迈林法律评论

2024 年 5 月

MYLINK
迈林律师事务所

国际贸易

遭遇跨境电邮诈骗时，如何追索资产?

How to Recover Assets in case of Cross-border Email Scams?

前言

文章伊始，我们设置如下交易场景：你所在的医药公司长期与日本一家医疗科技公司存在合作。双方交易习惯都是中方先发货，日本公司收到货物验收合格后五个工作日左右将货款汇过来。然而，在你公司给日本公司发货过去二十多天后，对方既没有反馈产品质量问题也没有汇款过来。而后你联系日本公司，对方却说货款早在十天前就汇出去了并提供了相关汇款单据。此时，你可能已经意识到自己遭遇了诈骗，却无从下手...

At the beginning of the article, we set up a scenario: Your pharmaceutical company has a long-standing partnership with a Japanese medical technology firm. Under your typical transactions, your company sends the goods first, and after the Japanese company receives and checks them (usually within five working days), they send over the payment. However, after more than twenty days since your company shipped the goods, you haven't heard back about any issues with the product quality or received the payment. When you contacted the Japanese company, they claimed they had sent the payment ten days ago and provided proof of the transfer. This is when you might realize you're facing a possible scam but don't know what to do next...

跨境交易中，网络黑客利用外贸邮箱进行诈骗的案例层出不穷。本文中，我们将结合具体案例分析跨境电邮诈骗中的常见类型，以期能为相关企业和个人提供防范电邮诈骗的识别思路，以及在不幸遭遇诈骗后的资产追回策略和法律救济途径。

In cross-border trade, email scams using fake identities are increasingly common. This article will analyze specific cases to explain the common types of cross-border email scams. Our goal is to help businesses and individuals recognize these scams, and provide strategies for recovering assets and legal remedies if fraud occurs.

I. 电邮诈骗有哪些常见形式?
What are the common forms of email scams?

a. 网络黑客利用技术截获到付款内容的邮件以确定诈骗对象，而后注册一个邮箱名相似的“李鬼邮箱”，模仿交易方电邮行文特点给国外客户发邮件，要求支付货款到其指定账户，再将钱款取走。所谓的“李鬼邮箱”即通过混淆字形、增减字符或更换邮箱后缀等方式进行，例如

Hackers intercept emails relating to payment to identify targets for fraud. They then create a "fake email" account similar to the original sender's email (e.g., by using similar-looking characters, adding or removing a few letters, or changing the email suffix), and then mimic the email style of the trading partners to instruct the foreign client to pay into their own account. Subsequently, the hackers withdraw the money.

原邮箱 Original Email	“李鬼邮箱” "Fake Email"
Scarlett@163.com	（混淆字形）(Typo deception) Scar1ett@163.com
	（增减字符）(Adding/removing characters) Scarlet@163.com
	（更换邮箱后缀）(Changing suffix) Scarlett@l63.com

b. 网络黑客利用技术盗取受害人的邮箱密码，获取邮箱权限后，“潜伏”并监测业务进展。等到国外客户付款时，立即改变邮箱相关设置，例如后续收件自动转发至黑客控制的邮箱，黑客则仍使用原邮箱发邮件通知国外客户变更银行账户信息，但受害人对此毫不知情。

Hackers steal email passwords using technology to gain access and monitor business communications. When the foreign client makes a payment, they alter the email settings to reroute notifications to themselves. They then use the original email to instruct the client to change payment details, unbeknownst to the victim.

c. 在我们碰到的案例中，为逃避资金追索，黑客可能还会安排境外同伙同时与国内其他企业（“企业 C”）进行业务洽谈并取得企业 C 的银行账户资料，然后通过前述 a 或 b 手段指示国外客户将款项直接付给企业 C，并从企业 C 正常订货，而后其同伙就可以不花一分钱而骗得从企业 C 的供货。

In cases we have encountered, to evade fund recovery, hackers may arrange for overseas accomplices to simultaneously negotiate business with other domestic enterprises ("Enterprise C") and obtain Enterprise C's bank account details. They then use methods described in (a) or (b) to instruct foreign clients to directly pay funds to Enterprise C, who then fulfills orders legitimately. The accomplices can thus defraud Enterprise C without spending a penny.

相比于前述手段 a 和 b，手段 c 因为涉及多方交易主体，以及企业 C 善意第三人的存在，极

具迷惑性且追回款项的难度更大。
Compared to scenario (a) and (b), scenario (c) involves multiple parties and the presence of an innocent third party (Enterprise C), making it more confusing and significantly more challenging to recover funds.

II. 电子邮箱为何会被网络黑客入侵?
Why do email accounts get hacked?

a. 使用免费公共邮箱，存在邮箱安全隐患。公共邮箱不仅存在邮箱密码被黑客轻易获取的风险，甚至可以被轻易注册域名相同的邮箱来实施诈骗，导致付款方无法有效识别。
Using free public email services poses security risks. These accounts are easily accessed by hackers who can also create fake accounts with similar domain names to deceive payers, making it difficult for payers to identify valid recipients.

b. 点击极具迷惑性的钓鱼邮件。此类邮件往往具有正常邮件的外观，以各种合理的内容诱骗点击链接或是填写邮箱密码，从而被植入木马病毒或被窃取密码。
Clicking on deceptive phishing emails can lead to malware installation or password theft. Such emails often appear legitimate, enticing recipients to click on links or provide email passwords under various plausible pretexts.

针对上述问题，从技术层面而言，我们建议：
To address these issues, technically speaking, we recommend:

(1) 在国际贸易中，企业应尽量避免使用公共邮箱（特别是安全性较低的免费公共邮箱），而应当选择付费企业邮箱，同时设置安全系数较高的密码；
In international trade, companies should avoid using free public emails (especially those with low security) and opt for paid business email services with strong security features.

(2) 定期对使用的邮箱进行密码更新；
Regularly update email passwords.

(3) 定期进行电脑木马查杀、检查邮箱设置，如“自动转发”“邮件收发过滤器”“拦截设置”等。
Periodically scan computers for malware and review email settings like automatic forwarding, filtering, and blocking.

此外，我们需要特别指出的是，如因为中国企业使用安全系数存在问题的邮箱，导致黑客入侵并造成国外客户资金损失的，国外客户有权起诉中国企业，就资金损失要求中国企业承担全部或部分赔偿责任，理由是中国企业作为交易方有义务确保邮箱的安全使用，而国外客户

在交易过程中并无任何过错。
It's important to note that if the use of insecure email results in a hacker attack and financial loss for a foreign client, the client can sue for full or partial compensation. This is because the company has a duty to ensure secure email use, and the client is not at fault.

III. 为避免遭遇电邮诈骗，可采取的预防措施
Preventive measures to avoid email scams

除上述所提及的提升邮箱使用安全性外，根据我们的经验，中国企业还可以采取以下防范措施：
In addition to the aforementioned measures to enhance email security, based on our experience, the following measures can be considered：

a. 在与国外客户签署合同/订单时，为确保资金汇入安全，应当在合同/订单中明确在任何情况下，国外客户的资金应当汇入最初合同/订单确定的收款账号，否则相关汇款损失应由国外客户自行承担。
   Clearly state in contracts/orders that all payments must go to the agreed-upon receiving account to ensure secure fund remittance. Otherwise any loss due to a deviation should be borne by the client.

b. 如确需变更收款账户的，中国企业和国外客户的业务联系人应约定以电话或其他非邮件方式进行二次确认，确保汇款的安全性。
   If changes are needed, business contacts of the parties should confirm such changes through a second confirmation via phone or other non-email methods to ensure payment security.

此类预防措施的采用不仅可有效避免国外客户的资金损失，也有助于避免中国企业在发生资金损失后被追诉的风险。
These measures not only protect clients from financial loss but also shield Chinese companies from being sued after suffering financial losses.

IV. 遭遇邮箱诈骗，是否还能追回货款?
Can funds be retrieved after an email scam?

如果已经被骗，向诈骗分子的银行账户汇款，只要及时采取补救措施，仍有一定的机会追回货款：
If fraud occurs, there is still a chance to recover funds if payments were directed to the hacker's designated domestic bank account in China:

1. 资金被汇入黑客指定的中国境内银行账号的情形
When funds are transferred to a bank account in China designated by hackers

(1) 及时联系银行并报警以冻结资金
Quickly contact the bank and report the police to freeze funds

遭遇诈骗后，国外客户可第一时间联系收款银行要求冻结资金，并同时向公安机关报案以申请紧急止付。公安机关在收到报案后，或接收到银行转交的举报资料后，将通过发布紧急止付指令要求银行进行止付操作，以临时冻结账户。如果款项已被转入下一账户，尽可能促使银行披露资金流向，以便寻找当地律师介入采取相应措施。
Upon encountering fraud, foreign clients can immediately contact the receiving bank to freeze funds and simultaneously report to the police to apply for an urgent stop payment. Upon receiving the report, or upon receiving report data forwarded by the bank, the police will issue an urgent stop payment order to require the bank to temporarily freeze the account. If the funds have been transferred to the next account, efforts should be made to urge the bank to disclose the fund flow, facilitating local lawyers to intervene and take corresponding measures.

(2) 提起民事诉讼
File a civil lawsuit

随着诈骗手段的更新和资金转移的提速，以及受报案时间等因素影响，报案路径无法确保资金冻结的成功率。如果通过前述方式无法追回货款，受害方可以考虑提起民事诉讼以减少损失。诉讼路径有如下选择：
With the rapid evolution of fraud methods and the speed of fund transfers, and considering factors such as reporting time, the path of reporting cannot guarantee the success rate of freezing funds. If recovery through the above methods is unsuccessful, victims may consider initiating civil litigation to mitigate losses. The litigation options include:

- 付款方向收款方提起不当得利之诉
Suing the recipient for unjust enrichment

此类案件中，若实际收款方为网络黑客控制的空壳公司，由于收款方通常不敢应诉且没有收取货款的合法依据，受害公司的诉求往往能够得到法院的支持。
In such cases, courts often support victims if the recipient is a shell company controlled by hackers since the recipient typically does not respond and lacks a legitimate basis for receiving payments.

然而，在前述第 I 部分列举的情形 c 中，由于收款方与黑客存在真实贸易关系，通常会积极应诉和抗辩，付款方将存在一定的败诉风险。
However, in the methods listed in Section I, especially scenario C, where the recipient

has a genuine trading relationship with hackers, they tend to actively respond and defend, posing a certain risk of losing the lawsuit for the payer.

- 付款方向银行提起损害赔偿之诉
  Suing the bank for damages

  在天津市一中院作出的一则民事判决书中，法院以银行未协助办理紧急止付和快速冻结等予以止损的措施、涉嫌违反相关规定为由，判令银行向受害人承担一定比例的赔偿责任。鉴于此，如果付款方在向银行提出冻结资金的申请而被拒绝时，付款方应保留相关证据以便事后维权。
  In a civil judgment issued by the Tianjin No. 1 Intermediate People's Court, the court held that the bank's failure to assist in urgent stop payments and rapid freezing measures, and suspected violations of relevant regulations, ordered the bank to compensate the victim for a certain percentage of damages. Therefore, if the payer's application to freeze funds is rejected by the bank, the payer should retain relevant evidence for subsequent rights protection.

2. 资金被汇入黑客指定的非中国境内银行账号的情形
   If funds were directed to a non-China based bank account specified by the hacker

在我们碰到的诈骗案例中，资金被要求汇入香港银行账户情形较多。在此，我们以收款账户为香港账户为例进行分析。
In the fraud cases we have encountered, many cases have specified that funds should be transferred to a Hong Kong bank account. Here, we analyze the case by specifying that the receiving account is a Hong Kong account.

国外客户应第一时间联系其银行终止付款，并要求其银行通知收款银行以取消汇款。同时，国外客户应委托包括律师在内专业人员或通过香港电子报案中心向香港警方报案。必要时聘请香港本地的律师，向警方争取对相关银行发出“不同意处理书”，及时冻结银行账户。由于冻结期限通常不超过六个月，受害人即使能够成功冻结账户，也应尽快启动民事诉讼程序。
Foreign clients should contact their banks to terminate payments as soon as possible, and instruct their banks to notify the receiving bank to cancel the remittance. At the same time, foreign clients should entrust professional personnel including lawyers or through the Hong Kong e-Report Center to report the case to the Hong Kong police. When necessary, they can hire local lawyers in Hong Kong to obtain the "letters of no consent" from the police to freeze the bank account. As the freezing period usually does not exceed six months, even if the victim successfully freezes the account, they should quickly initiate civil litigation procedures.

V. 结语
Conclusion

在涉及跨境交易，尤其是付款安排时，应多方面谨慎确认，同时企业内部也需要对邮件系统定期安全升级并对相关人员做好安全培训。如果不幸遭遇电邮诈骗，则应把握黄金时间，通过立即报警等方式阻止资金进一步转移，并及时聘请具有追索经验的法律顾问，通过法律途径尽可能追回资金。

In cross-border transactions, especially involving payments, thorough verification is crucial. Businesses should regularly update their email systems and provide security training to relevant personnel. If faced with email fraud, swift action is essential to prevent further loss by immediate reporting and timely hiring of legal consultants experienced in recovery methods through legal means.

如您对本文有任何问题，请联系：

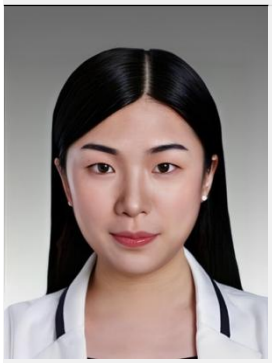
If you have any questions about this article, please contact us via:

陈祥龙，执行合伙人

Erex Chen, Managing Partner

Tel: +86 21 68556511

Email: erexchen@mylinklaw.com



张丽丽，律师

Doris Zhang, Attorney

Tel: +86 21 68556500

Email: doriszhang@mylinklaw.com