02 FEB 2022

Statement on inspection in GC Exchange A/S

(The Area Of Anti-Money Laundering)

Introduction

In January 2022, the Danish Financial Supervisory Authority conducted an inspection at GC Exchange A/S (the company). The inspection was an examination of the area of anti-money laundering. It covered the company's customer due diligence and monitoring, including high-risk customers and transactions, as well as the company's handling of alerts and reporting to the Money Laundering Secretariat.

The company offers services with virtual currency (VASP) and currency exchange operations. The inspection was limited to examining the company's offering of services with virtual currency.

Risk Assessment

The Company facilitates cryptocurrency trading, primarily involving Bitcoin and Ethereum, by offering:

- Exchange between fiat currencies and virtual currencies
- Exchange between different types of virtual currencies
- Transfer of virtual currencies

The Company primarily services business customers.

National Risk Context

- The Money Laundering Secretariat's 2022 National Risk Assessment identifies crypto-assets as a significant money laundering risk area,concluding that criminal actors are highly likely to increase the use of crypto-assets for laundering illicit proceeds.
- The Danish Security and Intelligence Service's (PET) 2022 National Risk Assessment of Terrorist Financing highlights cryptocurrencies as a high-risk channel for terrorist financing, due to their speed, lack of geographic limitations, and the existence of obfuscation mechanisms (e.g., mixers, privacy coins).

Given these factors, the Company's services are considered inherently high-risk in relation to money laundering and terrorist financing.

The inspection revealed the following:

Risk Assessment

•The Company has prepared a written risk assessment, but it is not sufficiently detailed.

• The assessment does not adequately cover specific risks associated with different customer categories, transaction types, or geographic exposure.

Customer Due Diligence (CDD)

• The Company conducts basic identity verification of customers.

• However, procedures for enhanced due diligence (EDD) on high-risk customers are insufficient and inconsistently applied

Ongoing Monitoring

• The Company has implemented transaction monitoring, but the scope and frequency of monitoring are inadequate considering the high-risk nature of its business.

• Alerts are generated but not always reviewed in a timely manner.

Suspicious Transaction Reporting

• The Company has filed some reports with the Money Laundering Secretariat.

•Nevertheless, several cases were identified where the Company should have submitted reports but failed to do so.

Recommendations

The Authority recommends that the Company:

Strengthen Risk Assessment

•Update and expand the Company's AML risk assessment to include detailed analysis of specific risk factors (e.g., customer type, product, geography, transaction size).

Enhance Due Diligence Procedures

•Implement more robust enhanced due diligence (EDD) measures for high-risk customers.

• Ensure consistent application of these measures.

Improve Monitoring Systems

•Expand transaction monitoring coverage to reflect the Company's risk profile.

• Establish procedures for timely review and escalation of alerts.

Increase Reporting Compliance

•Ensure that all relevant cases are reported promptly to the Money Laundering Secretariat.

• Provide additional training to staff on identifying and reporting suspicious activities.

Risk Responsibility Statement Report

Purpose of the Report

This report aims to clearly explain the risks arising from customer operational errors and other uncontrollable factors during the company's business operations. It emphasizes that the company will not prioritize assuming any responsibility in such situations, in order to safeguard the stability of company operations and protect its legal rights.

Analysis of Risk Sources

I.Customer Operational Errors

Customers may incur financial losses or abnormal transactions due to incorrect operations, mis-clicked trades, or input errors while using the company's platform or services.

Examples include but are not limited to:

- Transferring funds to an unintended account
- Placing or canceling orders incorrectly
- Forgetting or misconfiguring trading parameters
- These risks are considered the result of individual customer actions, which the company cannot predict or control in advance.

II. Other Uncontrollable Factors

- External system environment abnormalities, such as network interruptions, third-party payment platform issues, or financial market fluctuations.
- Problems arising from third-party service providers, such as clearing institutions or partner banks.
- Force majeure events, such as natural disasters, policy changes, or other unpredictable incidents.

III. Company's Risk Assumption Position

- The company has established comprehensive safety and operational guidelines; however, it will not prioritize assuming responsibility for losses caused by customer operational errors or other uncontrollable factors.
- The company will provide operational manuals and educational resources to help customers reduce the risk of errors, but ultimate responsibility remains with the customer.
- If losses are caused by major system failures or the company's own negligence, the company will assume responsibility in accordance with applicable laws and contractual agreements.

IV. Risk Prevention Recommendations

- Customers should carefully read the operational guidelines and fully understand the risks before each transaction.
- It is recommended to enable security measures, such as two-factor authentication and transaction confirmation notifications, to reduce operational error risks.
- Customers should self-assess their risk tolerance and operate rationally to avoid significant losses due to mistakes.

V. Conclusion

In summary, customer operational errors and other uncontrollable factors may result in transaction or financial losses. The company will not prioritize assuming any related risks. The company will continue to optimize the platform and operational guidelines to assist customers in reducing the risk of errors, but ultimate responsibility remains with the customers themselves.

Conclusion

The Danish Financial Supervisory Authority (Finanstilsynet) has assessed that GC Exchange is a recognized trading platform with both security and potential risks. The inherent risk assessment of GCEX being used for money laundering or terrorist financing is considered within a safe range. However, the Authority urges GCEX to strengthen its review processes in the following areas: customer due diligence, customers' use of the exchange for potential money laundering activities, and related factors such as the financial products offered by the company, exposure to high-risk countries through customer transactions, and the company's significant volume of cross-border transactions with foreign jurisdictions.

The company has amended its customer risk assessment in order to classify customers individually according to risk and to incorporate all relevant risk factors into the categorization, particularly regarding customers' usage patterns and the jurisdictions with which they are connected. If a customer's activities violate regulations, the Financial Supervisory Authority may cooperate with the financial authorities of the customer's home country to conduct joint investigations and retains the right to freeze all of the customer's assets.

The company is required to obtain sufficient customer due diligence information, including details on the purpose and intended nature of the business relationship, with particular emphasis on acquiring adequate information regarding the customer's expected activities.

FINANSTILSYNET
Strandgade 29
1401 Copenhagen K
Tel. +45 33 44 72 82
CVR No. 10 96 48 84

02 FEB 2022

GC Exchange A/S 檢查聲明

（反洗錢領域）

引言 202 2 年 1 月，丹麥金融監管局對 GC Exchange A/S（以下簡稱“該公司”）進行了反洗錢專項檢查。此次檢查重點涵蓋客戶盡職調查與監控機制，包括高風險客戶及交易的監管，以及公司對洗錢預警資訊的處理流程和向反洗錢秘書處提交報告的相關工作。
該公司提供虛擬貨幣服務（VASP）和貨幣兌換業務。此次檢查僅限於審查該公司提供的虛擬貨幣服務。
風險評估：本公司主要為商業客戶提供加密貨幣交易服務，主要包括比特幣和以太坊，具體包括：•法定貨幣與虛擬貨幣之間的兌換•不同種類虛擬貨幣之間的兌換•虛擬貨幣的轉賬。

國家風險背景•洗錢秘書處的 2022 年國家風險評估將加密資產確定為重大洗錢風險，得出結論稱犯罪分子極有可能增加使用加密資產來清洗非法收益。
•丹麥安全和情報局（PET）202 2 年國家恐怖主義融資風險評估強調，加密貨幣是恐怖主義融資的高風險管道，因為它們的速度、缺乏地理限制以及存在混淆機制（例如，混合器、隱私幣）。
鑒於這些因素，公司的服務被認為在洗錢和資助恐怖主義方面具有內在的高風險。

檢查發現：風險評估 • 公司已編制了書面的風險評估，但其詳細程度不夠。

• 評估沒有充分涵蓋與不同客戶類別、交易類型或地域風險敞口相關的特定風險。

客戶盡職調查（CDD） • 公司對客戶進行基本身份驗證。

然而，針對高風險客戶的強化盡職調查（EDD）程式不充分且應用不一致。持續監控 • 公司已實施交易監控，但考慮到其業務的高風險性質，監控的範圍和頻率不足。

• 生成了警報，但並非總是及時進行審查。

可疑交易報告 • 公司已向反洗錢秘書處提交了若干報告。

儘管如此，我們還是發現了一些公司本應提交報告卻未能提交的案例。

建議監管機構建議公司：加強風險評估，更新並擴展公司的反洗錢風險評估，以包括對特定風險因素（如客戶類型、產品、地域、交易規模）的詳細分析。

加強盡職調查程式

• 對高風險客戶實施更完善的強化盡職調查（EDD）措施。確保始終適用這些措施。

改進監測系統

• 擴大交易監控範圍，以反映公司的風險狀況。

• 制定及時審查和升級警報的程式。

提高報告合規性

確保及時向反洗錢秘書處報告所有相關案件。

• 為工作人員提供關於識別和報告可疑活動的額外培訓。

風險責任聲明報告

本報告的目的在於，明確說明本公司在經營過程中因客戶操作失誤及其他不可控因素所導致的風險，強調本公司不對此類情況承擔任何責任，以維護公司經營的穩定性，保護公司的合法權益。

風險源分析

客戶操作失誤客戶在使用本公司平臺或服務時，可能因操作錯誤、誤點單或輸入錯誤而造成經濟損失或異常交易。

一、示例包括但不限於：

- 錯誤轉賬至非預期賬戶
- 錯誤下單與撤單操作
- 忘記與錯誤設置交易參數
- 此類風險屬於客戶個人操作行為，公司無法判斷或控制

二、其他不可控因素

- 外部系統環境異常，例如網路波動、第三方支付平臺問題或金融市場波動。
- 由第三方服務提供商，計算機數據問題，清算機構或合作銀行所引發的問題。
- 不可抗力事件，例如自然災害、政策變更或其他不可預見的事件。

三、公司的風險假設建議

- 公司已建立全面的安全和操作準則；但是，公司不會優先承擔因客戶操作失誤或其他不可控因素造成的損失。
- 公司將提供客服咨詢，以幫助客戶降低錯誤風險，但最終責任仍由客戶承擔。
- 如果損失是由重大系統故障或公司自身的疏忽造成的，公司將根據適用的法律和合同協議承擔責任。

四、風險防範建議

- 客戶在進行每筆交易前應仔細閱讀操作指引並充分理解風險。
- 建議啟用安全措施，例如雙因素身份驗證和事務確認通知，以降低操作錯誤風險。
- 客戶應自我評估風險承受能力，理性操作，避免因失誤造成重大損失。

五、**結論綜上所述，客戶操作失誤等不可控因素可能導致交易損失或財務損失，本公司不承擔任何相關風險，本公司將繼續優化平臺和操作指引以協助客戶降低錯誤風險，但最終責任由客戶自行承擔。**

結論

丹麥金融監管局（Finanstilsynet）評估認為，該公司 GC Exchange 是為安全與隱患並存認可較高的交易所，該交易所 GCEX 被用於洗錢或恐怖融資的內在風險評估為安全範圍，督促該交易所 GCEX 提升以下情況的審核如：用戶個人的咨詢審核，用戶利用交易所 GXEC 進行洗錢行為，因素：公司提供的金融產品、通過客戶業務暴露於高風險國家的風險敞口，以及該公司與海外司法管轄區之間頻繁的跨境交易量。

公司已修改其客戶風險評估，以便根據風險對客戶進行單獨分類，並且將所有相關風險因素納入風險分類，特別是客戶的使用操作和客戶所連接的司法轄區，如若客戶的使用違反將會通過金融管理局配合該用戶國家金融管理局相互調查並有權利凍結用戶所有資產。

公司被要求獲取足夠的客戶盡職調查資訊，包括相關業務關係的目的和預期性質的資訊，特別強調獲取關於客戶預期活動的足夠資訊。

金融與技術
斯特蘭德街 29 號，
1401 哥本哈根；
電話：+45 33 44 72 82；
CVR 編號：10 96 48 84；