一般资料概要 – 网上银行服务

本文檔提供有关使用网上银行服务（「网上银行服务」）的一般资料概要，仅供参考。详情请参阅：

- 户口及有关服务的条款及条件(个人户口)，
- 网上银行服务的条款及条件，或
- 银行网站。

1. **费用及收费**
    - 与网上银行服务相关的费用及收费，请参阅服务收费表（一般银行服务）。

2. **个人资料保护**
    - 有关网上银行服务对客户个人资料的保障，请参阅有关个人资料(私隐)条例之客户通告及私隐政策声明。

3. **客户的承诺与义务**
    - 客户应承诺在使用网上银行服务(包括但不限于银行网站、银行流动应用程式、保安编码器和流动保安编码)时遵守网上银行服务的条款及条件，以及银行不时规定的有关网上银行服务的使用政策及程序。
    - 除此之外，客户承诺：
        i. 不会对网上银行服务、银行网站、银行流动应用程式、流动保安编码或前述所包含的任何软件的任何部分进行干扰、修改、解读、反向工程或以其他方式变动或未经授权进入网上银行服务、银行网站、银行流动应用程式、流动保安编码或前述所包含的任何软件的任何部分；
        ii. 不会以在流动装置或作业系统供应商支持或确保的配置外进行过修改的任何装置或作业系统（例如，已经被「越狱」或「刷机」的装置）进入或使用银行网站、银行流动应用程式或流动保安编码。被越狱或刷机的装置指在未经流动服务提供商及/或电话制造商批准的情况下不再受限于其所设置之限制的装置。在被越狱或刷机的装置上使用银行网站、银行流动应用程式或流动保安编码可能会损害安全并导致欺诈性交易；及
        iii. 仅从官方流动电话应用程式网上商店（例如 Google Play 或 Apple App Store）下载银行流动应用程式及其更新。
    - 如果客户违反上述承诺，银行有权终止客户的网上银行服务（包括但不限于银行网站、银行流动应用程式、保安编码器和流动保安编码）而不通知客户，并就此对客户采取法律行动。
    - 如果客户未采取本行或客户电子装置制造商不时告知或公布的任何安全措施，客户须对因使用网上银行服务而引致或与其相关的所有后果全权负责并承担所有责任。
    - 客户使用网上银行服务时一旦遇到任何不正常情况或困难，客户应尽快通知银行。

- 客户向银行声明及保证，客户使用网上银行服务时将符合一切适用法律、规则及法规，以及网上银行服务适用的用户手册、政策及程序、网上银行服务的条款及条件及客户与本银行订立的任何其他协议（可不时予以修订）。

4. 客户对未经授权的交易的责任

- 一般而言，如发生未经授权的网上银行交易，而客户方面并无严重疏忽、欺诈或错误（例如客户未能妥善保管接驳网上银行服务（包括但不限于银行网站、银行流动应用程式、保安编码器及流动保安编码）的设备），则客户将无须负责其所蒙受的任何直接损失。
- 但客户应明白及确认客户的信用卡、客户名称、私人密码、流动保安编码密码和流动保安编码（如适用）及/或保安编码有被未获授权人士不当使用或被用于未获批准的用途的风险。如果有下列任何情形，客户应在合理可行情况下尽快通知银行：
  - i. 客户得知或怀疑信用卡、客户名称、私人密码、流动保安编码密码（如适用）、保安编码器（如适用）及/或保安编码已遗失、被窃、受损害、被泄露给任何未获授权人士或被任何未获授权人士取得；
  - ii. 或有人用信用卡、客户名称、私人密码、流动保安编码密码（如适用）及/或保安编码作出任何未获授权的指示或交易；或
  - iii. 流动保安编码受到任何损害或未获授权的使用。
- 若客户未能在合理可行情况下尽快通知银行该等事情，或存在欺诈或严重疏忽行为，一切由他人使用任何信用卡、客户名称、私人密码、流动保安编码密码（如适用）、流动保安编码（如适用）及/或保安编码进行的交易及所引致的直接损失，可能需由客户负责。

客户重要通知

- 客户应对其所有作为和不作为负责，并应遵守相关申请表和网上银行服务的条款及条件。
- 如有诈欺行为，客户将须承担所有损失。
- 如果客户有重大过失（这可能包括客户故意允许他人使用其设备或身份验证资讯的情况），或在发现其用于登入网上银行服务的身份验证资讯或设备已被泄露、遗失或被盗，或在发现未经授权的交易后未能在合理可行的情况下尽快通知银行，则客户将须承担所有损失。
- 若客户未能遵守下列保障措施，则将承担所有损失：
  - i. 客户有义务采取合理措施确保用于登入的任何电子装置及网上银行服务（例如个人计算机、产生一次性密码的安全设备和储存数字证书的智能卡）或身份验证资讯（例如密码和保安编码）安全且保密。
  - ii. 客户必须采取合理措施确保其电子装置安全和其身份验证资讯保密（例如密码），以提防诈欺。
  - iii. 除此之外，应提醒客户：
    - a. 销毁密码的原始印刷本；

b. 采用生物识别凭据、流动保安编码或装置绑定作为启动相关交易（例如非接触式行动支付）作为身份验证资讯之一所涉及的风险，以及确保电子装置和身份验证资讯安全的相关保护措施；
c. 不应允许其他人使用他们的身份验证资讯；
d. 定期更改密码和流动保安编码密码（如适用）
e. 切勿将密码写在任何用于存取电子银行服务的电子装置上或通常存放着该电子装置或附近的任何物品上；
f. 不得在未经掩饰的情况下写下或记录密码；
g. 当他们发现其帐户出现异常或可疑交易后，应尽快通知银行；和
h. 需要确保他们在银行注册的联络方式是最新的，以便及时接收银行的重要通知（例如，用于在线支付的简讯和电子邮件通知）。

- 如果客户未采取本行或客户电子装置制造商不时告知或公布的任何安全措施，客户须对因使用网上银行服务而引致或与其相关的所有后果全权负责并承担所有责任。

5. 安全事件报告

- 如果客户的保安编码器或与流动保安编码绑定之流动装置遗失或被窃，客户应在合理可行情况下尽快拨打银行不时规定的电话号码通知银行，并在银行要求时作出书面确认。
- 如客户未能在合理可行情况下尽快向银行知会该等事项，或在其他情况下有欺诈或严重疏忽的行为，所有涉及任何人士使用其所失之保安编码器或与流动保安编码绑定的流动装置（视乎情况而定）所进行的未经授权交易而引致的直接损失，一律可能需由客户负责。银行补发新保安编码器或流动保安编码（如适用）时可收取费用。
- 客户可以透过以下任何一种方式向银行发出通知：
  i. 致电银行于银行网站或银行流动应用程序发布之 24 小时客户服务热线 +852 2779 5533;
  ii. 联络银行任何分行; 或
  iii. 银行不时通知的任何其他方法。

若本一般资料概要的英文版本和中文版本之间有任何不一致，则以英文版本为准。