电子银行[1]使用条件和安全须知

中国银行股份有限公司德国境内分行[2]为客户提供安全便捷的电子银行服务。为保证安全，电子银行客户须注意以下事项：

1 电子银行服务

账户所有人或被授权人（以下统称：客户）可以通过电子银行办理本行设定范围内的银行业务。此外，客户还可以通过电子银行查询其在本行的相关信息。电子银行交易的金额以客户与银行协定的交易限额为准。

2 使用电子银行的前提条件

客户应在银行开立一般活期存款账户，提交开通电子银行的申请书并签署协议。客户在通过电子银行办理业务时，需要使用个人安全工具（即密码）和认证工具（即 E-Token 动态口令牌）来验证身份（见第 3 条）及授权交易（见第 4 条）。

3 登录电子银行

客户登录电子银行需满足以下条件：

- 客户输入自己设定的用户名、密码、动态口令及验证码
- 客户的身份验证通过
- 客户的电子银行未被冻结

客户在登入电子银行系统后，即可执行查询或其他交易。

1 电子银行包括个人网上银行、个人手机银行以及公司网上银行。

2 中国银行股份有限公司德国境内分行（以下简称：本行/银行）包括中国银行股份有限公司法兰克福分行、杜塞尔多夫分行、汉堡分行、柏林分行和慕尼黑分行。

4 电子银行业务

4.1 业务办理和授权

客户在执行并授权电子银行业务（如汇款）时需要输入密码及动态口令。客户在提交业务后可以在电子银行查询到所提交业务的状态。

4.2 撤销业务

撤销不同种类的电子银行业务须遵守各业务单独的一般业务条款。撤销已提交的银行业务只能在银行网点办理。

5 电子银行业务处理流程

(1) 各类型的电子银行业务（如汇款业务）有其相应的操作受理时间，在电子银行操作时间（受理期限）之后或非营业时间收到的电子银行交易指令，我行会在下一工作日受理。

(2) 银行仅会执行满足以下条件的交易：

- 客户通过个人密码和认证工具验证身份成功
- 客户有办理该种类业务的权限
- 遵守电子银行的数据格式
- 没有超过协定的电子银行交易限额
- 满足根据各类业务的特殊适用条款设定的执行条件（比如有足够的账户余额，正确的 IBAN 及 BIC 码等）

(3) 如果上述执行条件不成立，银行将不会执行相关电子银行业务。同时本行会通过电子银行通知客户该业务不予执行，如果可能，会一并告知拒受理的原因，以及客户应该怎样修改。

6 交易限额

对于电子银行汇出汇款业务，我行交易限额如下：

❖ 私人客户：

- 单笔转账最高限额 30,000 欧元
- 每日累计最高限额 30,000 欧元

❖ 公司客户（针对每种汇款类型）：

- 单笔转账最高限额 2,000,000 欧元
- 每日累计最高限额 5,000,000 欧元

公司客户可以在我行规定的最高限额下单独设置限额。

7 客户的电子银行交易信息

本行至少每月一次通过与客户协定的方式告知其通过电子银行进行过的交易信息。此外客户也可以通过电子银行自行查阅电子银行交易的状态。

8 登录电子银行

客户有义务保证，只能通过输入以下网址登录网上银行：

http://www.boc.cn/de ,

http://www.bankofchina.com/de 或

https://ea.ebs.bankofchina.com/login.html?bn=FRA

客户有义务保证，仅在谷歌官方 App 市场或苹果官方 App 市场下载手机银行 App。

提示：

如果您将我行网上银行网址存储在浏览器的收藏夹中，请您登录之前检查该网址是否为真正的中国银行网址。

您可以通过 IE 浏览器菜单中“工具”>>“选项”>>“内容”>>“证书”，查看网址证书的有效性。

请小心识别虚假网站。若有任何怀疑，请立即通过拨打热线电话与我们联系。

识别虚假网站的方法：

虚假网站会利用各种手段，模拟我行网页，这些方法包括：

- 套用真正网站的图片

- 将客户转链接至真正的网站，让客户可正常登录网上银行，而不知道其个人数据已被虚假网站窃取
- 使用与真网站接近的域名， 容易与真实网站混淆

成功登陆后会显示欢迎界面，请仔细查看欢迎界面上的最后登陆时间是否正确。如果显示的最后登陆时间与您的记忆不符，就有可能是虚假网站或 App。

9 密码和动态口令的保密义务

客户有义务保证：

- 对自己的密码进行保密，并且只能在上文提到的渠道中使用，用于登录。
- 妥善保管自己的动态口令牌，以防他人窃取。

由于其他任何人，只要持有动态口令牌及客户密码，即可使用电子银行并执行业务。因此客户须特别注意以下事项:

- 不要将密码以电子形式存储（比如存在电脑中）。
- 在输入密码时候要确保，他人不能窥探到密码。
- 请勿在本行网上银行域名以外的地址输入密码（比如不要在在线购物网站）。
- 请勿在电子银行程序以外的地方传送密码，比如通过邮件。
- 请勿将密码和动态口令牌保存在一起。
- 请勿使用他人容易猜出的密码，比如生日、电话号码或者车牌号。请使用难以破解的字母和数字组合作为密码。
- 请勿将电子银行和其他网络服务项目（如邮箱）设置同样的密码。
- 客户应定期修改密码。
- 密码不应该写在纸张上。如果已将密码写在纸张上，则应妥善保管纸张，避免其他人获得（比如保存在保险箱里）。
- 请勿将登录用户名和银行账号等个人信息透露给可疑或身份不明的人员或网站。

10 安全行为

客户不可在网吧、图书馆等公共场所使用电子银行。陌生电脑可能有病毒，会窃取您的用户名和密码。另外，在公共场合使用电脑，容易被陌生人窥视。

请不要查看任何不明来历的电子邮件，也不能通过邮件链接登录网银。

客户在登录电子银行过程中离开电脑或者离开电子银行界面，须点击“退出”键退出登录并关闭浏览器。

在进行交易之前以及之后应检查账户余额，并同时建议您定期检查账户余额。如有异常，请立即拨打热线电话通知我们。

11 客户系统安全

建议您为自己所使用的计算机或智能手机设定密码，以防止他人擅自盗用您的资料。

客户应安装防火墙以防止他人对您所使用的电脑进行未授权的访问。此外应安装并定期更新杀毒软件，以免被计算机病毒及恶性程序入侵。

建议您确保网上下载的软件不是虚假软件，没有植入病毒。诈骗人员可能将欺诈软件隐藏在您从网上下载的某款软件当中。

建议您使用 Microsoft Internet Explorer 浏览器。

请您定期下载安装最新的操作系统和浏览器的安全补丁。

建议您每次操作完毕后清除浏览器里缓存和历史记录，这样可以保证您的账户信息不会遗留在该台电脑中。

建议您关闭“自动完成”功能以防您的登录数据遗留在该台电脑中：

1. 打开您的 Internet Explorer，点击“工具”>>“Internet 选项”>>“内容”
2. 在“设置”下点击“自动完成”
3. 去掉“表单上的用户名和密码”前面的勾并点击“清除密码”。

12 本行的沟通渠道

如果有紧急的安全问题银行会通过电子银行欢迎界面的信息提示您。

如果银行确定某一交易行为为欺诈交易或者当您已向本行举报了可疑交易行为时，我们将会通过电话或者书面形式通知您。

除我行官方登录界面之外，本行任何时候都不会要求您提供密码。

13 客户的告知和通知义务

一旦客户确认动态口令牌遗失、被盗、被冒用或客户发现其密码及动态口令被其他未经授权的人使用，应立即通知我行（即冻结告知）。

用户可以通过以下热线电话告知银行冻结电子银行用户权限：

- 营业时间[3]请拨打：+49 69 170090 0
- 非营业时间请拨打：+49 69 170090 777（请您通过选择按键 1-0-8 以便和我们的工作人员联系，我们提供英语和中文服务）

客户应立即向警方举报遭遇的盗窃或者冒用行为。

如您怀疑您的电子银行动态口令牌或密码丢失，建议您也及时与我行联系并冻结电子银行。客户在确认某一业务申请未经授权或者出现执行错误后，须立即通知银行。

如果您收到钓鱼邮件或者冒用我行名称的虚假网址，请通知我们。

14 冻结电子银行使用资格

14.1 由客户发出冻结通知

银行可应用户要求，特别是在用户发出冻结告知的情况下：

- 冻结客户的某一个或者全部电子银行用户名的登录权限
- 或者使动态口令失效

14.2 由银行发出的冻结

在下列情况下，银行有权利冻结用户的电子银行登录权限：

- 由于某些重大原因，在银行有相应许可的情况下解除与客户的电子银行合同
- 出于与保护动态口令或者密码安全有关的事实理由
- 或者怀疑某一交易未经授权或者有欺诈意图

[3] 营业时间：德国当地时间 星期一至星期四 9：00-12：00，13：00-16：00；星期五 9：00-12：00，13：00-14：30

银行须在冻结用户之前，或者最迟在冻结之后立即通知客户并告知冻结的主要原因。

14.3 自动冻结

当天输错 5 次密码，则银行将自动冻结当日的电子银行使用资格。累计连续 15 次输入错误密码，银行将正式冻结电子银行使用资格。解冻需要本人前往银行办理。

14.4 取消冻结

如果冻结的原因不再存在，银行将取消冻结或者重置密码以及动态口令，并且应该立即通知客户。客户可以拨打银行热线电话咨询如何取消冻结并且提交必要的书面授权材料。

15 责任规定

15.1 未授权的电子银行交易和没有执行或执行错误的电子银行交易情况下银行承担的责任

针对未授权的电子银行交易和没有执行或执行错误的电子银行交易，银行承担的责任遵循客户所操作的电子银行业务对应的业务条款。

15.2 在被他人冒用认证工具情况下的客户责任

15.2.1 在通知银行冻结之前发生的未经授权的支付业务中的客户责任

(1) 在动态口令牌遗失、被盗或者因其他原因丢失的情况下，如果在客户通知银行冻结之前，因他人盗用而产生了未经授权的支付业务，不论是否是由于客户原因造成了电子银行认证工具的丢失、被盗或因其他原因的丢失，客户应赔偿的金额至多为 50 欧元。

(2) 在动态口令牌没有遗失、被盗或者因其他原因丢失的情况下，但客户没有承担保护密码的责任，被他人未经允许而使用并在其通知银行冻结之前由此而产生了未经授权的支付业务，那么客户应赔偿的金额至多为 50 欧元。

(3) 如果客户为非个人消费者，因其疏忽或者故意违反本须知中规定的告知和注意事项而造成了未经授权的支付业务，则客户须赔偿所有损失，不管损失金额是否超过第（1）和第（2）条中规定的 50 欧元。

(4) 如果因为银行没有确保可以接收客户发出的冻结告知并因此而造成客户损失，那么即使客户没能向银行发出冻结告知，也无须承担第（1）、（2）和（3）条中所规定的损失。

(5) 如果在客户通知银行冻结之前业已发生未经授权的支付业务，且客户故意或者因重大过失而没有履行该须知中所规定的注意义务或者客户行为带有欺诈意图，则由客户承担由此产生的全部损失。

以下情形下，客户可能存在重大过失：

- 在客户获悉其认证工具或个人密码遗失、被盗、或被不当使用，但没有立即告知银行，
- 将密码存在电脑的用户系统中，
- 将密码透露给他人并因此被他人盗用，
- 在明显是本行网上银行域名以外的网页地址输入密码，
- 在电子银行程序以外的地方比如通过电子邮件透露了密码，
- 或者将密码标注在动态口令牌上或者将二者存放在一起。

(6) 对在客户和银行协定的交易限额期限内所产生的损失，赔偿金额不应高于协定的交易限额。

15.2.2 客户发出冻结通知后的银行责任

在收到客户的冻结通知后，本行将承担在冻结通知之后通过未授权的电子银行交易所造成的一切损失。但客户行为带有欺诈意图的情况除外。

15.3 免责条款

因意外的、不可预见的事件引发的责任纠纷，应归入免责范围。该类事件是指责任方对结果无法施加影响且即使注意也无法避免发生的不可抗力因素。

16 其他

我行会定期检验本安全须知的适用性，并及时根据法律发展更新本安全须知。客户可在中国银行法兰克福分行的网页上查阅最新版本的安全须知。请各客户经常阅读安全须知，提高自身的安全意识。

中文版本的客户安全须知仅供参考，具体以德文版本为准。