CG FINTECH

# 反洗钱和反恐怖主义融资政策

www.cgfintechfx.com
+ 971 4555 9581
support.en@CG FinTech

## 1. 引言

1.1. CG FinTech 致力于打击任何形式的洗钱、恐怖主义融资或犯罪活动，严格遵守相关适用的监管法规。

1.2. 我们的洗钱报告官（“官员”）和其他合规执行人员负责实施适当的反洗钱和反恐怖主义融资（“AML 和 CTF”）政策和程序。本 AML 和 CTF 政策将涵盖以下程序和流程：

(a) 客户尽职调查要求；

(b) 实施记录保存要求；

(c) 报告要求；

(d) 通知我们的官员和员工有关洗钱和恐怖主义融资的政策、流程、程序和系统；

(e) 培训我们的官员和员工识别和处理洗钱和恐怖主义融资活动；

(f) 对 CG FinTech 的官员和员工进行审查，以确保他们适合从事反洗钱和反恐怖主义融资相关工作；

(g) 官员的角色和职责；

(h) 建立独立审计职能，以测试 AML 和 CTF 的流程、程序和系统；

(i) 我们在处理洗钱和恐怖主义融资时采用的系统。

1.3. CG FinTech 已建立了一系列 AML 程序，并将在所有交易中应用我们的 AML 和客户了解（“KYC”）程序。我们将采取一切合理措施，确保存在适当的保护措施，以防止违反适用的法规，防止和减轻洗钱和恐怖主义融资（“ML 和 TF”）活动。遵守 AML 和 CTF 系统一直是我们首要的优先事项，以维护我们在全球金融行业和监管机构中的商业声誉。

1.4. 我们在实施 AML 和 CTF 系统时采取基于风险的方法，以便检测 ML 和 TF 风险。我们将至少每年更新一次 AML 和 CTF 系统和政策，以考虑新的和新兴的风险，包括：

(a) 我们在业务过程中可能面临的洗钱和恐怖主义融资风险的性质和程度；

(b) 我们业务的性质、规模和复杂性；

(c) 新产品和新业务实践的发展，包括新的交付机制；

(d) 对于新产品和现有产品的新或发展中的技术的使用。

## 2. 定义和解释

2.1. 以下术语应具有以下含义：

(a) “适用法规” 指：

I. 相关监管机构的法规、规则或命令；

II. 客户所在司法管辖区的相关监管机构的法规、规则或命令；

III. 相关金融交易所市场的规则；以及

IV. 适用于本政策的所有其他法律（及其不时修订）。

(b) “CG FinTech” 指以下适用的任何一个实体：

I. CGTrade (Mauritius) Limited，毛里求斯，公司注册号 166217，注册地为 The Cyberati Lounge, Ground Floor, The Catalyst, Silicon；

II. CG Trade Inc，注册地为 32F2+655, Castries - Gros Islet Hwy, Rodney Bay, St Lucia，公司编号 2024-00155。

(c) “政治公众人物”或“PEP” 指被赋予重要公共职能的个人，如国家元首、首相、部长、高级政治人物、高级政府官员、司法或军事官员、国有企业或国际组织的高级执行成员和政治党派官员。

www.cgfintechfx.com
+ 971 4555 9581
support.en@CG FinTech

(d) “犯罪收益” 指直接或间接来源于严重犯罪的财产，包括：

(i) 任何直接来源于犯罪的财产之后转化或改变的财产；以及

(ii) 自犯罪发生以来从该财产中获得的收入、资本或其他经济收益。 如果犯罪收益（原始收益）与其他财产混合，且无法轻易分离，则整个财产中原始收益所占的比例视为犯罪收益。

(e) “扩散融资” 指提供资金或金融服务，用于制造、获得、持有、开发、出口、转运、中介、运输、转移、储存或使用核武器、化学武器或生物武器及其运载工具及相关材料（包括用于非法目的的技术和双重用途商品），违反国家法律或（如适用）国际义务的行为。

(f) “相关监管机构” 指适用于 CG FinTech 业务操作和服务提供商的相关监管机构，包括但不限于美国证券交易委员会、美国金融业监管局、英国金融行为监管局、澳大利亚证券和投资委员会、欧洲证券和市场管理局、塞舌尔金融服务管理局、毛里求斯金融服务委员会、瓦努阿图金融服务委员会等。

(g) “财富来源” 指个人全部财富（即总资产）的来源。

(h) “资金来源” 指个人与我们之间的业务关系中，特定资金或其他资产的来源（例如，作为业务关系的一部分被投资、存入或转账的金额）。

(i) “恐怖主义融资” 指：

I. 以任何方式直接或间接提供或收集任何财产：

(aa) 意图将财产用于；或

(ab) 知道该财产将被用于（无论该财产是否实际被用于），以实施一个或多个恐怖行为

II. 以任何方式直接或间接向或为某人提供财产或金融（或相关）服务，知道或疏忽地不考虑该人是否是恐怖分子或恐怖分子相关人士；或

III. 以任何方式直接或间接为某人收集财产或 soliciting financial（或相关）服务，知道或疏忽地不考虑该人是否是恐怖分子或恐怖分子相关人士。

www.cgfintechfx.com
+ 971 4555 9581
support.en@CG FinTech

## 3. 洗钱

3.1. 洗钱的阶段如下：

(a) 布置 - 处理来自非法活动的现金收益；

(b) 分层 - 通过创建复杂的金融交易层来分离非法收益的来源，伪装资金来源、规避审计痕迹并提供匿名性；

(c) 整合 - 创建明显合法的印象，以合法化犯罪来源的财富。在分层过程成功的情况下，整合方案有效地将洗钱收益重新融入一般金融系统，收益看似来自合法业务活动。

3.2. 一些可能的洗钱迹象包括但不限于：

(a) 客户不愿意提供信息；

(b) 客户提供的信息不完整或不一致；

(c) 不规则的资金转账和交易；

(d) 无解释的第三方投资；

(e) 交易量异常高；

(f) 资金来源于监管不力的来源；

(g) 无明显合法或经济目的的交易；

(h) 交易不必要地复杂；

(i) 客户的生活方式超出已知收入来源；

(j) 商业结构不必要地复杂；

(k) 无有效理由使用银行账户；

(l) 客户似乎在为另一个实体或个人行事，但对另一方的身份含糊其辞；

(m) 客户在一个名字下有多个账户或多个名字下有多个账户，且账户之间有大量的转账；

(n) 客户存入资金后请求提取资金。

## 4. 客户尽职调查（“CDD”）

4.1. CG FinTech 已建立 KYC 政策以验证所有客户的身份，并进行客户尽职调查（“CDD”）。我们执行持续的尽职调查流程，以监控客户的账户、服务或与我们的业务关系，以识别、减轻和管理我们可能面临的涉及洗钱、恐怖主义融资或其他严重犯罪的风险。

4.2. 我们在以下情况下执行 CDD：

(a) 个人在我们处开设账户；

(b) 个人使用我们的服务；或

(c) 个人与我们建立业务关系。

4.3. 我们在以下情况下执行 CDD：

(a) 进行交易的个人；

(b) 代表他人进行交易的个人；以及

(c) 实际控制人； 如果我们有合理理由相信个人代表另一方进行交易。我们将验证该个人是否被授权代表他人进行相关交易。

4.4. 此外，我们在以下情况下执行 CDD：

(a) 在与客户建立业务关系之前；

(b) 在客户进行涉及等于或超过 USD2,000.00 或其等值外币的大额现金交易或国际货币转账时，无论是单次操作还是多个操作，如果我们合理认为它们是相关的。在确定交易是否相关时，我们将考虑第 9.6 条款的因素与交易的时间框架；

(c) 当我们被相关监管机构、支付服务提供商或服务提供商要求执行适当的 CDD 时；

(d) 当我们为客户执行电子货币转账时；

(e) 当我们怀疑客户涉及犯罪收益、恐怖主义融资或严重犯罪时，无论交易水平如何；

(f) 当我们怀疑客户的资金来源来自第三方时；

(g) 当我们怀疑交易涉及犯罪收益，或可能用于恐怖主义融资或实施严重犯罪时；

(h) 当我们对客户身份或之前获得的信息的真实性或充分性存有疑问时；

(i) 在执行我们的常规 CDD 流程时。

4.5. 所需文件清单：

4.5.1. 如果客户是个人，我们将收集以下信息：

(a) 客户的全名；

(b) 客户的出生日期；

(c) 客户的住址；

(d) 客户的职业；

(e) 客户的国籍；

(f) 客户的居住国家；

(g) 客户的职业或业务活动；

(h) 客户与我们之间关系的性质和目的，包括：

I. 具体交易的目的；或

II. 预期的交易行为的性质和水平；

(i) 授权任何声称代表客户行事的人的授权；

(j) 客户的收入或资产；

(k) 客户的资金来源，包括资金的来源；

(l) 客户的财务状况；

(m) 客户使用资金的实际控制人；以及

(n) 客户交易的受益人，包括资金的去向。

4.5.2. 如果客户是外国注册的公司，我们将收集以下信息：

(a) 外国公司的全名；

(b) 客户的注册国家和完整注册细节；

(c) 公司主要营业地点和注册地址的完整地址；

(d) 公司结构；

(e) 每位公司董事和秘书的姓名；

(f) 公司开展的业务活动的性质；

(g) 公司实际控制人和控制结构的姓名和地址；

(h) 公司成立、注册或注册的国家；

(i) 规定约束客户的权力的条款；

(j) 授权任何声称代表客户行事的人的授权和身份；

(k) 与我们建立业务关系的目的和预期性质。

4.6. 我们严格禁止与使用虚假、虚构或误导性名字的客户建立任何业务关系，并记录任何客户使用不同于客户普遍已知名字的情况。

4.7. 对于无法合理提供标准身份证据的客户，我们将根据具体情况考虑并寻求同意使用其他身份确认，以免客户无法合理地获得产品和服务。如果合理证明对实际控制人的身份和验证存在疑问，我们可能会根据本 AML 和 CTF 政策对客户的高级管理人员进行 CDD。

## 5. 客户风险评估（“CRA”）

5.1. CG FinTech 将采用基于风险的方法进行客户风险评估。我们会考虑具体产品、服务、客户、实体、交易数量、交易量、客户关系的性质、地理位置、账户或关系的目的、涉及的资产水平、交易的规模以及业务关系的规律性或持续时间等因素来评估每个客户的风险。

5.2. 我们不会接受以下识别为高风险的客户：

(a) 处理大量现金或复杂异常大交易且无法核实的客户。

(b) 在短时间内进行大额一次性交易或同一账户进行多次交易的客户。

(c) 位于或通过高风险司法管辖区进行业务的客户，或在已知腐败、组织犯罪、武器或毒品生产、分销、储备或获取水平较高的司法管辖区进行业务的客户。

(d) 符合 PEP 定义的客户。

(e) 资金来源无法核实的交易。

(f) 目的或合法性不明显的交易。

(g) 可能有利于匿名性的交易。

5.3. 我们将在客户尽职调查（CDD）的初始阶段进行客户风险评估，以确定需要实施的 CDD 措施的程度和持续监控措施。随后，我们将采取基于风险的方法进行持续监控，以管理和减轻洗钱及恐怖融资风险，并确保所有相关信息得到更新。客户风险评估框架应与 CG FinTech 与客户业务的性质和规模相称。

5.4. 当我们有合理的怀疑理由时，将要求客户识别和核实交易的来源或目的地。

5.5. 我们进行机构洗钱/恐怖融资风险评估的步骤包括：

(a) 记录风险评估过程，包括通过定性和定量分析以及从相关内部和外部来源获得的信息，识别和评估相关风险；

(b) 在确定整体风险水平以及适用的缓解措施之前，考虑所有相关的风险因素；

(c) 获得高级管理层对风险评估结果的批准；

www.cgfintechfx.com
+ 971 4555 9581
support.en@CG FinTech

(d) 设立更新风险评估的流程；

(e) 在必要时提供风险评估给相关监管机构。

## 6. 简化尽职调查（“SDD”）

6.1. 如果 CG FinTech 确定洗钱和恐怖融资风险较低，CG FinTech 可以采用简化尽职调查（“SDD”）方法。

6.2. 可以应用 SDD 的客户包括：

(a) 财务机构；

(b) 具有下列条件的机构：

(i) 在等效司法管辖区注册或成立；

(ii) 从事类似财务机构的业务；

(iii) 由该司法管辖区的监管机构监督，监督职能类似于任何监管机构；

(c) 在任何证券交易所上市的公司；

(d) 投资工具，其中负责执行类似 CDD 措施的人员是：

I. 财务机构；

II. 注册或成立的机构，该机构：

1. 采取措施确保遵守类似适用法规和条例的要求；

2. 由监管机构监督这些要求的遵守情况；

(e) 政府或任何公共机构；

(f) 等效司法管辖区的政府或从事类似公共机构职能的机构。

6.3. 在 SDD 的情况下，我们将：

(a) 识别客户并核实客户的身份；

(b) 如果建立业务关系且其目的和预期性质不明显，获取有关业务关系的目的和预期性质的信息；

(c) 如有人声称代表客户行动，

I. 识别该人并采取合理措施核实该人的身份；

II. 核实该人代表客户行事的授权。

## 7. 加强尽职调查（“EDD”）

7.1. 如果 CG FinTech 确定洗钱和恐怖融资风险较高，CG FinTech 将采用加强尽职调查（“EDD”）方法和加强持续监控。在与高风险客户进行或继续业务关系和/或交易之前，需要获得 CG FinTech 高级管理层的批准。

7.2. 适用于 EDD 的高风险情况包括：

(a) 客户风险因素：

(i) 业务关系在异常情况下进行（例如，我们与客户之间存在显著的不明地理差异）；

(ii) 涉及没有明确合法商业目的的壳公司或法律安排；

(iii) 拥有代名股东或持有记名股的公司；

(iv) 现金密集型业务；

(v) 法人或法律安排的所有权结构看起来不寻常或过于复杂，考虑到法人或法律安排的业务性质；

(vi) 客户或客户的最终受益人是 PEP 或外国 PEP

(b) 产品、服务、交易或交付渠道风险因素：

(i) 匿名交易（可能涉及现金）；或

(ii) 从未知或未关联的第三方收到的频繁付款。

(c) 国家风险因素。我们严格禁止与高风险国家的客户进行所有交易、银行转账和业务往来，包括但不限于：

(i) 被可信来源（例如相互评估或详细评估报告）识别为未具备有效 AML 和 CTF 系统的国家或地区；

(ii) 财务行动特别工作组（FATF）识别的国家；

(iii) 被可信来源识别为具有显著腐败或其他犯罪活动的国家或地区；

(iv) 被联合国等发出的制裁、禁运或类似措施所涉及的国家或地区；

(v) 被可信来源识别为提供资金或支持恐怖活动的国家、地区或地理区域，或已指定恐怖组织在其运作的国家。

7.3. CG FinTech 保留从独立来源获取信息以进行加强尽职调查的权利。这包括但不限于：

(a) 获取客户的额外信息（例如职业、资产规模、所有权和控制结构、客户或最终受益人的声誉、通过公共数据库、互联网等获得的信息），并更频繁地更新客户和最终受益人的识别数据；

(b) 获取有关业务关系和交易的预期性质、目的和背景的额外信息；

(c) 获取客户资金来源或财富来源的信息；

(d) 获取有关预期或已执行交易的理由的信息；和/或

(e) 要求第一次付款通过客户名下的银行账户进行，该账户须符合类似的 CDD 标准。

7.4. 我们的 EDD 包括

(a) 增加为客户尽职调查目的获取的信息数量：

(b) 关于客户或最终受益人的身份或所有权和控制结构，以确保对关系的风险有充分了解。这可能包括获取和评估关于客户或最终受益人的声誉的信息，并评估对客户或最终受益人的任何负面指控。例子包括：有关家庭成员和亲密商业伙伴的信息；有关客户或最终受益人过去和现在的商业活动的信息；以及不利媒体搜索；

(c) 关于业务关系的预期性质，以确定业务关系的性质和目的是否合法，并帮助公司获得更全面的客户风险档案。这包括获取以下信息：

I. 可能通过账户的交易数量、规模和频率，以便发现可能引起怀疑的偏差，必要时请求证据；

II. 客户为何寻求特定产品或服务，特别是当不清楚为何客户的需求不能通过其他方式或不同司法管辖区更好地满足时；

III. 资金的去向；

IV. 客户或最终受益人的业务性质，以更好地理解业务关系的可能性质。

(d) 增加为客户尽职调查目的获取的信息质量，以确认客户或最终受益人的身份，包括：

(a) 要求第一次付款通过客户名下的可核实银行账户进行；

(b) 确认客户的财富来源和用于业务关系的资金来源不是犯罪活动的收益，并且与我们对客户及其业务关系的了解一致。资金或财富来源可以通过所得税申报表、审计账目副本、工资单、公共契约或独立可信的媒体报道等进行验证；

(c) 增加审核频率，以确保我们继续能够管理与单一业务关系相关的风险，并帮助识别需要进一步审查的交易，包括：

I. 增加业务关系的审核频率，以确定客户的风险档案是否发生变化以及风险是否仍可管理；

II. 获取官员/指定官员的批准，以开始或继续业务关系，以确保高级管理层了解我们所面临的风险，并能够对管理该风险的程度做出知情决定；

III. 更加定期地审查业务关系，以确保任何客户风险档案的变化得到识别、评估，并在必要时采取行动；

IV. 进行更频繁或深入的交易监控，以识别可能引起洗钱或恐怖融资怀疑的异常或意外交易。这可能包括确定资金去向或核实某些交易的原因；

(d) 官员需要在进行任何与通过加强尽职调查程序的客户的业务之前提供批准或拒绝。

7.5. 我们将对任何被认为是高风险的情况、客户或交易应用 EDD 措施。

7.6. 资金来源和财富来源

(a) 财富来源指的是个人所有财富（即总资产）的来源。

(b) 资金来源指的是特定资金或其他资产的来源，这些资金或资产是个人与我们之间业务关系的主题（例如，作为业务关系的一部分被投资、存入或转账的金额）。

7.7. 资金来源和财富来源措施如何纳入我们的 EDD 流程

(a) 财富来源通常会表明客户应有的财富规模，以及个人如何获得这些财富的情况。虽然我们可能没有关于未存入或未处理的资产的具体信息，但可以从个人、商业数据库或其他公开来源收集一般信息。

(b) 资金来源信息不应仅限于知道资金可能来自哪里，还应了解产生资金的活动。获取的信息应具备实质性，并建立资金来源或获取原因。

7.8. CG FinTech 的政策是不接受来自任何第三方的资金，但在发生特殊情况时，我们将进行 EDD 以识别和核实其最终受益人，包括法人、合伙企业、信托和其他法律安排。

## 8. 验证

8.1. 我们将在建立客户关系之前，通过客户服务和风险管理部门验证和筛选客户信息。我们的 CDD 范围包括但不限于零售客户、业务合作伙伴、董事会成员、股东和最终受益人。我们进行以下 CDD 措施：

(a) 通过独立筛选系统识别、验证和筛选客户的身份和信息；

(b) 如果涉及最终受益人，识别并采取合理措施以验证最终受益人的身份，以确保我们了解最终受益人是谁，包括在客户为法人或信托的情况下，采取措施了解法人或信托的所有权和控制结构；

(c) 获取与我们建立的业务关系的目的和预期性质的信息（如果目的和预期性质不明显）；

(d) 如果有人声称代表客户行动：

i. 识别该人，并使用可靠和独立来源提供的文件、数据或信息采取合理措施以验证该人的身份；

ii. 验证该人代表客户行事的授权；

(e) 如果我们认为身份验证不足或需要与客户交易相关的附加细节，我们保留要求客户提供额外细节的权利（包括但不限于银行对账单、银行账户证明、电子钱包或电子货币对账单），并保留不建立业务关系或继续进行任何交易的权利。如果客户拒绝提供所需的信息，或提供虚假/误导性信息，我们可能会冻结客户账户、限制交易或账户活动、终止业务关系和/或报告给监管机构。在确认客户身份和交易细节后，所有账户上的限制将被解除。

8.2. 在身份验证过程中，我们将请求原件的副本和带颜色的扫描副本；如果我们认为必要，也可能要求提供多个身份文件以进行交叉验证。

8.3. 当使用电子验证或客户未亲自出席进行身份验证时，我们将进行额外的验证检查以管理冒充欺诈的风险。此检查可能包括：

(a) 要求首次付款通过客户名下的受监管信用机构的账户进行；

(b) 在开设账户之前，通过验证的家庭或商务电话号码与客户进行电话联系；

(c) 与已验证的地址上的客户进行沟通；

(d) 要求将副本文件由适当人员认证。

8.4. 如果我们无法对某人进行规定的身份验证过程，我们将：

(a) 不为该人开设账户；

(b) 不与该人建立业务关系；

(c) 如果已经存在业务关系，我们将终止现有的业务关系。

www.cgfintechfx.com
+ 971 4555 9581
support.en@CG FinTech

## 9. 报告

9.1. 如果在 14 个工作日内（如果涉及第 4.4(d)和(e)条款，则为 2 个工作日）未能提供或获得满意的身份或验证证据，我们将向相关监管机构提交可疑活动报告。在没有监管机构的指示之前，我们将不继续进行该交易。

9.2. 如果我们合理怀疑客户不是其所声称的身份，我们将在该情况发生后的 3 个工作日内采取以下一个或多个行动：

i. 收集必要的客户识别信息；

ii. 从可靠和独立的来源验证关于客户的某些信息，以确保合理满意地确认客户的真实身份。

9.3. 在确定和实施适当的基于风险的系统和控制措施时，我们将考虑客户业务的性质、规模和复杂性以及我们可能面临的洗钱和恐怖融资风险，包括但不限于以下因素：

(a) 客户类型，包括 PEP；

(b) 提供的指定服务类型；

(c) 我们提供指定服务的方式，包括任何新产品、业务实践和新兴技术的开发；

(d) 我们处理的外国司法管辖区，包括金融行动特别工作组（FATF）识别的高风险司法管辖区。

9.4. 如果发生以下任何事件：

(a) 可疑交易；

(b) 可疑活动；

(c) 洗钱实体进行的交易；

(d) 涉及恐怖分子的财产的交易；

(e) 没有合法目的的交易；

(f) 我们的监督机构或审计师有合理理由怀疑交易或尝试交易或其掌握的信息涉及犯罪所得或与恐怖融资有关；

(g) 第 3.2 条款描述的任何交易；

(h) 该交易应暂停，未经主管授权不得继续进行。我们的前线员工应立即向主管报告任何可疑交易或活动，主管将根据需要在 2 个工作日内向相关监管机构提交可疑活动或可疑交易报告。

9.5. 如果识别出洗钱的可疑迹象，该交易应暂停，未经主管授权不得继续进行。在进行适当调查后，主管将向相关监管机构报告，如果我们认为存在潜在的严重洗钱和恐怖融资风险。如果我们认为某人进行 2 次或更多次交易以规避第 4.4(b)条款描述的金额阈值，我们应向相关监管机构提交可疑交易报告。在提交报告之前，我们将考虑以下因素：

(a) 交易的方式和形式；

(b) 每笔交易涉及的货币金额；

(c) 交易中涉及的货币总额；

(d) 交易发生的时间段；

(e) 交易之间的时间间隔；

(f) 发起或进行交易的地点；

(g) 相关人员对交易方式或形式的任何解释。

9.6. 处理可疑活动报告和可疑交易报告的程序

9.6.1. 在进行适当调查后，主管将考虑是否向监管机构报告该事项。所有与主管和相关机构有关的记录应由主管保留，期限不低于监管机构关闭该事项后的 7 年。可疑活动报告或可疑交易报告应包括：

(a) 涉及可疑活动或交易的个人或实体的个人信息和联系方式；

(b) 可疑活动或交易的详细信息；

(c) 观察到的可疑活动或交易指标；

(d) 在询问交易或活动时，相关人员提供的任何解释。

9.6.2. 向相关监管机构提交可疑活动报告或可疑交易报告提供了对报告中披露的洗钱和恐怖融资行为的法定辩护，前提是：

(a) 可疑活动报告或可疑交易报告在我们进行披露行为之前提交，并且这些行为或交易在相关监管机构的同意下进行；或

(b) 可疑活动报告或可疑交易报告在我们完成披露行为或交易后提交，并且该报告是我们主动提交的，并在合理时间内完成。

9.7. 所有通知将严格保密。然而，请注意，可能会有情况要求我们揭示个人身份，例如当法律要求时，因此无法保证匿名性。

9.8. 我们意识到，若某人知道或怀疑已经向相关监管机构披露了信息，若其向其他人披露任何可能妨碍随后的调查的事项（通常称为“提示”），是违法的。客户对可能的可疑活动报告、可疑交易报告或调查的了解可能会妨碍未来调查涉嫌洗钱和恐怖融资行为的努力。因此，如果我们怀疑涉及洗钱和恐怖融资的交易，我们将在进行 CDD 过程时考虑“提示”的风险。我们将确保员工在进行 CDD 时了解并敏感于这些问题。

9.9. 我们不会向任何其他人披露：

(a) 我们、我们的监督机构或审计师或其他人对交易或尝试交易或活动或尝试活动形成的怀疑；或

(b) 根据适用法规和条例向相关监管机构提交的报告；或

(c) 根据适用法规和条例提供给相关监管机构的信息；或

(d) 任何其他信息，从中任何信息接受者可能合理地推断出第(a)-(c)条款中的任何情况。

9.10. 第 9.9 条款不适用于以下披露：

(a) 向 CG FinTech 的官员、员工或代理人披露，他们已经或需要根据适用法规和条例提交报告或提供信息，与履行职责相关；或

(b) 向律师披露，以便获得关于该披露的法律意见或代表；或

(c) 向 CG FinTech 的监督机构披露；或

(d) 向执法机构或任何其他协助相关监管机构的人士披露。

9.11. 我们的主管的职责包括但不限于以下内容：

(a) 审查所有内部可疑交易报告和异常报告，并根据所有可用信息决定是否需要向相关监管机构提交可疑活动报告或可疑交易报告；

(b) 保留所有与此类内部审查相关的记录；

(c) 指导员工如何避免“提示”，如果提交了任何可疑活动报告或可疑交易报告；

(d) 根据适用法规和条例作为与相关监管机构、执法机构和其他主管部门在洗钱和恐怖融资预防、检测、调查或合规方面的主要联系点。

## 10. 持续 CDD 和交易监控

10.1. 我们将通过持续 CDD 和交易监控进行持续监控，以确保遵守 AML 和 CTF 系统。我们将在触发事件发生时审查现有 CDD 记录，并维护足够的系统以根据采用的风险基础方法监控交易。监控的程度应与客户的洗钱和恐怖融资风险档案成比例。

10.2. 持续 CDD

10.2.1. 我们通过以下方式持续监控客户活动：

(a) 定期审查与客户有关的文件、数据和信息，以确保其最新和相关；

(b) 对客户进行的交易进行适当的审查，以确保这些交易与我们对客户的了解、客户的业务、风险档案和资金来源一致；

(c) 识别复杂、金额异常大或模式异常的交易，或没有明显经济或合法目的的交易，这些交易可能表明洗钱和恐怖融资。

10.2.2. 所有客户的审查频率应为：

(a) 高洗钱和恐怖融资风险的客户应每 6 个月审查一次；

(b) 中等洗钱和恐怖融资风险的客户应每年审查一次；

(c) 低洗钱和恐怖融资风险的客户应每 2 年审查一次；

或如果我们认为必要，进行更频繁的审查，以确保保留的 CDD 信息与我们对客户、客户业务、资金来源和风险档案的了解一致。

10.2.3. 所有被归类为高风险的客户将接受全面审查。这将包括：

(a) 重新确认地址

(b) 重新确认公司结构（如适用）

(c) 重新确认资金和财富来源

(d) 进行负面新闻筛查

(e) 完整审查交易档案，包括请求的新产品

10.3. 交易监控

10.3.1. 我们维护足够的系统以基于风险的方式监控和审查所有交易，我们将检查和审查交易是否正常，基于以下因素：

(a) 业务的规模和复杂性；

(b) 业务中产生的洗钱和恐怖融资风险；

(c) 系统和控制的性质；

(d) 为满足其他业务需求而已经存在的监控程序；

(e) 提供的产品和服务的性质（包括交付或沟通方式）。

10.3.2. 我们定期审查交易监控系统和流程的充分性和有效性，包括采用的参数和阈值。采用的参数和阈值包括以下因素：

(a) 交易的性质和类型（例如，异常大小或频率）；

(b) 一系列交易的性质（例如，将单笔交易拆分为若干现金存款）；

(c) 交易的对手方；

(d) 支付或收款的地理来源/目的地；

(e) 客户的正常账户活动或营业额；

(f) 客户的行为 - 交易活动的突然和/或显著变化，如受益人或目的地的变化；

(g) 客户的关联关系 - 识别看似不相关的账户或客户中的共同受益人和汇款人。

## 11. 记录保存

11.1. 我们将以保密的方式编制、组织并保存所有原始和复印的身份验证文件、交易记录、客户尽职调查（CDD）信息、向官员报告的反洗钱（ML）和反恐融资（TF）报告、与可疑活动报告、可疑交易报告相关提交的所有文件、处理可疑交易报告的员工、可疑交易报告的结果以及其他必要的文件。这些记录将在与客户的业务关系结束后至少保存 7 年。

11.2. 客户相关记录保存要求

(a) 我们必须保留以下文件的原件或复印件：

i. 在识别和验证客户的身份、客户的实际拥有者以及声称代表客户行事的人的过程中获得的数据和信息记录；以及

ii. 与客户的业务关系以及与客户和任何实际拥有者的业务往来相关的文件；

(b) 上述(a)项所提到的文件和记录必须在与客户的业务关系期间保持有效，并且从业务关系结束之日起至少保存七年。

11.3. 交易相关记录保存要求

11.3.1. 我们将保留与每笔交易相关的文件的原件或复印件以及获得的数据和信息记录，包括但不限于以下内容：

i. 交易的性质；

ii. 交易的金额及其货币；

iii. 交易进行的日期；

iv. 每个人的姓名、地址及职业、业务或主要活动，如下：
(aa) 进行交易的人；以及

(ab) 交易是为谁进行的，或为谁的最终利益进行的，如果我们有合理理由相信该交易是代表其他人进行的；

v. 与交易相关的任何账户/服务的类型和识别号码；

vi. 如果交易涉及除货币以外的可流通票据：

(aa) 票据的出票人；

(bb) 票据所绘制的机构名称；

(cc) 收款人名称（如有）；

(dd) 票据的金额和日期；以及

(ee) 票据的编号（如有）和票据上出现的任何背书细节；

vii. CG FinTech 的名称和地址，以及准备相关记录或记录部分的 CG FinTech 的每位官员、员工或代理人的名称和地址；

viii. 与该交易相关的任何其他信息。

11.3.2. 根据 (a)项要求保留的记录必须从交易完成之日起至少保存七年，无论业务关系是否在此期间结束。

## 12. 反洗钱（AML）和反恐融资（CTF）筛查程序

12.1. 筛查和监控

客户将通过 Refinitiv Limited 的 World-Check One 筛查系统与制裁名单、政治暴露人士、监管执行、执法、洗钱、恐怖融资、不利媒体报道进行筛查。客户将被添加到 World-Check One 的持续监控列表中，其详细信息将每 12 小时由系统自动搜索一次。当出现任何正面匹配时，我们将收到警报。

12.2. 筛查程序

我们筛查：

(a) 在建立关系时，客户及其任何实际拥有者与当前数据库进行筛查；

(b) 客户及其任何实际拥有者与数据库中的所有新标识和更新标识进行筛查，尽快处理；以及

(c) 跨境电汇中的所有相关方在执行转账前与当前数据库进行筛查。

12.3. 报告怀疑

如果有任何恐怖融资、扩散融资和制裁违规的怀疑，我们将向相关监管机构提交可疑活动报告或可疑交易报告。我们将报告任何被冻结的资产或按照金融制裁要求采取的行动，并向相关监管机构提交可疑活动报告或可疑交易报告。

## 13. 反洗钱（AML）和反恐融资（CTF）审计功能

13.1. 年度内部审计

官员和合规部门将每年对我们的 AML 和 CTF 政策进行内部审计，以确保政策得到更新。我们意识到遵守适用法规的法定责任，并且将每年至少更新和审查一次我们的 AML 和 CTF 政策。

13.2. 风险评估

我们将定期识别和评估可能出现的洗钱和恐怖融资风险，包括：

(a) 我们在业务过程中可能合理预期面临的洗钱和恐怖融资风险的性质和水平；

(b) 我们业务的性质、规模和复杂性；

(c) 新产品和新业务实践的发展，包括新的交付机制；

(d) 对新技术或发展中技术的使用，无论是新产品还是现有产品。

## 14. 培训计划

14.1. 培训提供

CG FinTech 的所有相关员工将接受本 AML 和 CTF 政策提供的相关政策和知识培训。此外，所有相关员工还将了解其职位描述，并接受有关洗钱和恐怖融资交易的责任培训。他们将被指导如何识别和处理可能涉及洗钱和恐怖融资的交易。

14.2. 培训范围

14.2.1. 员工将了解到：

(a) 我们的法定义务和他们的法定义务以及未报告可疑交易的可能后果；

(b) 适用法规和规定下与我们相关的其他法定和监管义务，以及违反这些义务的可能后果；

(c) 我们与 AML 和 CTF 相关的政策和程序，包括可疑活动和交易的识别和报告；

(d) 员工在履行其与 AML 和 CTF 相关的角色时需要了解的新兴技术、方法和趋势；

(e) 升级程序，即一旦识别出 AML 和 CTF 风险后应采取的行动；

(f) 员工在我们合规工作中的角色及其执行方式；

(g) 记录保存和记录保留政策；

(h) 不遵守适用法规的纪律处分（民事和刑事）

14.2.2. 针对特定员工的培训

(a) 新员工（无论职位高低）

I. 介绍洗钱和恐怖融资的背景以及 AML 和 CTF 对我们的重要性；

II. 识别和报告可疑交易的必要性和义务，以及“告密”犯罪。

(b) 前线员工（即直接接触客户的员工）

I. 他们在公司 AML 和 CTF 战略中的角色的重要性，作为潜在洗钱者和恐怖融资人员的第一接触点；

II. 与 CDD 和记录保存要求相关的公司政策和程序；

III. 在不同情况下识别异常活动的指导或技巧，这些情况可能引发怀疑；

IV. 报告异常活动的相关政策和程序，包括报告线和可能需要额外警惕的情况。

(c) 后台员工

I. 有关客户验证和相关处理程序的适当培训；

II. 识别异常活动的方法，包括异常结算、支付或交付指令。

(d) 管理层（包括内部审计人员）

I. 涵盖 AML 和 CTF 制度所有方面的高级培训；

II. 针对我们的 AML 和 CTF 要求的具体培训；

III. 监督或管理员工、审计系统、执行随机检查以及向相关监管机构报告可疑交易的职责相关的具体培训。

(e) 官员

I. 关于官员职责的具体培训，包括评估提交的可疑交易报告和向相关监管机构报告可疑交易；

II. 保持对 AML 和 CTF 要求/发展的一般了解的培训；

III. 接收公司人员的可疑活动报告；

IV. 与适当员工协调所需的 AML 审查/会议。

14.3. 培训效果监测

我们将通过以下方式监测培训的有效性：

(a) 测试员工对 AML 和 CTF 政策和程序的理解，对其法定和监管义务的理解，以及识别可疑交易的能力；

(b) 监测员工对我们 AML 和 CTF 系统的遵守情况以及内部报告的质量和数量，以便识别进一步培训需求并采取适当行动；

(c) 监控培训出勤情况，并跟进缺席培训的员工。

14.4. 培训频率

我们将每年至少为所有相关员工进行 AML 培训、研讨会和评估。

14.5. 培训记录

我们将观察并记录已接受充分培训的员工，培训的时间或最后一次培训的时间，并在此后提供额外的、必要的和充分的培训。

## 15. 语言和修订

15.1. 官方语言

本 AML 和 CTF 政策的官方语言为英语。CG FinTech 可以提供其他语言版本的政策仅供参考，如英语版本与其他语言版本存在不一致或差异，以英语版本为准。

15.2. 政策修订

客户承认 CG FinTech 保留随时修改或更新本 AML 和 CTF 政策的权利，恕不另行通知客户。AML 和 CTF 政策的修订将立即生效，并在 CG FinTech 网站上发布后对客户具有法律约束力。客户承诺定期在 CG FinTech 网站上查看本 AML 和 CTF 政策。

*(本页其余部分故意留空)*