欺诈 —— 入侵商业电子邮件

您知道要注意的危险信号吗?

如果您在国际供应链行业中工作，那就有可能在正常的业务过程中，无意中接触到多种类型的支付诈骗。这些诈骗方法往往都很复杂，涉及国际上的多方合谋。 其诈骗收益通常用于其他犯罪活动，如毒品走私、人口贩卖、现代奴隶制和恐怖主义。

在当今快节奏的数字化环境中，商业交易和沟通几乎都要通过网络进行，欺诈风险也随之增加，使得尽职调查比以往任何时候都更为重要。本通讯将带您了解全球供应链中最常见的支付欺诈方法，以及您可以采取的预防措施，从而减轻您的风险。

有哪些风险?

在我们的行业中，哪些类型的诈骗是最常见的?

支付欺诈

通常情况下，有一个骗子伪装成为一个您定期给其付款的企业，会指示您将款项支付到另一个账户。欺诈人会监视电子邮件系统，从而等待一个合适的付款请求。他们会复制邮件的风格和语言，以确保不会被发现。通常他们所使用的电子邮件地址与您经常发送的地址几乎是相同的——有时甚至是完全吻合的。

CEO欺诈

CEO欺诈是一种常见的支付诈骗，即有一封似乎是来自内部邮件的指令，声称是公司高级管理人员发送的，要求您紧急汇一笔款项给一个新客户或与现有客户类似的一个新开设的账户。

采购欺诈

在全球供应链中，企业普遍依赖于分包商提供物流服务；然而，这可能会让您暴露于骗子假冒分包商签发虚假发票的风险中。

骗子会潜入计算机系统，监控电子邮件，以收集诈骗所需的信息。通常，伪造的发票很难与特定的委托保持一致，或者它可能是先前采购订单的副本，但银行信息不同。

骗子可能会使用一些策略，例如不付款在信用评级、商业地位上的负面影响，以及威胁采取法律行动，迫使交易通过。

为避免成为欺诈活动的受害人，当您在工作时收到此类电邮，请考虑以下指引:

TT CLUB
IS MANAGED
BY **THOMAS**
MILLER

如需更多信息
请发送邮件至 **riskmanagement@ttclub.com**
或访问我们的网站 **ttclub.com**