Securely sharing sensitive intelligence among multiple parties for AI-driven fraud prevention

Fraudprotect **is startup that aims to build anti-fraud models and solutions for finance and payment companies. Due to an increase in fraudulent transactions for many customers, an online payment service provider hired Fraudprotect to develop a strategy to reduce this fraud.**

To construct a robust anti-fraud system, Fraudprotect would require consumer transaction information (which includes the money spent, when, and on what) from their client.

The online payment company provides them with data, but the data is highly protected with limited and restricted access.

If intelligence is transmitted in a secure and trustworthy manner

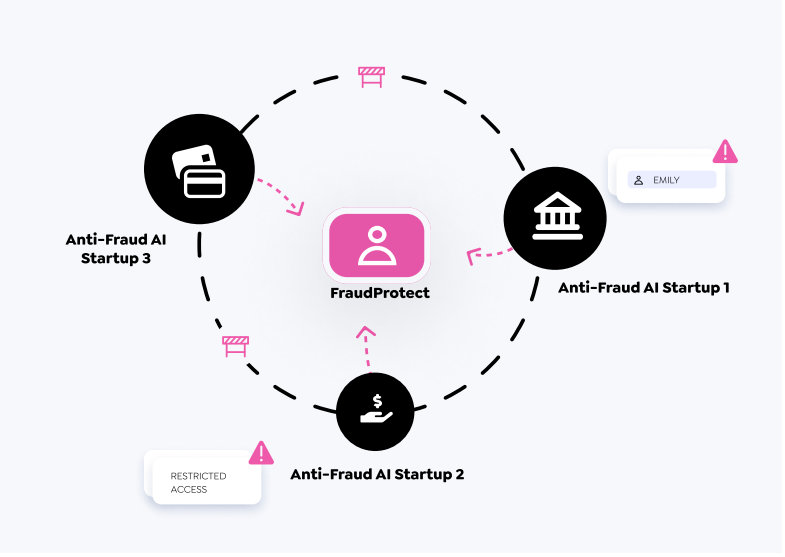
Fraudprotect **can benefits by**

- Building accurate services since they will have more access to data
- Reusing their models in other contexts as the basis of their models is strong

Data providers or financial service providers benefits by-

- Accessing fraud intelligence from the entire ecosystem (which include banks, online payment services, credit card compaines) rather than just their own data

The Challenge : Gap in Trust



Fraudprotect will develop a model that will be extremely effective in detecting and blocking fraudulent transactions. However, the online payment service provider only gives limited data with limited access to Fraudprotect, and the following issues persist:

⚠ The cold-start problem

To begin with, there is insufficient data for Fraudprotect to develop a basic model for their solution as the data provided contains proprietary and sensitive elements related to financial transactions.

⚠ Privacy

The transaction data shared is non-public and may contain personal information such as credit card numbers and location. This data is heavily regulated and overseen by rigorous privacy rules, making it extremely difficult for organizations like Fraudprotect to work with. It is costly and time-consuming to demonstrate privacy and trust with various parties.

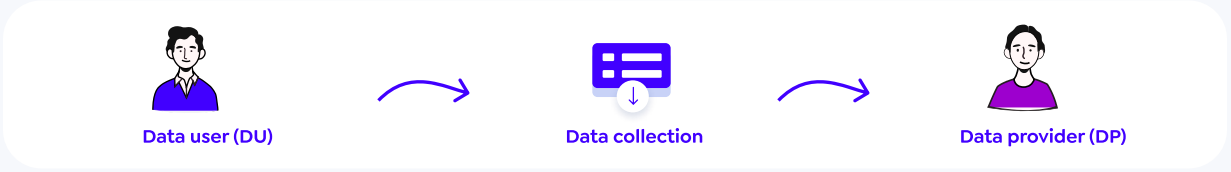
⚠ Establishing a feedback loop

Setting up an efficient feedback loop on a simple model built with limited and constrained inputs becomes difficult. Fraudprotect is unable to update the model and achieve SOA performance as a result.

Will Fraudprotect be able to gain full access to this data from their client in order to construct a more effective anti-fraud system?

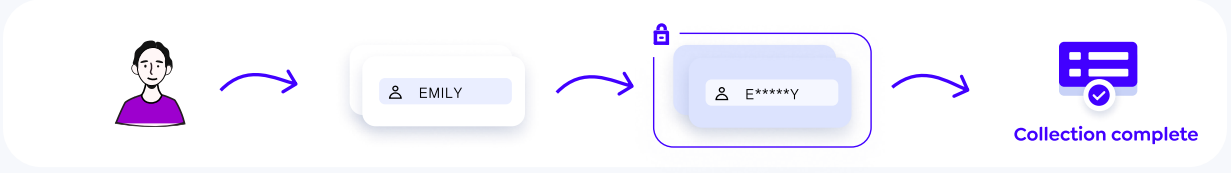
The Solution : Fluid Platform

An end-to-end platform that provides a privacy-first, win-win solution!



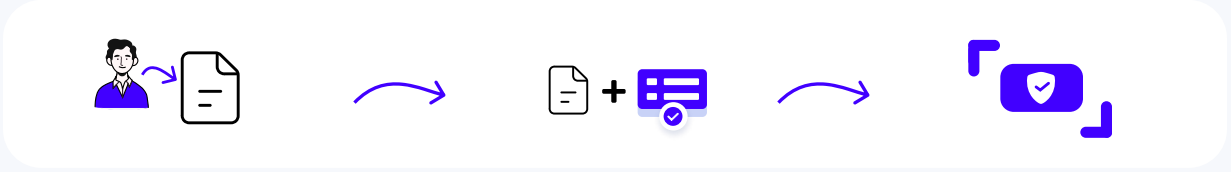
1. Data User creates a Data Collection

2. Data User specifies the data and sends the request to the Data Provider



3. DP applies the policies and shares the data. DP has the power to revoke access

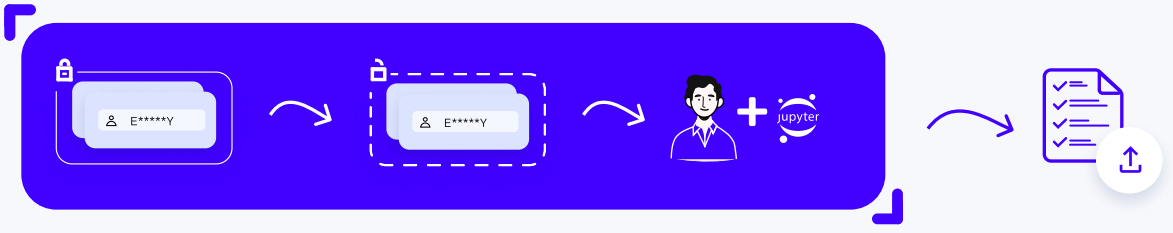
4. Data is stored in an encrypted form, and can only be accessed in Secure AI Enclave.



5. Du creates a new project.

6. Attaches the Data Collection to the project

7. Initiates the Secure AI Enclave



8. Encrypted data can be accessed and decrypted only in the Secure AI Enclave.

9. DU can Explore, Analyze data, Train and Deploy AI models- through a Jupyter notebook

10. DU can export the result

Fluid platform enables all parties to collaborate and make the most of their sensitive data. For this collaboration to go smoothly, Fluid provides several key features:

Simplified collaborations

Get intelligence from partners without 'seeing' the sensitive parts of data - avoid hundreds of hours of manual coordination and ad-hoc processes.

Zero-risk data science

All access within secure enclave with built-in data science tools and 100% observability where CreditMart data scientists can access data without compromising Lender's conditions

Attestation as proof of privacy

Technologically verifiable evidence that all access was as per the purpose and controls prescribed by the Lenders (Data providers)

The Fluid effect : Win-Win for all

CreditMart- Access to deeper consumer insights

- Significant time reduction for taking experiments to the market
- More accurate contextualization of credit offerings
- High predictability in qualifying of leads
- Audit-ready proof of privacy for customers from Day 1
- More client relationships without compliance overheads

Lenders - Gaining value from data without risking exposure

- Improved consumer-centric service without compromising trust and privacy
- Better quality leads for their credit products and loans
- Fully compliant on sensitive data without overheads on technical and legal teams' workloads
- Better financial inclusion for their products

Other Use cases of Fluid

Better fraud detection through co-opetition

Among various companies who can now pool their transaction data to identify and mitigate various flavours of fraud.

Privacy-first marketing and advertising

By bringing consumer insights from various sources, without risking exposure of first-party cookies and personal information.

Schedule a Demo + Consulatation

BOOK