产重组的《重组报告书》中就网络安全威胁的风险做出专项风险提示。

（以下无正文）

（此页无正文，为《中国国际金融股份有限公司关于上海证券交易所对青岛天华院化学工程股份有限公司问询函的回复》之签章页）

中国国际金融股份有限公司

2018 年 12 月 27 日