漢坤律師事務所

汉坤法律评述

融贯中西 · 务实创新

2018 年 3 月 20 日

争议解决

跨境电邮诈骗及资产追回策略简介

廖荣华 | 廖海清

伴随着电子邮件在商务往来中的广泛应用，网络黑客入侵电子邮件系统实施诈骗的案件日益增多。此类案件在跨境交易中尤为突出，因跨境交易中时差、语言等因素导致各方高度依赖电子邮件通信往来，包括交易款项支付安排，这给网络黑客以可乘之机。最常见的诈骗方式表现为网络黑客使用与外贸企业或公司高管完全相同或相似的电子邮件发出付款指令，此类案件也因此被称为外贸诈骗或 CEO 诈骗。待骗局被觉察后，因资金经转不同国家的银行且网络黑客通常使用空壳公司开立银行账户来接收资金，司法机关或金融机构难以迅速认定诈骗行为并拦截或冻结被骗资金，受害者在此情形下经常是束手无策。

汉坤争议解决团队近几年内代表多家跨国公司处理有关电邮诈骗和资产追回的案件，积累了丰富的实务经验。本文旨在概要介绍电邮诈骗的常见类型和手段、受害者主要的救济途径及相关法律和实务操作问题。由于个案特殊性会影响到具体策略的选择，资产的顺利追回离不开熟悉当地司法流程的律师团队的及时介入和高效处理。

一、 电邮诈骗

1. 电邮诈骗的常见类型

类型	常见骗局	后知后觉
外贸诈骗	外贸企业 A 与境外客户 B 洽谈一桩货物买卖已久，在双方即将达成交易时，网络黑客“变身”外贸企业 A 向境外客户 B 发送电子邮件： 1) “货物已出境，但我司原银行账户正在接受审计不方便接收新款项，请将款项付至我司如下香港子公司账户……”； 2) “本公司正与原收款账号开户行协商解决纳税问题，请将本款项付至我司关联公司账户……”。	外贸企业 A 迟迟未收到货款，再行发送邮件或决定电话联系境外客户 B，双方惊讶发现款项已经错误汇出。
CEO 诈骗	网络黑客“变身”公司高管 A 向财务人员 B 发送标题为“紧急且保密的并购”的电子邮件：“我正在中国出差进行一个高度保密的并购项目，请立即将前期律师费/咨询费付至如下中国公司账户，请勿与第三人交流本邮件内容及款项支付目的。”	高管 A 出现在财务人员 B 面前或财务人员 B 向高管 A 补办付款审批手续时，惊觉诈骗行为。

2. 电邮诈骗的常见步骤

1) 确认目标

网络黑客通过公司网站、外贸论坛等平台搜集外贸企业或跨国公司的联系邮箱，通常安全等级低的企业免费邮箱或不以公司名为后缀的私人邮箱会被锁定为目标邮箱。网络黑客随即通过技术手段入侵目标邮箱并截获双方邮件往来内容或窃取目标邮箱密码后直接登录邮箱掌握双方交易动向。

2) 暗中观察

网络黑客潜入目标邮箱后并不急于采取行动，而是阅览所有与交易相关的邮件，熟悉公司内部组织架构和财务流程、高管行程、交易进展等信息，甚至会刻意模仿双方电邮行文特点，为在付款关键环节的仿冒行动做好准备。

3) 仿造邮件

在要付款的关键环节，网络黑客采用技术手段切断双方的邮件往来，并仿造外贸企业邮件要求变更汇款账户，或者仿冒公司高管邮件向财务人员发出汇款指示。

网络黑客直接登录并用目标邮箱发送诈骗邮件较为少见，更多的是采用与真实邮箱高度相似的仿冒邮箱发送诈骗邮件。为了降低相对方对仿冒邮箱的警觉，网络黑客通常在发出变更付款账号的邮件之前便不时使用仿冒邮箱与相对方进行正常沟通往来，比如交换单据、询问交易进展等。常见仿冒手段举例如下：

仿冒手段	真实邮箱	仿冒邮箱
字形混淆型	apple@qq.com	app1e@qq.com
字符增减型	sasaki@sahathai.com	sasaki@sahatthai.com
替换后缀型	vicky@yahoo.com	vicky@ymail.com

4) 洗白款项

最初网络黑客得手之后通常立即提现或多次转汇后提现，但提现存在容易暴露行迹的问题，目前常见销赃手段已升级为通过二次交易洗白赃款。详言之，网络黑客在向境外客户发出变更账号的仿冒邮件之前，会另外以采购商身份与其他外贸公司洽谈货物采购并要求该外贸公司提供收款账号，告知其收到款项后安排货物出境，而该收款账号便成为网络黑客仿冒邮件中要求境外客户变更支付的账号。如此一来，网络黑客不用现身便既能收货转卖，又洗白了诈骗款项，增加了案件破获和资金追回的难度。

二、 资产追回的策略和途径

当意识到遭遇电邮诈骗后，受害者应立即第一时间联系开户行和警方，促使银行尽快冻结资金或提供资金进出明细。对于境外付款方而言，应立即联系汇款行及时阻止汇款，即便汇款已经执行，通常汇款行较之境外付款方更容易与收款行取得联系，尤其是两家银行之间存在反洗钱等方面合作时，收款行通常会更愿意配合限制或延缓资金转移。

我们注意到，当境外受害者直接向中国当地警方报案时，警方常以管辖问题或报案材料不完备等理由不予立案，并建议受害者向其所在地警方报案或通过国际刑警合作机制维权，从而延误挽回损失的最佳时机。而境内收款行在此类案件中经常处于两难境地，一方面对受害者的遭遇表示同情，另一

方面因受限于对客户信息的保密义务且案情并未明朗，因而经常以尚未收到司法机关的指令为由，表示无权对涉嫌账户采取措施。此时，受害者聘请当地律师及时准备报案材料、整理证据和安排翻译、从立案管辖和银行业相关监管规定向警方和银行提供说明性文件则对案件受理和资金冻结至关重要。

一旦资金被成功冻结之后，则为下一步的资产追回赢得了较为充裕的时间，受害者可以考虑如下步骤进一步追回资产：

1. 当地刑事侦查起诉或国际警务合作

在资金被有效冻结或网络黑客在收款行所在地范围内时，当地警方启动立案侦查程序无疑是抓获犯罪嫌疑人和追索资产最高效的方法。即便资金已被转走，当地警方介入亦将有助于查清资金流向和采取下一步行动方案。我们在办案实务中曾成功协助客户促使当地警方要求收款行披露资金流向，在追查到资金流入香港公司账户后，通过与香港方面的律师协作促使香港警方对香港公司及其相关高管采取相应调查措施。

对于跨境电邮诈骗，理论上还可请求国际刑警组织救济。一般由汇款方将案件报送至国际刑警组织在其所在国的国家中心局，该国家中心局会将请求转送至收款方国家中心局，并请求其采取行动。但实务中国际刑警组织较为关注大案要案，办理流程亦不公开，受害人较难与其取得有效联络或知晓和预见办案结果。所以，受害方通常不会将此作为单一救济，而与向当地警方报案等措施结合使用。

2. 民事诉讼

电邮诈骗的高科技和跨境特点使得抓获网络黑客或成功追回资金的几率不高，如果受害企业或个人无法通过警方追回款项，多会求助民事诉讼。一般来说，实务中存在如下诉讼路径选择：

1) 境外付款方对收款方提起不当得利之诉

在收款方为网络黑客或其控制的空壳公司时，收款方通常不敢或不会出庭应诉，其无任何合法理由收款，境外付款方提出的不当得利之诉基本能得到支持。

但一旦涉及款项洗白环节，案情则会复杂化，如果收款方与网络黑客存在贸易关系或者委托收款关系，境外付款方存在一定败诉风险。所谓不当得利，即没有合法依据取得利益，造成他人损失。此类案件中收款方通常会积极应诉，抗辩其所收款项存在货物买卖或受托收付等合同依据。根据我们的经验及对司法实务的观察，此类案例的判决结果很大程度上取决于双方的举证情况。

2) 境外付款方对收款方账户开户行提起财产损害赔偿之诉

当收款方账户为网络黑客所控制且款项已被转走时，起诉收款方意义不大。由于网络黑客在开户过程中常使用虚假身份证件或材料，实践中亦有境外付款方起诉收款行，认为收款行对开户人证件资料的真伪审查中存在过错，应当对其遭受的财产损失承担赔偿责任。根据我们的观察，此类案件中法院对银行是否负有实质性审查义务以及审查程度如何存在不同意见，判决结果并不统一。

3. 外交途径

目前大部分国家都会在境外大使馆内设置警察或警务联络处等职能部门，促进派驻国家与当地警方在跨境犯罪方面开展信息交流和协助执行等工作，各国领事馆一般负有促进和保护派驻国家在华贸易和投资方面利益之职责。因此，境外付款方亦可尝试自行或委托律师联系驻华使领馆需求保护。中国当地警方收到使领馆照会或求助，通常会更为重视并积极采取行动。

三、结语

近年来，电邮诈骗成逐年上升趋势，骗局设计和实施环节与本文所述大同小异。外贸企业和跨国公司应谨慎提防，对邮件和网络系统的进行安全升级，防范于未然。一旦遭受电邮诈骗，首先应考虑的是立即采取措施防止资金被提取或转移，然后通过警务、司法或外交等各种途径追回资金。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国法律及实务的最新动态和发展，上述有关信息不应被看作是特定事务的法律意见或法律依据，上述内容仅供参考。

如您对上述内容有任何问题或建议，请与汉坤**廖荣华律师（+8621-60800990; andy.liao@hankunlaw.com**）联系。