FREEDOM FINANCE EUROPE LTD

Device Authentication Policy

1st of May 2024

Name of document: **Device Authentication Policy**

Type of document: **Internal and Client Policy**

Version History

Version	Date of update	Reason of update	Date of approval	Remarks
1.0	01.05.2024	New Policy	23.05.2024	n/a

Table of Contents

1. Introduction

1.1. Freedom Finance Europe Limited (hereinafter called the “Company”) is a Cypriot Investment Firm ("CIF") registered with the Registrar of Companies under the number HE 324220 and regulated by the Cyprus Securities & Exchange Commission ("CySEC") under license number 275/15.

1.2. Following the requirements and/or obligations implemented by the following laws and regulations and in compliance with the current legal framework, but not limited to:

- Directive 2014/65/EU of the European Parliament and the Council on markets in financial instruments (“MiFID II”);
- the Law 87(I)/2017 regarding the provision of investment services, the exercise of investment activities and the operation of regulated markets and other related matters, as amended from time to time (the “Law”);
- the Investment Services and Activities and Regulated Markets Law No 144(I)/2007;

In order to comply with its safekeeping and cybersecurity obligations, the Company adopted this Device Authentication Policy, which sets out security measures implemented by the Company to verify:

i. New Clients’ devices, and
ii. New secured session while Clients use web browser.

1.3. The Policy is adopted by the Execution Committee and communicated to everyone involved to ensure their commitment to it, including Company’s Clients.

2. Definitions

“Application” means “Freedom24 by Freedom Finance app” available from Apple Store, Google Play and AppGallery;

“Access Codes” means the Client’s access codes, any login code, password(s), Client Account number, Client’s Electronic Authentication Means and any information required for accessing the Company’s Electronic Trading Platform;

“SMS Authentication” means initiation of the Secure session with secure Access Codes provided by the Company via SMS notifications and/or via Telegram push notifications sent to the mobile number given by the Client in the Member Area;

“Verified device” refers to a device that the client has successfully verified by undergoing either the Standard or Alternative device authentication method;

“Standard Device Authentication” means the method designed for the client to verify the Client’s Device, as described in clause 8 herein;

“Alternative Device Authentication” means the method designed for the client to verify the Client’s Device, as described in Annex 1 herein;

“Mobile device” means a handheld electronic instrument designed for wireless communication and computation, including but not limited to smartphones, tablets, and wearable devices;

“QR Code” refers to a Quick Response code, which is a two-dimensional barcode consisting of black squares arranged on a white square grid, which can be read by a mobile device using an Application. It contains encoded information that serve as a means of efficiently storing and transmitting information, facilitating various applications, including but not limited to authentication, identification, and data retrieval;

“Company’s Electronic Trading Platform” an internet website, Application or another electronic medium that enables Clients using the facility (access codes) provided by the Company to enter into Transactions or carry on dealings with the Company via an internet website, Application or through some other electronic medium;

“Company’s website” or “**Company Portal”** means www.freedomfinance.eu, www.freedom24.com, www.freedom24.eu, www.bondsfreedom.com, www.tradernet.com, www.tradernet.com.ua, www.tradernet.ua, www.ffin.com.cy, www.freedomfinance.com.cy, www.tradernet.kz, www.tradernet.ru, www.freedomfinance.eu, or any other website that may be the Company’s website from time to time;

“Live Support” means a way for the Client to have real-time, back-and-forth communication with the Company available at http://freedom24.com/ and within the Application;

“AWS” means Amazon Web Services, a third party company;

“Liveness check” means Detecting face liveness procedure executed by Amazon Recognition (AWS) or SumSub;

“SumSub” means Sum and Substance, a third-party company;

“identity verification module” means the procedure executed by SumSub and/or Amazon Web Services .

For the purpose of this Policy Authentication and Verification means the same.

3. Scope and purpose

3.1. This Policy aims to set appropriate and sufficient measures and procedures to ensure secure access of the Client to its member area within Company's Electronic Trading Platform.

3.2. This Policy is adopted to prevent cybersecurity threats:

i. unverified access;
ii. fraud;
iii. stealing assets;
iv. spyware;
v. phishing.

4. General Principles

4.1. The mandatory device authentication procedure has been implemented to achieve the purposes of this Policy.

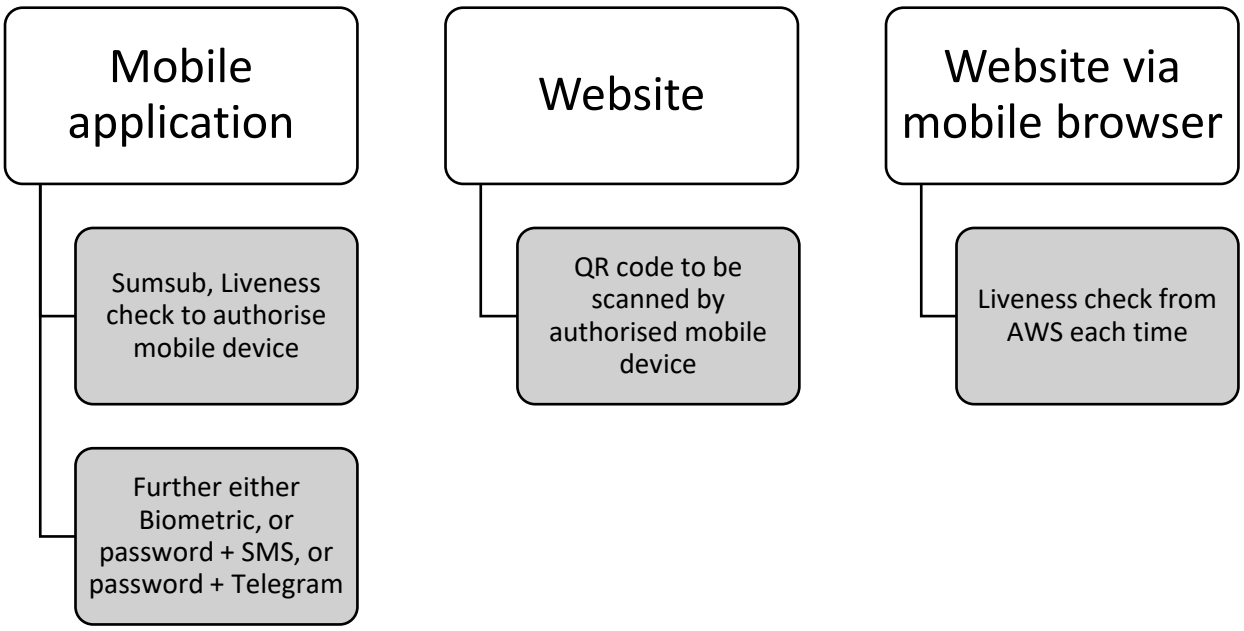
4.2. The mandatory device authentication procedure applies to all devices you use to access the Company's Electronic System.

4.3. To access the Company's Electronic System through a mobile application, you can only use a Verified device. To verify a mobile device, you should complete either the **Standard Device Authentication** or the **Alternative Device Authentication**. Once authentication is complete, your device will be saved as Verified.

4.4. To access the Company's Electronic System through the website, you must scan a QR code using a Verified mobile device.

4.5. To access the Company's Electronic System through a mobile browser, you should complete the Liveness check each time.

5. Scheme



6. Services implemented

6.1. The security measures adopted include:

i. Detecting face Liveness using Amazon Rekognition (AWS) https://docs.aws.amazon.com/rekognition/latest/dg/face-Liveness.html;

ii. CompareFaces using Amazon Rekognition (AWS) https://docs.aws.amazon.com/rekognition/latest/APIReference/API_CompareFaces.html;

iii. SumSub https://sumsub.com/privacy-notice-service/;

iv. SMS Authentication;

v. QR codes.

7. Privacy notice

7.1. The Company is a controller of your personal data. There are PRIVACY AND COOKIES POLICY and DATA PROTECTION POLICY in place. You can find them on Company's website.

7.2. The Company is liable for data protection and data processing under the Data Protection Regulation, other laws protecting data used in the member states of the European Union, and other regulations connected with data protection.

7.3. If you have any concerns, please address them to the Data Protection Officer: Oleg Tupiko, email: dpo@ffineu.eu

7.4. Third-party privacy information is represented in Appendix № 7 to the General Terms of Business

8. Standard Device Authentication, Mobile devices

8.1. The Mobile device on which the client opened an account and completed verification in SumSub is considered Verified for that client.

8.2. The Device mentioned in clause 8.1 remains Verified until the application is reinstalled. On mobile web, verification is valid until the session cookie is updated, after which re-verification is required.

8.3. When installing the application on a new device, the verification procedure must be completed to open a secure session. If a third party logs into another client's previously verified device, they will also need verification, which serves as additional protection of the Client's data.

8.4. If the device has not been verified, verification is required the first time an attempt is made to open a Secure session in the application and each time it is on the mobile web.

8.5. The verification starts with comparing the Client's photo with the one previously verified through SumSub. If the photo previously verified through SumSub is unavailable, the Client uses the SumSub identity verification module to upload an identity document proving the client's identity.

8.6. When the step under clause 8.5. is completed, the Client uses AWS identity verification module to conduct a Liveness check to verify that the client undergoing the Livness check is a real human and looks like on the verified photo in the database. If the Liveness check fails, the client is prompted to repeat the check.

8.7. After a successful Liveness check, the client's photo is compared with the verified photo in the database. If they match, the Mobile device is considered verified.

8.8. In case of a failed Liveness check, the client is shown an error message from the AWS.

8.9. In case of a Liveness check error, the SumSub identity verification module is used to conduct the Liveness check and compare the client's face with the photo from the database.

8.10. After verification, the client can open a Secure session on the device using standard methods (biometrics, SMS Authentication).

9. Opening a Secure Session via QR Code

9.1. A QR code is generated and displayed in a pop-up window when attempting to open a Secure session on desktop devices. The QR code is periodically updated for security purposes.

9.2. Scan the QR code in the mobile application's "Add Device" section to open a Secure session on a desktop device. Access to this section is possible only with an active Secure session in the application, which requires device verification.

9.3. After successfully scanning the QR code in the mobile application, the Secure session is automatically opened on the desktop device.

9.4. If the QR code is scanned incorrectly or has expired, the Secure session on the desktop device will not open, and the Client will be prompted to rescan using a valid QR code.

Annex 1. Guidance for Alternative Device Authentication

Alternative Device Authentication can be done through contacting Live Support, real-time, back-and-forth communication with the Company available at http://freedom24.com/ and within the Application and or via email as set in clause 35.2 of General Terms.

QR code authorization scheme may be disabled at the customer's official request in exceptional cases, solely at the Company's discretion.