恒生銀行
HANG SENG BANK

恒生中国《付款诈骗》认知指南

协助保护您的企业，防范诈骗和网络犯罪

支付诈骗：保护您的企业

诈骗是现今企业最常见的威胁之一。

支付诈骗可导致重大财务损失。各种规模的企业都面临风险。本指南旨在协助您和您的员工察觉及预防支付诈骗和骗局，并在您沦为受害者时采取正确的行动步骤。

突破1.03万亿美元
全球反诈总会（GASA）表示，2024年全球诈骗损失已突破1.03万亿美元。

资源来源：汇港资讯

本指南将协助您了解可能会影响您业务的常见诈骗与骗局，并概述您可以采取哪些实用步骤，避免您的企业成为诈骗犯的受害者。在整个机构内推广此主题的教育，有助于提升业务的整体防护能力。本指南提供多项实用贴士及核对清单，可供管理层及相关团队共享使用。

可能威胁您业务的诈骗类型

骗徒如何与您联络

- **【授权支付】**（APP）是指企业被冒充合法收款人的骗徒所诱导，而主动将款项汇出。最重要是了解骗徒所采用的联络方式，对防范此类骗案至关重要。
- **网络钓鱼**是诈骗的常见手法。此类攻击旨在骗徒试图欺骗用户点击一个连结，从而下载恶意程式或被导向至伪冒网站。网络钓鱼连结可能藏于电邮、短信或各类通信平台的信息中。
- **电话诈骗**是您接获涉及金钱的电话，则极有可能是诈骗。骗徒可能冒充您熟悉并信任的机构或权威人士，例如银行或警方。他们或会掌握您的个人资料，甚至利用【改号欺骗】，使来电号码看似真实可信。
- **短信诈骗**是指骗徒发送伪冒银行或其他合法机构的虚假短信。其目的是诱使您回复个人或财务资料，从而盗取您的账户紫金。骗徒也可能通过常见的通信平台发送诈骗信息。

商业电邮诈骗

商业电邮诈骗

伪冒电邮是骗徒常用的诈骗手法之一。

当付款到期时，骗徒可能发送一封看似由供应商发出的电邮，内容模仿真实信息的格式与语气。他们会声称您的付款银行资料已更新，并提供新的账户资料，要求您按指示付款。

这类电邮往往难以辨识：

◆骗徒常会使用供应商的真实电邮地址，或伪装成极为相似的地址。
◆他们会制作看似真实的发票。
◆供应商员工的电邮签名也可能毫无异样。
◆信息内容往往带有急切语气，例如声称与敏感交易有关，需即时汇款。
◆骗徒可能已掌握整段电邮往来记录，并能以相似语气及措辞回复。
◆最重要的是——所要求的付款往往确实到期。
◆唯一的分别可能只是银行账户资料已被更改。

电邮入侵如何发生?

电邮账户盗用

- 骗徒使用骇客技术或已窃取的账户资料，入侵企业的电邮账户。
- 电邮账户详细资讯可能是因网络钓鱼或资料外泄，而被骗徒获取。
- 不法份子可能会搜集有关使用者的联络人资料、邮件撰写风格和个人资料，使他们所杜撰的信息看起来更可信。

伪冒电邮

- 不法份子开立一个与真实电邮地址非常相似的账户
- 或者他们可能利用伪冒的电邮格式和标题，企图令收件人不容易察觉，并将其当作为真实的邮件来回复

冒充高层主管诈骗

不法份子假冒公司的高层人员

- 他们通常向财务部门发送电邮，要求紧急汇出一笔大额款项，原因可能是用于收购项目或其他重要交易。
- 被冒充的高层主管往往正值休假或不在办公室，令相关细节难以即时核实。
- 骗徒可能透过网络钓鱼攻击或资料外泄入侵电邮账户，并从公司网站或社交媒体收集资讯，以增加信息的可信度。

账户盗用

账户盗用

什么是账户盗用?

此类诈骗一般由于骗徒诱导您泄露个人资料，从而取得您的银行账户存取权限。他们会重设密码及安全验证资料，使您无法登入账户，并可能更改账户所连结的电话号码、地址及电邮地址，令其可如同合法客户般操作账户。

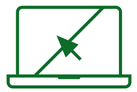
遥距账户盗用

此类诈骗是指骗徒控制您的装置某网站，并在您毫不知情或未经授权的情况下，从您的银行账户进行付款。骗徒通常会先发送链接，要求您浏览或下载特定软件，以取得您的装置的远端存取权限。通过阅读本指南，您将了解骗徒常用的手法，并掌握防范措施，保护自己及业务免受侵害。

电话号码诈骗

这是指骗徒通过更改来电显示号码，伪装成您的银行的官方电话号码。该号码可能与真实号码完全相同，或仅相差一个数字。骗徒也可能使用隐藏号码来致电。

恶意程式与网络钓鱼



骗徒会利用恶意软件及链接窃取个人资料。

这些资料可能被用作诱导您误信某通电话属真实来电，或用以入侵您的银行账户。

授权代码

请注意：包括银行在内的任何机构，绝不会指示您如何使用实体或数码保安装置（即【保安编码】），也不会要求您提供网上理财授权代码。

账户盗用

建议贴士

- ✓ 切勿透露您的网上理财使用者名称、密码、授权代码或任何一次性密码（OTP）。
- ✓ 请记住，来电号码有可能被伪造，切勿单凭来电显示判断对方身份。
- ✓ 如接获不明来历的电话，请挂线并改用经独立渠道核实的电话号码（例如对方官方网站所列的号码）回拨查询。建议使用另一部电话，或先联络熟悉的联络人，以确保通话线路安全无虞。
- ✓ 对可疑电邮及短信务必提高警觉，尤其是含有链接或要求提供资料的信息。所有要求提供资料的信息，应直接向相关公司核实，并参照上述联络方式。
- ✓ 切勿因不明来历的电话而点击任何链接、浏览网站或下载软件。
- ✓ 您的保安编码装置属个人专用。如有人来电要求您使用该装置，请立即终止通话并联络您的银行。
- ✓ 恒生绝不会要求您参与任何正在进行的调查、指导您如何回答问题，或要求您将资金转至所谓的【安全账户】。
- ✓ 请确保公司已设立既定程序，让员工通报可疑情况，并确保全体员工均了解【遥距账户盗用】诈骗的风险。
- ✓ 加强员工教育——确保所有人员均认识【遥距账户盗用】诈骗手法，并建立相应的通报及处理流程。
- ✓ 在付款流程中建立严谨的尽职审查文化，例如采用双重审批机制，以加强风险防控。

如何减少付款诈骗风险

减少付款诈骗风险

每间企业均可采取一系列简单且成本不高的措施，以减少付款诈骗及骗局的风险。防范工作人人有责。

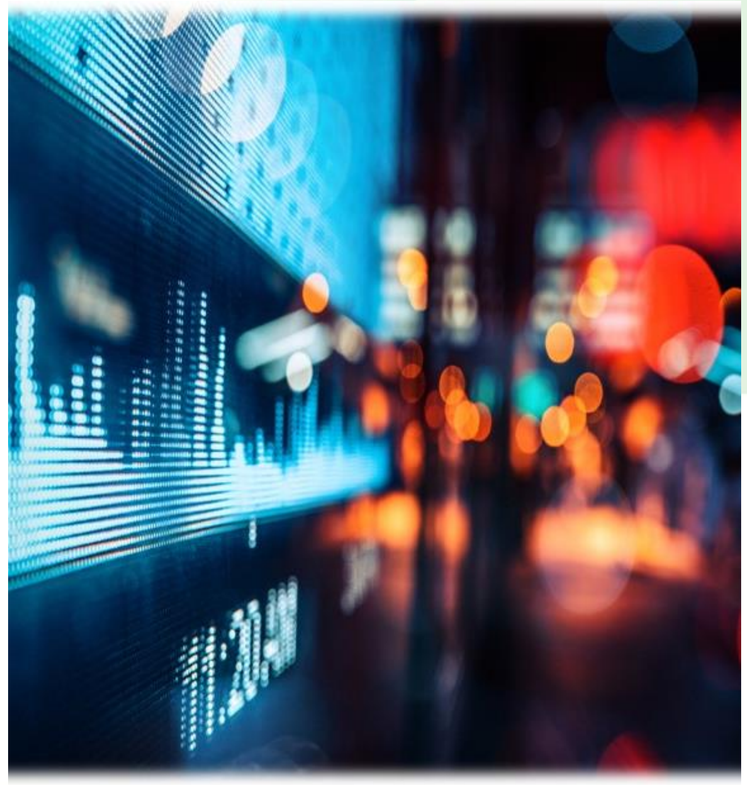
◆ 在您的业务中可能存在弱点的部分培养警觉意识

◆教育员工如何识别和避免诈骗，并确保他们了解公司的安全政策和程序

◆对任何不寻常或与业务背景不符的付款要求，应主动提出查询。

◆最重要的是，任何新增的收款人或银行账户资料，务必通过已预先建立的可靠渠道（例如已知联络人及电话号码）核实。

◆接下来的数页投影片将提供更详尽的指引，为负责付款的同事提供支援。



检查电邮地址

骗徒会冒充可信人士。

- 即使电邮署名为您熟悉的人士（如您认识或经常联络的人士）,也应核对电邮地址是否正确。
- 如发送人属公司同事，其电邮地址应可在公司通讯录中查核（如有提供）。
- 请特别留意网域名称的拼写是否正确。骗徒常会建立与真实网域极为相似的伪冒地址，只改动一两个字母，企图混淆收件人，例如 J@rnbusiness.com与 J@mbusiness.com.
- 显示名称可能隐藏真实的发件人电邮地址，切勿只凭表面判断。

仔细检查电邮

[紧急要求】是常见的警号。

- 如电邮涉及付款事宜，且语气紧急或声称无法回电，应视为可疑信息。
- 部分网络钓鱼电邮语句粗疏，即使拼字正确，语法也可能错误。对晚来电邮务必保持高度警觉，尤其是含有链接或附件的。请注意：生成式人工智能令骗徒更容易制作自然语气、内容逼真的恶意电邮。
- 如您并未预期收到该信息，或不认识发件人，切勿点击链接或开启附件。

新收款人或变更账户资料均需核实

请务必通过已知联络方式与指示方核实其要求。

- 在可行的情况下，应致电您熟悉的联络人进行确认。例如：如变更付款资料要求来自公司内部人员，请直接致电同事确认；如变更要求来自供应商，请致电您经常联络的负责人，并同时核对银行代码及账户。
- 切勿直接回复该电邮或使用电邮内所提供的联络方式。
- 一般情况下，网络不法分子在获得登入账户权限后，会向账户联络清单上的相关人士发送钓鱼邮件。这代表着即使电邮的内容相当可疑，您仍可能会因为电邮地址正确无误，而认为真的是由该寄件人发出。此时，您应致电寄件人，既可以确认电邮中的要求，也可提醒他们的电邮账户或已遭入侵。

减低付款诈骗风险

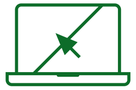
任何类型的企业均可能面对诈骗风险，手法也多不胜数

制定及落实有关汇款的保安机制

确保所有付款均经妥善核实，是防止诈骗最关键的一步。建立既定的程序，防止汇款团队在未经核实的情况下授权新增或更改的付款指示。按照所订立的保安机制，就可确保汇款团队不会仅根据，看起来真实的付款指示，未经验证的电邮或电话指示转移资金。此外，也应鼓励员工直接联络收款人以确认新的或变更的付款要求。

提高员工警惕性

企业应为员工提供充足的培训，教导员工防诈骗是公司任何一员的责任，并建立一套能让员工向管理层安心反映疑虑的企业文化。



审慎管理您的数码足迹

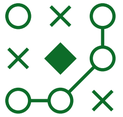
在社交媒体平台上过度分享个人资讯，可能令骗徒掌握您、您的朋友、家人及联络人的资料，并用作冒充身份。减少公开个人资讯，有助降低成为攻击目标的风险。

鼓励员工三思而后点击

在点击可信任的网站上的链接虽然无妨，但点击未经验证电邮和即时信息中的链接，则应可免则免。将鼠标悬停在链接上，您便可看到隐藏的网址并验证其真实性。在点击任何电邮内的链接或下载任何附件之前，请再三查证，尤其应注意是否出现拼写和文法错误。

加密您的密码可靠性

请考虑使用密码管理器或密码短语，密码短语通常比传统密码更长，但更容易记住且难以破解。鼓励员工随机选择三个单词，并选择字母、数字和符合组合，以加强密码的可靠性。



在遇上诈骗/网路攻击时应采取的措施

如果您或您的公司不幸成为诈骗/网路攻击时受害者，请迅速采取应对措施，及时举报已发现或疑似的事件有助于保障公司免受进一步的攻击，减低损失。请尽快与您的银行或相关的财务机构联络，以确保及时得到所需的支援。

检查清单：高级管理层

最有效抵御诈骗的方法，就是防范于未然。以下检查清单可为您提供一些实用建议，助您保护企业的网络安全。

- 贵公司是否已设立既定程序，要求核实所有新增或变更的付款指示？员工是否清楚可从何处取得可靠的联络资料？
- 贵公司是否已制定明确的付款申请流程，包括申请人、申请方式及在有疑虑时的核实方法？
- 贵公司所使用的密码是否具备足够强度（例如：最少字元长度、包含字母、数字及符号）？贵公司是否已考虑使用密码管理工具，或采用密码短语？
- 是否已评估并在可行范围内实施多重认证？
- 员工是否清楚在发现可疑付款或已发出诈骗付款时应如何应对？
- 贵公司是否已制定网络事故应变计划，例如电邮账户遭入侵时的处理流程？
- 是否定期与负责汇款的员工讨论潜在诈骗风险？
- 贵公司是否设有政策，禁止共用使用者名称及密码以存取汇款系统？
- 贵公司是否已设立双重交易审批机制？
- 面对具有高风险的汇款时，团队中的成员是否主动联系高级主管？

检查清单：处理付款-第1/2部分

在最容易受诈骗威胁的业务范畴,应时刻保持警觉及采取合适的行动，请参考下列建议，有助相关的人员以更严谨的方法处理付款指示，并培养对诈骗有警觉性的企业文化。

- **想一想：该要求是否不寻常或与业务背景不符？是否合乎逻辑？**任何涉及汇款或账户资料的电邮，如语气紧急或声称无法回电，均应视为可疑。如您并未预期收到该信息，或不认识发件人，**切勿点击任何链接或开启附件。**

- **请核实电邮地址是否属真实及可信。**即使电邮署名为您熟悉的人士（如您经常联络的人士），也**应核对电邮地址是否正确。**骗徒会冒充可信人士。如属公司同事，其电邮地址应可在公司通讯录中查核（如有提供）。

  另外，请特别留意网域名称的拼写是否正确。骗徒常会建立与真实网域极为相似的伪冒地址， 只改动一两个字母，企图混淆收件人，例如 J@rnbusiness.com 与 J@mbusiness.com.显示名称可能隐藏真实的发件人电邮地址，切勿只凭表面判断。

- **即使汇款指示来自高级管理层，也应保持警觉，提出质疑。**骗徒深知员工更倾向听从高层指示，因此常会冒充高级主管或业务伙伴发出付款要求。切勿单凭电邮内容信任付款指示，即使发件人身份看似可信。骗徒也可能通过常用的即时通讯平台进行诈骗。

请注意，骗徒有可能已入侵并取得您正在通讯的电邮账户的存取权限

检查清单：处理付款-第2/2部分

核实新增或更改的付款资料，有助减低付款诈骗的风险。除了回拨电话加以确认，还有多项重要措施可进一步减低风险。

请注意，骗徒有可能已入侵并取得您正在通讯的电邮账户的存取权限

◆ 核实新收款人或账户的资料变更

在可行的情况下，请使用可靠的联络方式向对方查证，并请尝试与您认识的人确认。例如，如果变更请求来自公司内部人员，请直接致电该人员以作确认。如果来自供应商，请致电与您经常联络的人员以作确认。请勿回复电邮或使用电邮中的联络方式。一般情况下，网络不法分子在获得登入账户权限后，会向账户联络清单上的人士发送钓鱼邮件。这代表着即使电邮的内容相当可疑，您仍可能会因为电邮地址正确无误，而认为真的是由该寄件人发出。此时，您应致电该寄件人，既可以确认电邮中的要求，也可提醒他们的电邮账户或已遭入侵。

◆ 切勿直接回复该电邮或使用电邮内所提供的联络方式。如骗徒已入侵他人账户，他们极有可能更改联络资料，令您最终与骗徒通话。

◆ 请主动致电付款指示方确认，切勿依赖对方来电。骗徒深知回拨核实是常见程序，可能会先行联络您，以避免此步骤

生成式人工智能（AI）与诈骗

人工智能诈骗

骗徒可能利用生成式人工智能来欺骗个人和企业

为保障自身及企业安全，了解骗徒如何运用此技术至为重要。

生成式人工只能已成为骗徒所使用诈骗手法的工具之一，使骗徒手法更逼真。由于此技术能模仿语言风格，甚至复制影像及声音，骗徒更容易冒充您熟悉及信任的人士或企业。

常见手法包括：

- **语音冒充**--骗徒致电企业员工，冒充公司行政总裁，指示员工将一笔【机密】款项汇入一个暂记账户。由于员工误以为正在与行政总裁通话，便批准了该笔付款。
- **深度伪造技术（deepfake)**--骗徒可能会复制供应商公司某位成员的完整外貌与声音，以冒充其身份。骗徒假扮已知的供应商公司代表，安排与付款方公司通话，并要求更改银行账户资料。由于负责付款的同事误以为自己【亲眼见到】熟悉的供应商代表，便批准更改银行账户资料。

什么是生成式人工智能?

- 人工智能（AI）是一种允许电脑模仿人类思维和决策的技术。人工智能通过分析大量数据并不断学习，从而使所作出的决策更贴近人类思维模式。
- 随着人工智能接收及分析更多数据，人工智能的决策将不断改进，并能够做出与人类相似的决策，这使得骗徒更容易冒充人或企业。
- 生成式人工智能则运用相同技术来创造内容，包括文字、图像、影片及/或音讯。

请勿假设电话或视像通话必定真实可信。如对方要求提供敏感资料、指示向新收款人付款，或施加压力要求即时行动，请格外警惕。企业应设有清晰明确的增加新收款人的付款程序。无论员工对收款人有多大信任，该程序也不应被绕过。

如何保护自己免受这些威胁?

深度伪造提高了骗徒诱骗受害者的能力。虽然如此，很多现行的措施仍能有效降低这些风险。以下介绍了一些关键的防骗措施。

谨记常用的防诈骗措施

- 特别留心那些要求您迅速采取行动的短信/电邮/电话/影片-这些通常是诈骗的迹象。
- 请注意，恒生绝不会通过电邮或短信要求您提供任何个人或公司账户资料及财务资料。
- 确保尽量只接受来自已批准的公司通讯渠道传送的付款指示。骗徒通常通过微信等公开通讯渠道联络受害者，因为他们无法使用经批准的公司渠道。
- 务必检查和验证从短信/电子邮件/网上收到的资讯，尤其是在任何人都可以发布帖文的论坛或网站。如果不确定信息真伪，请与客户经理确认。

每日安全代码

每日安全代码是每日产生的独特且具时效性的代码，仅分发予获授权人员。这些代码可用作验证通信及交易，为防骗加设一重难以被骗徒复制的安全保障。以下是有效实施方式：

- 每日独立代码：每日产生一组独特代码，供员工使用。
- 安全分发：通过加密电邮或公司内部安全平台分发代码。切勿与组织外部人士分享代码。
- 核实程序：在敏感交易、高价值通讯或任何需要身份验证的情况下，要求提供当日代码。

监察及培训

- **人工审核**：针对大额交易或异常交易的审核，制定合适的内容不控制机制，包括设定交易限额，日终跟踪异常交易，并设定多于一人作交易批核。在执行重要交易时，建议当面进行交易，避免损失。
- **网络钓鱼防范意识**：为员工提供持续的培训，帮助员工辨识并懂得应对网络钓鱼攻击。网络钓鱼攻击通常是接连其他更精密的攻击。
- **深度伪造防范意识**：教导员工了解深度伪造技术的风险以及骗徒如何将其用于欺诈。培训应涵盖如何辨识深伪诈骗、遵守保密协定的重要性，以及如何举报可疑活动。

如何分辨深度伪造技术-额外指引

人工智能技术迅速发展，意味着深度伪造（deepfake)内容将愈来愈难与真实影像分辨。虽然以下建议有助识别较低阶段的伪造手法，但仍应考虑额外的控制措施以加强防范。

请记住“即使对方的外貌与声音看似来自您公司内部人士，若其要求异常，仍应保持怀疑态度。对于大型或不寻常的交易，维持一定程度的人工审核始终是良好做法。

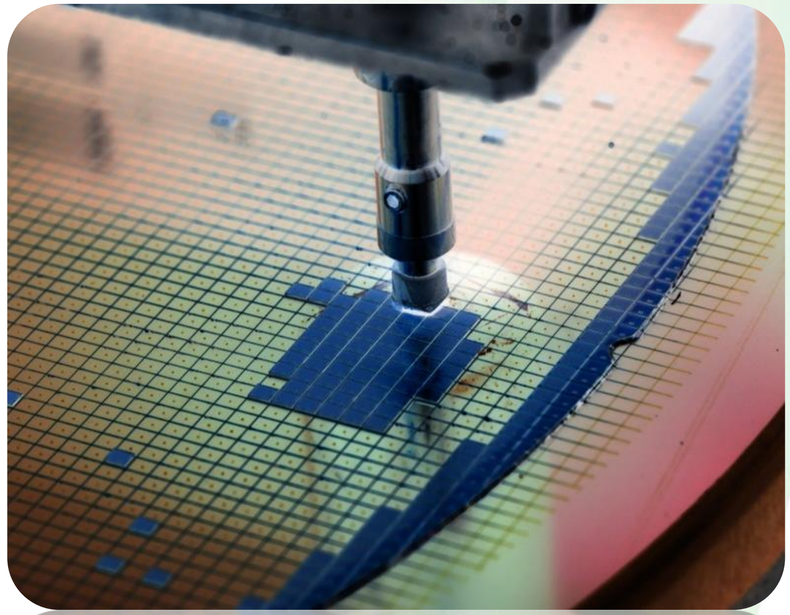
1. 眼睛会产生反光，无法正常呈现光照的自然物理特性
2. 面部表情不自然或五官位置异常，或身体移动方式不自然
3. 头发或皮肤可能呈现模糊或异常移动
4. 口型无法对上。注意聆听音调和音量的变化
5. 背景可能与通话场景不符。可能会显示奇怪的反射或异常现象
6. 似乎没有开灯或有奇怪的阴影

如果不幸成为诈骗受害人，怎么办

如果您不幸成为诈骗受害人

立即采取适当措施，可把诈骗所造成的损失减至最低，同时也提高追回资金的可能性。

- **停止与骗徒的一切联络。**
- **尽快通知所有相关人士和组织**（员工、客户和财务机构），**并须立即联络银行，发出退款指示。**因为资金转移速度非常快，一旦被转移，退款程序便会更困难。
- **向有关当局举报诈骗个案。**
- **保留所有与诈骗相关的证据查看您的财务记录，以辨别任何未经授权的交易或可疑活动。**包括电邮、收据及其他通讯记录，以便日后取证之用。
- **检视并改善公司的保安政策和措施。**



向恒生举报诈骗

如您不幸成为诈骗受害者，请务必迅速采取行动！

我收到一封来自恒生银行发出的可疑电邮

- 请停止，切勿回复电邮
- 切勿点击任何链接
- 切勿开启任何附件

建议拨打公司客户服务热线与我们联络，我们会作进一步跟进。
中国内地可拨打：800-830-8008
非中国地区可拨打：+86：400-830-8008

我需要报告一宗诈骗活动

如果您已授权付款，并且认为您已成为诈骗的受害者，或者怀疑您已泄露安全性资料，请立即致电公司客户服务热线。

您可以24小时随时致电我们。

另请通知您的客户关系经理或客户服务代表。

有人致电我，自称来自恒生，但行为可疑

有人致电我，自称来自恒生，但行为可疑

结束通话，并使用已验证的电话回拨，以确认来电真实可信。请勿向来电者提供任何资讯。恒生绝不会要求您提供安全装置产生的代码。

如果您遭受网络攻击，请采取以下措施：

- **关闭所有受影响设备的网络连线，**以防止恶意软件散布或未经授权的入侵。
- **更改所有受影响账户的密码，**包括电邮、网络和其他可能泄露了资料的账户
- 聘用信誉良好的网络保安公司，对您的系统进行**全面检查**，以发掘其他漏洞或入侵活动。
- **尽快通知所有相关人士和组织，**例如员工、客户和监管机构，并为他们提供所有相关资料。
- **确定攻击来源，**并采取措施，防止未来再次遭受类似的攻击。

恒生銀行
HANG SENG BANK

免责声明：

本文件由恒生银行（中国）有限公司（“恒生中国”）发布。其中的内容仅供阁下参考，如有任何更改，恕不另行通知。

恒生中国对本文件中所载之任何信息或观点，或形成任何观点之基础的公正性、准确性、完整性或正确性并无作任何明示或默示的担保、申述、保证或承诺，亦不会就任何人使用或依赖本文件所载的观点而承担任何形式的责任。本文件包含的信息来自于恒生中国认为可靠的来源，但仍请阁下自行核实有关资料，对本文件所载观点的相关性、准确性及充足性自行作出评估，并就此评估进行其认为需要或合适的独立调查。如本文件中的任何内容标注为引用、总结或翻译自第三方报告的，则该等信息仅阁下参考，阁下不应该依赖该等内容或者将其认为是该等报告的准确、完整的重述。阁下可通过本文件列示的出处来源/渠道或链接，直接读取该等报告的原文，以获得更全面和详细的信息。

恒生中国不提供任何法律，税务，会计，监管或相关的专业建议，阁下应当自行就该等方面进行独立评估并获得专家建议（如阁下认为需要）。特别是，本文件可能包含对法规的某些引用。如果包含法规，恒生中国并未声明对法规的引用是详尽无遗的。可能还存在其他可能与提案相关的法规。恒生中国不会就监管法规提供建议，阁下应该咨询自己的合规或法律顾问。