UNIONBANK

Request for Proposal

Solution for Transaction Fraud and Device Monitoring

Dear Sir / Madame,

Union Bank invites you to participate in the procurement process for “Solution for Transaction Fraud and Device Monitoring”.

The purpose of this Request for proposal is to accept evaluate and select the best Proposal that meets the Bank's requirements for this process, according to the requirements listed in this request for Proposal.

The proposals will be evaluated in accordance with the selection criteria below that will determine the winning bid:

- Proposed solution.
- Evaluation based on the best and final offer for the requested services.

Thank you in advance for your reply and best regards,

Administration Department

Union Bank Sh.A.

Date issued 1 July 2024

TABLE OF CONTENTS

1. Introduction

Union Bank (hereinafter "the Bank", or "UB") is a financial institution registered as a commercial bank on 9 January 2006. For further information regarding the Bank's activities, size and financial situation, please visit our website: www.unionbank.al.

Union Bank is seeking proposals from qualified vendors for the implementation of a comprehensive Transaction Fraud Monitoring Tool and Device Monitoring solution. The tools must comply with the Payment Services Directive 2 (PSD2) regulation.

2. Project Objective

The objective of this project is to acquire and implement robust solutions for:

- **Transaction Fraud Monitoring Tool**: Real-time monitoring of transactions to detect and prevent fraud, including compliance with PSD2 requirements such as Strong Customer Authentication (SCA) and transaction risk analysis. It is essential to provide detailed reporting and analytics on fraud trends and incidents; and to minimize false positives and ensure seamless customer experience.
- **Device Monitoring**: Monitoring and validation of devices used in payment transactions to ensure security and compliance with PSD2, which covers secure communication and transaction protection.

3. Scope of Work

Solution should meet the following requirements:

3.1. Compliance Requirements

Solution must be compliant with Bank of Albania regulatory requirements for Strong authentication and Open Banking Solution based on PSD2. (Rregullore 29/2022 "Për autentifikimin e thelluar të klientit dhe standardet e përbashkëta, të hapura dhe të sigurta të komunikimit")
The regulation can be accessed at the following Link:
https://www.bankofalbania.org/Supervision/Regulatory_Framework/Acts_expected_to_enter_into_force/Document_Title_32053_1.html

3.2. Business requirements – Transaction Fraud and Device Monitoring system

Union Bank must comply with PSD2 requirements. Union Bank shall be able to establish and implement preventive security measures for operational and security risks. The system should provide security measures and fraud prevention capabilities, including risk assessment and real-time detection of misuse of payment transactions or access, including any potential thread.

The mechanism should include but not limited to the following:

- Should consider at minimum, the following risk-based factors (based on RTS/Article 2):
  a. authentication elements, compromised or stolen.
     i. Insecure Software Configurations Detection
     ii. Insecure Mobile Device Configurations Detections
     iii. Behavioral Biometrics
  b. the amount of each payment transaction.

c. known fraud scenarios in the provision of payment services which should include but not limited to*:
   i. Social engineering attacks detection
   ii. Account Takeover Detection
   iii. Session Stealing
d. signs of malware infection in each session of the authentication procedure.
e. traces (log) of the use of the access device or program (software) provided to the user of payment services and abnormal use of the access device or program, in cases where the access device or program is offered (provided) by the provider of payment services.

- Transaction risk Analysis, to define if a transaction should be considered as fraudulent or not and use this result as an exception to the SCA in compliance with paragraph (2c) of article 22 of the regulation 29/2022 of Bank of Albania, which says:

(c)* payment service providers as a result of performing a real-time risk analysis have not identified any of the following:

i. abnormal spending or behavioral pattern of the payer.
ii. unusual information about the payer's device/software access.
iii. malware infection in any session of the authentication procedure.
iv. known fraud scenario in the provision of payment services.
v. abnormal location of the payer.
vi. high-risk location of the payee.

- Ability to define a "Calculation of fraud ratios/norms" in compliance with article 23 of the regulation 29/2022 of Bank of Albania, which will be given by the bank.

- Ability to record and monitor the following data for each type of payment transaction, particularly highlighting remote and non-remote payment transactions, to use the exceptions in compliance with article 25 of the regulation 29/2022 of Bank of Albania:
  a) the total value of unauthorized or fraudulent payment transactions, the total value of all payment transactions, and the fraud rate resulting from them, including the breakdown of payment transactions initiated through customer authentication and according to each of the exceptions.
  b) the average transaction value, including the breakdown of payment transactions initiated through customer authentication and according to each of the exceptions.
  c) the number of payment transactions where each of the exceptions has been applied and their percentage in relation to the total number of payment transactions.

- Ability of the solution to temporary/permanent block user access after specified failed SCA attempts.

- Monitoring system for SCA application, which will help bank to guarantee the quality/, completeness/accuracy and adequacy of data. Union Bank should be able to identify transactions where SCA is applied or SCA exemptions have been included.

- The supported circumstances and the will ad-hoc reviews, such as but not limited to deficiencies on the functioning of the solution detected while monitoring, audit/perceived increase in fraud attempts. Ability to adapt to changes of the legal or regulatory framework.

3.3. Other Requirements

- Providing and implementing the Transaction Fraud Monitoring Tool and Device Monitoring solution.
- Customizing the tools to align with our specific business requirements and compliance needs under PSD2 regulation.
- Advanced machine learning algorithms for fraud detection.
- Integrating the solutions with our existing payment systems and infrastructure.
- Customizable alert and notification system.
- User-friendly dashboard for monitoring and management.
- Comprehensive reporting and analytics tools.
- Training our staff on the use and maintenance of the tools. (if required after the project)
- Providing ongoing technical support and maintenance services.

4. Evaluation Criteria

- Technical capabilities and innovation of the proposed solution.
- Relevant experience and track record of the vendor.
- Cost-effectiveness and value for money.
- Implementation plan and timeline.
- Quality of customer support and service.
- References and case studies.

5. Project Organization & Governance

Project Management methodology will be defined accordingly, based on the proposal submitted by you in the technical proposal document.

Bank will contribute in project quality assurance during implementation, data migration strategy & approach as well as User Acceptance criteria tests.

6. Request for Proposal Timeline

Date	**Event**
1 July 2024	RFP Issued
5 July 2024	Deadline for submitting questions, clarifications
19 July 2024	Deadline for the Bank to submit the answers
29 July 2024	Deadline for bidders to submit proposals
20 August 2024	Deadline for the Bank to Notify selections
27 August 2024	Contract sign off

Proposals must be received on or before the deadline and submitted by email to **procurement@unionbank.al**

The proposal format must contain the list of documentation included in Annex 1 attached to this RFP.

The offer must remain valid for a period of at least 180 days from the date of the submission.

ANNEX 1: List of Proposal Documentation:

- Detailed description of your proposed solution, including technology stack, architecture, and key features; and how it specifically accomplishes the functions in scope of the bank's requirements.
- Administrative information / vendor profile (mailing address, phone number of designated point of contact). Key profiles of the company and detailed CV-s of the resources that will be engaged the bank's project.
- List of respective solution implementations performed in the last 5 years, specifying the bank/institution, the core platform integrated into and respective references.
- All respective certificates and authorizations you hold from any EU Country regulatory institutions regarding your solution and its compliance with PSD2.
- Key profiles of the company and detailed CV-s of the resources that will be engaged the bank's project.
- Project management approach (Including key project risk monitoring Procedure)
- Proposed Timeline of the project and resource allocation
- Hardware, database, and Operating System requirements
- Draft template of the contract proposed by company.
- Details on ongoing support, maintenance, and service level agreements (SLAs).
- Completed Third Party Questionnaire, attached as Annex 2 of this RFP.

Commercial Proposal which must include:

Detailed pricing information, including any setup fees, subscription models, maintenance costs, and additional charges for training services. Commercial Proposal must include:

- Total commercial proposal for the solution/s proposed
- Breakdown of applicable fees into phases of the project
- Conditions and deliverables for payments

Currency shall be in EUR, to be specified VAT and / or any other applicable tax included or not.

As a result of this request, a contract will be concluded with the selected Supplier.

Subcontracting will NOT be allowed during the realization of the contract, except when approved prior by the Bank. In case verified, it will lead to immediate interruption of the Contract.

To ensure same level of information for all participants, whatever answer or additional clarification that the Bank will give to one of the interested companies, will be shared with the rest of the participants in this process.

The form of communication for any question regarding the scope of this Request for Proposal will be done only through the e-mail address: procurement@unionbank.al

The Documentation requested must be submitted in a **sealed envelope** by **July 29th, 2024**, to the following address:

Departamenti i Administrates
Union Bank SHA
Bulevardi Zogu I, Sheshi Ferenc Nopçka, Nd. 5, H. 3, Njësia Bashkiake Nr. 9, Kodi Postar 1016, Tiranë, Shqipëri

With reference: ***"Solution for Transaction Fraud and Device Monitoring"***

Or in electronic version PDF Format, by email to the address: procurement@unionbank.al

The technical proposal and the commercial proposal must be submitted separately to each other; in separate envelopes if the proposal will be submitted on Hard Copy version or separately in pdf format if it will be submitted electronically.

ANNEX 2: Third Party Questionnaire

Third-Party Security Questionnaire

Please answer the following questions on part 1 and part 2 of this document. If a question is not applicable for your organization, write N/A

Part 1: Governance & Infrastructure Security Questions

1. Who is responsible for managing your information security and privacy program?
    a. Describe the experience and expertise of your IT security staff.

2. Do you outsource any IT or IT security functions to third-party service providers?
    a. If so, who are they, what do they do, and what type of access do they have?

3. How do you protect customer information?

4. Have you ever experienced a significant cybersecurity incident? If yes,
    a. Please define and describe it.
    b. Do you report them on any local or international CSIRT?

5. Does your organization have a security program?
    a. If so, what standards and guidelines does it follow?
    b. Does your information security and privacy program cover all operations, services and systems that process sensitive data?

6. How frequently are your employees trained on cyber security?

7. Do you employ a cybersecurity assessment performed by a third-party organization?
    a. If yes, what is the periodicity?
    b. What were the results of your most recent vulnerability assessment and/or penetration test? (The report may be required after contract signing).

8. Do you employ server hardening?

9. Do you keep your server operating systems patched?

10. What operating systems are used on your servers?

11. Do you have a data recovery capability? If yes,
    a. Do you backup your data?
    b. How do you store backups?
    c. Do you test backups?

12. Do you have automated tools that continuously monitor to ensure malicious software is not deployed and protect employee devices from ransomware and other types of malware?

13. Describe the processes and tools you use to reduce, control and monitor administrative privileges and privileged accounts.

14. Do you blacklist or whitelist communications?

15. Do you log security events? If yes,
    a. How do you analyze security logging information?
    b. How do you monitor your network to alert to cybersecurity events?

16. What processes/controls do you have in place to prevent the exfiltration of sensitive data, particularly sensitive customer data?

17. How do you plan and train for a cybersecurity incident? If yes,
    a. What processes do you have in place to respond to an incident?
    b. Do you regularly practice those things?

18. Do you have procedures in place for business continuity in the event that your office is inaccessible?

19. Do you have a disaster recovery plan? Describe it.

20. What types of physical protection do you have in place to prevent unauthorized access to data or infrastructure assets?
    a. Do you have a written policy for physical security requirements?
    b. Do you review physical and environmental risks? If yes, what is the periodicity?
    c. Is your network equipment physically secured?
    d. How many data centers store sensitive data?
    e. What countries are data centers located in?

21. How do you manage remote access to your corporate network? If yes,
    a. Do you use a VPN or another type of secure tunnel?
    b. Do you use Multi Factor Authentication?

22. Do you have a removable media policy and controls to implement the policy?

23. How do you monitor for unauthorized personnel, connections, devices, and software?

Part 2: Web Application Security Questions

1. What is the name of your application? And what does it do?

2. Does your application have a valid SSL certificate to prevent man-in-the-middle attacks?

3. Does your application require login credentials?

4. Does your application have the possibility to use 2FA?

5. How do users get their initial password?

6. Do you have minimum password security standards?

7. How do you store passwords? (Encrypted or plain text)

8. How can users recover their credentials?

9. Do you offer single sign-on (SSO)?

10. How do you assess the security of the software that you develop and acquire?
    a. Please provide the result of your last application assessment/pentest. (The report may be required after contract signing).

11. Is your application deployed on Cloud or On-Premises?