**Monitoring System Requirements**

**Regarding Compliance with the Strong Authentication Rule**

The monitoring system shall ensure compliance with the strong authentication rule, PSD2, European Directives and Strong Customer Authentication Rule approved by the National Bank of Georgia on 2 September 2020 and the Law of Georgia on Personal Data Protection.

The monitoring system aims to build a more secure ecosystem for all communications between consumers and bank so that they include:

* Mechanisms for strong customer authentication,
* Mechanisms for malware detection and a response to it, and
* Mechanisms for risk analysis that detect fraudulent transactions and allow their mitigation in real-time.

The system shall enable to exempt the application of the security requirements of strong customer authentication, subject to specified and limited conditions based on the level of risk, the amount and the recurrence of the payment transaction and the payment channel used for its execution.

The system shall incorporate into its solution the behavioural biometrics (angle of holding the device; the speed of character typing; duration of button presses) and device possession assessment (as evidenced by generating a signature by the device (hardware or software token); the app or the so-called browser whose possession is confirmed by connecting them to the device) using technologies, that makes is possible to apply end user’s possession and inherence elements for strong customer authentication.

The system shall have mechanisms in place that prevent the impersonation and manipulation of the user, shall also be able to detect malicious redirects to fraudulent third sites (Phishing) and even be able to integrate additional mechanisms to identify attempts to bypass the payment service provider’s security measures.

The payment transaction monitoring mechanisms shall take into account, at least, the following risk-based factors:

a) lists of compromised and/or stolen authentication elements;

b) the amount of each payment transaction;

c) known fraud scenarios in the provision of payment services;

d) signs of malware infection in any sessions of the authentication procedure causing delays and/or damage;

e) if the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.

**Transaction monitoring mechanisms**

Transaction monitoring mechanisms shall enable, in real-time, to detect unauthorised or fraudulent payment transactions for the purpose of the implementation of the security measures.

Those mechanisms shall be based on the analysis of payment transactions taking into account elements that are typical of the payment service user in the circumstances of the normal use of the personalised security credentials.

The transaction monitoring mechanisms shall enable a real-time risk analysis to identify any of the following:

1. abnormal spending or behavioural pattern of the payer;
2. unusual information about the payer's device/software access;
3. malware infection in any session of the authentication procedure causing delays and/or damage;
4. known fraud scenario in the provision of payment services;
5. abnormal location of the payer;
6. high-risk location of the payee.

The monitoring system shall have mechanisms in place that shall take into account the following risk-based factors:

a) the spending patterns of the individual payment service user;

b) the payment transaction history of each of the payment service provider's payment service users;

c) the location of the payer and the payee at the time of the payment transaction in cases where the access device or the software is provided by the payment service provider;

d) the identification of abnormal payment patterns of the payment service user in relation to the user's payment transaction history.

**Requirements of the elements categorized as possession**

The system shall be able to protect the elements of strong customer authentication categorised as possession from using by unauthorised parties to prevent replication of the elements.

**Requirements of devices and software linked to elements categorized as inherence**

The system shall enable to mitigate the risk that the authentication elements categorised as inherence and read by access devices and software provided to the payer are uncovered by unauthorised parties to prevent unauthorized use of these elements through unauthorized access to devices and software.

At a minimum, the system shall ensure that those access devices and software have a very low probability of an unauthorised party being authenticated as the payer.

**Requirements for the independence of the elements**

The system shall guarantee the independence of the elements used for strong authentication; namely, shall ensure that the use of the elements of strong customer authentication is subject to measures, which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements.

Besides, where any of the elements of strong customer authentication or the authentication code itself is used through a multi-purpose device, the system shall be able to mitigate the risk which would result from that multi-purpose device being compromised.

For these purposes, the mitigating measures shall include each of the following:

1. the use of separated secure execution environments through the software installed inside the multi-purpose device;
2. mechanisms to ensure that the software or device provided to the user has not been altered/modified by the payer or by a third party;
3. where alterations/modifications have taken place, mechanisms to mitigate the consequences thereof.

**Requirements for the creation and transmission of personalised security credentials**

Mechanisms that mitigate the risks of unauthorised use following the loss, theft or copying of the personalised security credentials and of the authentication devices and software before their delivery to the payer

**Requirements for the delivery of personalised security credentials, authentication devices and software**

Mechanisms used to ensure that the personalised security credentials, authentication devices and software are delivered to the payment service user in a secure manner, shall include the following measures and requirements:

1. effective and secure delivery mechanisms ensuring that the personalised security credentials, authentication devices and software are delivered to the legitimate payment service user;
2. mechanisms that allow the payment service provider to verify the authenticity of the authentication software delivered to the payment services user through the internet;
3. arrangements ensuring that, where the delivery of personalised security credentials is executed outside the premises of the payment service provider or through a remote channel:
4. no unauthorised party can obtain more than one feature of the personalised security credentials, the authentication devices or software when delivered through the same channel;
5. the delivered personalised security credentials, authentication devices or software require activation before usage;
6. arrangements ensuring that, in cases where the personalised security credentials, the authentication devices or software have to be activated before their first use, the activation shall take place in a secure environment.

**Technical specifications**

The proposed Software Solution shall be integrated and usable in the following types of apps:

Web Application

 React, .Net, .Net core

Mobile Application

 IOS, Android

 React Native

The Software Solution shall also have an API or other integration tools. The API or integration tool shall, at least, integrate all reports generated by the Software Solution into the Bank's unified reporting system.

* **The company shall submit a Certificate of Conformity/documentation.**
* **Implementation price shall be a one-time and annual (if any) fee.**