UK P&I CLUB

L P Bulletin

2016 年 9 月 28 日 星期三

防损公告 1112 号——09/16 ——网络诈骗——全球

2014年12月，协会调查部门Signum Services针对“发票造假”发布了防损意见（2014年12月16日防损公告1014号）。鉴于此类犯罪屡禁不止，有必要提醒会员应格外谨慎。建议会员要求其会计部门谨防诈骗。

上述诈骗或称“授权诈骗”或“钓鱼付款诈骗”。虽然所称不同，但手法基本一致。

通常，诈骗犯会攻入进受害者的电邮网络，这些电邮在近期曾发出付款要求。原始邮件发出后不久，诈骗犯会回复邮件，冒充原始邮件的发件人。诈骗方完全复制受害者邮件的格式，仅对信头稍作改动，经常是只修改一个字母。

这封新邮件声称原来的付款账号有问题，要求受害者向该账号的子账户付款，该账户其实是诈骗犯事先开立的账户。在个别案件中，诈骗犯甚至运用Photoshop软件对邮件随附发票的银行信息进行改动。

之后，受害者付款，但几天后才发现交易有诈。不幸的是，届时诈骗犯已经通过一系列银行转账转走诈骗款，无法追回。

让受害者迷惘的是，在这个号称安全有保障的现代银行业务的时代，诈骗犯竟然可以在另一个国家开立银行账户，而且会有资金转入。

诈骗犯可利用几种方式开立帐户，“ 地下网络”相关信息应有尽有，诈骗犯可从中得到协助。有组织的犯罪集团时常会收买银行职员，以便利用虚假身份开设银行账户。即使有些银行行员尽忠职守，因为无从着手，他们也无法核查外国户主的身份。举例来说，一名英国银行职员可以识别虚假的英国护照，却可能无法辨别罗马利亚护照的真伪。

此类诈骗一般容易得手，因为诈骗犯无需办理开设银行账户的手续。诈骗犯可轻易取得或伪造账单等单据，拦截邮件单据等。一旦获得足够受害者的个人身份和财务信息，诈骗犯便能接管受害者的银行账户或冒充受害人。诈骗犯会通过银行分行或呼叫中心破解受害者的网上安全信息，登陆其银行帐户，或通过团伙作案或安插人员进入受害者的所在银行，控制其账户。

通过“国际银行帐户号码”（IBAN）进行的交易是自动交易。由于银行每天需要处理大量付款业务，将汇款转入指定账户前，银行无法核查每项交易中汇款人指定的收款人的名称是否与该收款人账号持有人的姓名一致。只要汇款人提供的收款人银行代码正确，汇款将自动记入收款人账上，除非收款人账户被冻结。如果收款人账户冻结，汇款将自动退回。

诈骗犯通常跨越多个司法管辖区跨国作案，以致国家执法机关打击此类诈骗屡屡受阻，受害人想要追回被骗款项极其困难。

鉴于以上，建议会员提高防范意识，避免受骗。协会建议，无论在何种情况下，一旦收到可疑的付款要求，应重复核查该请求的真实性，最好是亲自向对方经手人核实情况，但前提是应确保该经手人的真实身份不是诈骗犯。

随附 TT Club 近期发布的相关文章，有兴趣的会员可点击阅读：
http://www.ttclub.com/loss-prevention/tt-talk/article/tt-talk-mandate-fraud-133885/

信息来源

David J. Thompson
Signum Services
Thomas Miller P&I (Europe) Ltd. Department
电话：+44 20 7283 5616