Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF
CAMBRIDGE
Judge Business School

CAMBRIDGE SUPTECH LAB
ACCELERATING THE DIGITAL TRANSFORMATION OF FINANCIAL SUPERVISION

REQUEST FOR EXPRESSION OF INTEREST (REOI)

Intelligence platform for flagging fraudulent fintech apps

Project: Development of a working prototype for an intelligence tool for flagging fraudulent fintech apps ("the Project") for a financial authority (the "Agency")

Description: A solution for financial authorities to flag fraudulent smartphone apps through the collection, storage, and analysis of app store reviews. Initially intended as an internal supervision tool, the tool must ultimately serve insights to the public through APIs and other interfaces that allow for development of additional services.

Contracting Entity: University of Cambridge, Judge Business School

Countries and Agencies: TBC before vendor selection and contracting

Grant Value: US$100,000

Publication Date: 24 February 2023

Expression of Interest Deadline: 09 March 2023 23:59 GMT Time (UTC +0)

Project Implementation Dates: May 2023 – November 2023

Procurement Process Managed by: Cambridge SupTech Lab at the Centre for Alternative Finance, the University of Cambridge Judge Business School

Submission: Email all documents to the Cambridge SupTech Lab's Launchpad at suptech-launchpad@jbs.cam.ac.uk with subject line "REOI: Cambridge SupTech Lab – Intelligence on Fraudulent Fintech Apps Project"

Language: All submissions must be written in English.

Supported by BILL & MELINDA GATES foundation

The Cambridge SupTech Lab

The Cambridge SupTech Lab ("the Lab") at the Cambridge Centre for Alternative Finance, the University of Cambridge Judge Business School, accelerates the digital transformation of financial supervision.

While financial services are becoming increasingly global, digital and complex, analogue processing and antiquated technologies in data gathering, validation, storage and analysis erode the analytical capabilities of supervisory agencies, who are often too late in protecting consumers from fraud and seeing signs of stress in the financial system, or miss the underlying causes. This is all happening while financial crime remains a trillion-dollar issue, and public agencies face new challenges such as the regulation and supervision of crypto assets, and monitoring environmental, social and governance (ESG) aspects of the financial industry's business.

The Lab aims to meet financial sector supervisors' needs by developing with them new methodologies and processes that further market oversight and empower consumers, and to deploy suptech applications that generate relevant, reliable, timely insights to inform their decisions. From research to executive education, to technical assistance, to crafting production-grade suptech solutions, we are committed to supporting the emergence and acceleration of the suptech ecosystem and to empowering a new generation of innovation leaders seeking to digitally transform financial supervision.

For more information about the Lab, please visit https://www.cambridgesuptechlab.org

The SupTech Launchpad

To accelerate the growth of the suptech marketplace, the Lab partners with financial authorities and technology vendors to co-create and deploy cutting-edge, scalable suptech applications. Our team helps detail the technical specifications, de-risk procurement for all parties, and provide project management support and hands technical assistance including security testing. Furthermore, we provide the vendors with coaching and opportunities to engage with investors and other stakeholders.

The most transformative Proofs of Concept (POCs) developed through the Innovation Leadership Programme are selected for agile prototyping and deployment. The process involves global competitions to crowdsource ideas from technologists and identify the best implementation partners among both other financial authorities and vendors. The Lab's Launchpad largely builds on the experience of the RegTech for Regulators Accelerator (R^{2}A), which successfully developed groundbreaking applications by introducing an agile mode of collaboration between financial authorities and vendors.

For more information, please visit https://lab.ccaf.io/launchpad/

I. Project Description

The focus of the project is to create a prototype of an intelligence tool for flagging fraudulent fintech apps. This prototype solution intends to solve the problem that represents the increase in the number of fake fintech applications and scams in the country under supervision of the Agency.

Online scammers follow non-transparent methods, collect exorbitant interest rates, cause harassment through harsh recovery measures, and unauthorised use of personal data. This has affected the general trust in the financial system, and especially on the fintech space and solutions. Moreover, due to involvement of malicious entities based in other countries, such apps have serious impact on national security, general economy and citizen's safety.

Therefore, the prototype solution that will be developed is an intelligent system to flag to supervisors any instances of potential fraud in fintech apps, based on metadata from (i) purported lending apps from app-stores; (ii) other concerned apps and (iii) other relevant sources within the system, to identify patterns and flag malign actors pre-emptively.

The creation of a robust system to detect frauds is essential for the protection of its users, continued growth, and reliability of the system. Ultimately the system should provide for the future ability to serve as a basis for applications that serve the generally public (e.g., a website or smartphone-based service that can act as a preventive anti-fraud measure while installing any fintech app in the phone of the customer).

II. Description of Required Solution

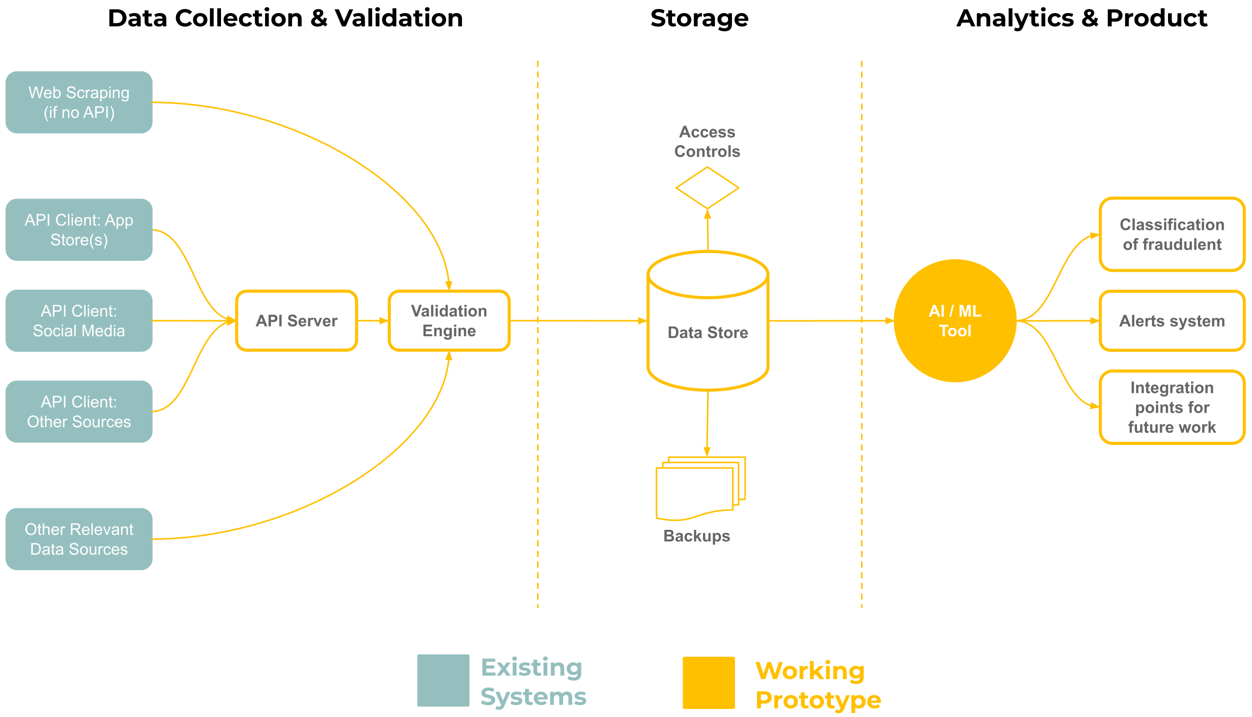
Basic Requirements

Through this tool, the Agency will be able to:

- Collect and analyse metadata to identify the bad actors in the digital lending space (fintech apps, in general), take action, and warn the customers as is appropriate, which should result in reduction in successful fraudulent activities and enhance the robustness of the fintech ecosystem.
- Pre-emptively screen out malicious apps, to the extent possible.
- Advance sustainable development of financial sector by ensuring people's trust in digital finance.
- Allow for the integration of additional future services, such as tools for end customers to identify fraudulent apps and receive alerts before installing such dubious apps.

High-level architecture

A more granular breakdown of the process follows, including developing APIs to access various databases, refinement of data schemas based on Data Structures, training of the AI/ML based decision engine, testing of the application as per the following data flow diagram:



Key Technical Requirements

The prototype for detecting fraudulent fintech apps will have the following key elements:

COMPONENT	ID	FEATURE	DESCRIPTION	PRIORITY
Data Collection	1.1	API Clients	If an app store has open APIs, a solution would capture metadata directly. In the absence of such endpoints, the solution should provide for a purpose-built web scraper.	HIGH
	1.2	API Server	Dedicated server to manage the API data and data from other sources.	HIGH
	1.3	Instrumentation	Validation engine to inspect and process the data.	HIGH
	2.1	Formatting	Create a data dictionary and store the data	HIGH

Centralized Storage	2.2	Access Controls	The storage mechanism must provide for varying levels of access controls with default access expiration dates	MED
	2.3	Automatic Backup	The storage system should automatically allow for cold storage backups in case of disaster recovery	MED
Decision Engine	3.1	AI/ML based analytics	A tool that analyses data from various sources (metadata on the app available in the app-store, data in the app, data from supervisory entities, unstructured data from social media etc.) to predict whether the app concerned is a good or a bad actor. Example: Network Analysis, Anomaly detection algorithm, etc.	HIGH

Scope limitations

In Scope:

- Development of the intelligence tool for detecting fraud among fintech apps using metadata, including: data collection and validation mechanisms, storage mechanisms, ML-based analytics, and interfaces for additional future products to integrate with.

Out of Scope:

- If selected app store do not have Open API, the API client for app store would be out of scope.
- Development of any product for end consumers or the general public.

III. Key vendor requirements

The Project requires a vendor with the capacity, relevant experience, and resources to design, develop, test, and deploy a prototype with the purpose of collecting and analyzing app store review data for the sake of detecting fraudulent apps.

General Launchpad qualifications

- Specificity: the competition is result oriented and the proposed solution needs to have a high level of detail and granularity with respect to the expected output.
- Precedent: the applicant needs to work on a novel solution.
- Geography: the vendor can be based in any jurisdiction. Data needs to be stored in an infrastructure compliant with the needs of the financial authority.
- Collaboration: the development of the solution should be conducted in collaboration with the team designated by the financial authority in each distinct phase.
- Sufficient experience to build an application that can serve the data needs of the financial authority, e.g.:

  - Integrate with existing application within a governmental entity
  - Allow the migration of existing data
  - Provide real time, on-demand support and the ability to generate reports or summary
  - Provide a high standard of application security.
- Demonstrated ability to:
  - Manage product life cycle
  - Develop, complete, implement, maintain, and deliver the appropriate technologies
  - Properly write documentation
  - Maintain an enterprise ecosystem.
- Experience with:
  - Suptech solutions
  - Working with regulators and financial authorities
  - Frontend Development and UI/UX Design (as needed)
  - Data products and practical applications of analytics and data science (e.g., AI/ML)
  - Software engineering
  - Application architecture and devops
  - Program/project management and business analysis
  - Agile methodologies for application development
  - Application integration and performance tuning/optimization.
- Knowledge including:
  - Cybersecurity and secure application development coding standards
  - Best practices in relevant fields to the solution at hand.
- Resources:
  - Technical expertise on related knowledge and experience
  - Sufficient staffing and computing resources required by the identified feature and time requirements and constraints
  - Sufficient specification of online, on-premises, and/or hybrid computing resources
  - Adequate project management staffing based on requirements

  - Software, hardware, network, and cloud computing licenses and subscriptions to cover development, implementation, and warranty period.
- Project management:
  - Methods that leverage agile delivery methodologies for project planning, design, building and testing, stakeholder engagement, and effective risk management to ensure on-time completion of the project without budget overrun.

Engagement-specific requirements

i. Capability:
   - Create an AI/ML based decision engine, scrape metadata from appstore, etc.

ii. Experience:
   - Experience in handling of projects based on AI/ML based decision engine creation
   - Scraping of metadata from Appstore and social media.
   - Creating API client and API Server

iii. Knowledge:
   - Best practices in designing, selecting, training, testing, validating, deploying and maintaining interpretable ML models, and to mitigate sources of algorithmic bias
   - Knowledge of app store metadata
   - Best practices and standards for API client and server development and documentation

iv. Resources:
   - The Agency has mainly on premises centralised servers, so a dedicated server for database and running the AI/ML based decision engine would be required. Vendor should support selection of such a system, and maintenance in case of any problems with the decision engine.
   - Agency has policy of Team only or Department only access, so concerned department staff who would deploy the product will need to be trained to successfully create the database and run the app.

IV. Project Award

The successful applicant will:

- Be awarded **US$100,000** to develop and test the required solution. This is a fixed-sum contract, which is to cover all the applicant's expenses related to the development and testing work, including staff time, hardware, software, travel, and all other project-related expenses.

- Receive tailored coaching
- Be invited to the Lab's pitch day to connect with funders and to a demo day to present their products to potential clients
- Be listed in the Lab's online Vendor Database.
- Be mentioned in a case study published by the University of Cambridge to share lessons from the project
- Engage with the suptech community through the Lab's hackathons and techsprints
- Be introduced to the global community of regulators and supervisors, investors, academics and development partners that are collaborating with the Cambridge SupTech Lab during other events hosted by the Cambridge Centre for Alternative Finance (CCAF).

V. Vendor Selection and Project Implementation

Timeline

Following the receipt of Expression of Interest submissions from qualified vendors, a Request for Proposals (RFP) will be formally issued to three shortlisted vendors on March 19th, 2023. The invited vendors will have ten days to submit their proposal. The winner of the RFP will be announced on May 2nd, 2023, with work commencing within three weeks. This Project will ultimately deliver a prototype that will be tested by the Agency no later than November 2023.

Key features of this initiative

- Blind review process: A panel of expert reviewers will score anonymised proposals without knowing the name of the vendor submitting them.
- Competitor scorecard: Applications will be assessed by the panel using a set of scoring metrics and weighing the relative importance of each attribute.
- Rapid turnaround time: We will select the winning vendor and award 50% of the **US$100,000** within 48 days from submission of the final proposal. The last 50% of the award will be granted in one installment upon completion of the deliverables according to projected timelines.

Project Structure

The Project has four phases, elaborated below:

1. Kickoff and interface design, including technical integration specifications
2. Development of a working prototype
3. Integration and development of additional data analytics and/or visualization.
4. Testing and signoff of the working prototype

Throughout all project stages, vendors are expected to meet weekly with key stakeholders of the Agency as well as the Lab's Launchpad team, to ensure close coordination and agility.

1. KICKOFF & INTERFACE DESIGN, INCLUDING TECHNICAL INTEGRATION SPECIFICATIONS

During the first phase, the selected vendor (in coordination with the Lab's Launchpad team) will gather requirements from the Agency and produce an initial Design Document that includes integration and user interface specifications. This living document should include specifications for the client-facing portion of the prototype, communicated in a manner such that clients of the prototype can understand how to integrate with systems and processes, submit data, and use the system without necessarily understanding the entire architecture behind the software. This includes specifications for the data integration (analytics and visualization) phase of the project as well. This Document is to be shared as needed with any other key stakeholders (e.g., vendors of relevant software used by the Agency, any financial institutions needing to integrate) to allow them to develop integrations and/or adapt existing software during the development phase. The design document should also include criteria for user acceptance testing for use during the testing phase.

2. DEVELOPMENT OF A WORKING PROTOTYPE

The selected vendor will build a working prototype that delivers on the requirements laid out in the REOI, RFP, Project Agreement, and any modifications to scope agreed during the previous Phase 1.

The Detector system will first receive a small subset (a representative sample) of all data required in a controlled environment. Initial data being submitted via the Detector will be sample data to start, with real data only being introduced to the system once proper security protocols and data sharing agreements are in place. Starting with a prototype and a small data set will allow the vendor to quickly identify and address any unforeseen issues early in the Project development cycle. For example, this data may include:

- Meta data from app stores
- Data on registered financial institutions from the website of the Agency's published data

- Data from sample apps previously collected, pertaining to both good actors and bad actors.

Once agreements are in place, the Detector's model can be trained, tested, and validated on more sensitive real data, complaints data drawn from the Agency's complaints system.

The working prototype will also facilitate candid discussions among Project stakeholders regarding issues such as model interpretability, potential externalities, and the like.

3. INTEGRATION AND DEVELOPMENT OF ADDITIONAL DATA ANALYTICS AND/OR VISUALIZATION.

Once the working prototype has been developed, tested, and accepted, the vendor will provide any analytics and visualization tools defined during the design stage.

Additionally, the selected vendor should (i) assess the needs of the Agency to understand which dashboards, reports, and statistics are most useful and/or difficult to produce; and then (ii) propose and develop a prototype mechanism for extracting and visualizing this information from data consumed, processed, and produced by the Detector working prototype. This could involve creating custom queries, scheduling the generation of reports, and outputting in various formats.

The final UI of the prototype must be done before the final tests of Phase 4.

4. TESTING AND SIGNOFF OF THE WORKING PROTOTYPE

Once the proof of concept has been completed to the satisfaction of the involved parties, integration and testing with real institutional data can begin. The working prototype will be tested with the Agency, based on any user acceptance criteria defined during the design stage, to allow the vendor to ensure that the prototype Detector can handle the acceptance, reporting, and detection of fraud within real data before the it is scaled into full production. This approach also minimizes the risk of interruption due to unforeseen technology failure and serves to inform estimates of the cost to scale the prototype to a production-grade service.

A cyclical final test of the prototype and improvements by the developers must be done until the product is adherent to the functional specification document.

VI. Rules and guidelines

Submission Requirements

Interested vendors must demonstrate that they are qualified to perform the services required for the Project. In particular, interested vendors are asked to address the following requirements in their submission in a format capable of being read by Microsoft Word, which should together be **no more than 8 pages in length** (minimum 11-point font):

1. Company background (including technical and managerial capabilities of the executives).
2. A list of past projects representative of the experience of the company and the executives.
3. Information on the qualifications of key staff to be involved in the Project, including whether they have experience working on suptech projects.
4. Summary of your working experience in the following geographies: (1) Philippines; (2) Indonesia; (3) Ghana; (4) Peru; (5) India.
5. Examples of prior experience related to the development of this solution prototype or similar technological solutions.
6. Indicative development / implementation schedule based on the timeline set out above.
7. Detailed description and examples of technical prowess that address both components of the key vendor requirements in section III.

All materials should highlight the relevance to the required solution described in this document.

Supporting documents may be submitted (e.g., company brochures, case studies, CVs, etc.) as attachments to the submission email. No page limits apply to these attachments, but evaluation will be based primarily on information included in the main body of the EOI.

Any questions prior to the submission deadline should be sent via email to Cambridge SupTech Lab's Launchpad at suptech-launchpad@jbs.cam.ac.uk with subject line "REOI: Cambridge SupTech Lab – Intelligence on Fraudulent Fintech Apps Project".

Disclaimer

This document is not a request for proposals. The Lab reserves the right to edit, invalidate, terminate, and/or reissue this REOI at any time and for any reason. The Lab also reserves the right to select a vendor through an alternate method and/or adopt an alternate timeline for vendor selection that differs from the method and/or timeline described in this document, the websites of the Lab and Launchpad, and any other communications related with the process. Furthermore, the Lab expressly disclaims responsibility for any costs incurred by any vendor in responding to this REOI, regardless of whether the REOI is edited, invalidated, terminated, and/or reissued at any time and for any reason.