ESTO AS

Vadim Kööp

Fraud Manager assignment

Tallinn 2025

Table of contents

List of figures

List of tables

1. Overview

A Fraud Manager at ESTO must be able to innovate and have a high-level vision for fraud prevention strategies, as well as execute projects by bringing together stakeholders and diving into technical details. The Fraud Manager is involved in all steps of the fraud management process, from risk assessment to implementation of controls and continuous monitoring. The Fraud unit focuses on protecting ESTO's financial ecosystem by developing sophisticated detection systems, verification processes, and rule-based engines that safeguard both our business and customers. The goal is to minimize financial losses from fraudulent activities while maintaining a smooth customer experience that doesn't unnecessarily impede legitimate transactions. ESTO currently operates in all Baltic countries, requiring the Fraud Manager to understand and adapt to varying fraud patterns and regulatory requirements across these markets.

1.1 Introduction

You are responsible for assessing the risk of fraudulent loan applications. We want you to come up with a concise and structured fraud detection framework for new customer onboarding. Your solution should demonstrate your ability to identify fraud risks specific to digital lending, implement appropriate verification measures & balance security with customer experience.

Information available when a customer signs up:

1 Personal Information
2 Name – first name + last name
3 ID code – personal ID code of the customer
4 Address – customer's self-reported address
5 Phone number
6 Email address
7 IBAN (bank account number)
8 Occupation category – self-reported (private sector employee; public sector employee; retired; student; entrepreneur; under government allowance; unemployed)
9 Net income (self-reported)
10 Monthly expenses (self-reported)
11 Monthly financial liabilities (self-reported)
12 Loan type (small loan; hire purchase; credit account)
13 Loan amount
14 Login method (Smart-ID; Mobile-ID; ID-Card) Where is password method? (Esto "Log in or register" form)
15 IP address
16 Official income data – from an official government provider that includes employer information and net income over the past 6 months
17 Bank statement – contains all transaction history (both incoming and outgoing) over the last 6 months

1.2 Tasks

1 **Data enhancement Identify and justify 3-5 additional data points/verifications you would collect/do during onboarding to strengthen fraud detection capabilities. For each data point:**
- Explain what specific fraud risk it helps to mitigate
- Describe how it would be collected (e.g., direct from customer, third-party API, etc.)

2 **Fraud detection framework Design a step-by-step fraud verification workflow that would apply to all new loan applications. Your framework should outline a multi-layered approach that includes:**
- Automated checks (specify which checks occur at which stage)
- Manual review triggers (what conditions would flag for human review)
- Decision points (how fraud risk levels are determined and corresponding actions for each level)
- Recommend specific third-party integrations to enhance verification capabilities

Note: We don't need to go into country specific details here. Think of a unified process that would be suitable across all countries.

3 **Implementation considerations**

Brief outline:
- How you would measure the effectiveness of your fraud framework?
- Key metrics you would track to monitor performance?
- How you would balance fraud prevention with customer experience?

Submission Format

Please prepare your response as a structured document with clear sections addressing each part of the assignment. Visual elements such as flowcharts for the fraud workflow are encouraged but not required.

2. Data Enhancement

To improve the fraud detection capabilities during customer onboarding, I propose collecting and verifying the following **six additional** data points or verification mechanisms. These additions are designed to uncover next patterns:

- Device-level fraud.
- Synthetic identities,
- False income claims,
- Identity manipulation.

Currently, such patterns are the most common threats in the digital lending environment.

2.1 Device Fingerprinting and Digital Footprint

Fraud Risk Mitigated:

- Synthetic identity fraud,
- Automated bot submissions,
- Device sharing within fraud rings,
- High-risk customers with no digital presence,
- Use of temporary or disposable contact details.

Description:

Device fingerprinting creates a unique identifier for a user's device by analyzing browser and system attributes such as browser type, version, timezone, screen resolution, and installed fonts. This technique helps detect if the same device is used to submit multiple loan applications or has a history of fraudulent activity.

By analyzing the age, activity, and connectedness of a customer's email address and phone number, it's possible to estimate the legitimacy of their digital identity. Fraudsters often use freshly created email accounts or phone numbers from VOIP services. A digital footprint score provides a fast and effective signal of whether the person exists online in a meaningful, traceable way.

Collection Method:

- Collected passively during the onboarding session through a third-party API integration (for example: FingerprintJS, SEON or ThreatMetrix).
- Third-party identity risk scoring APIs (for example: Ekata, SEON) evaluate data based on historical usage, social media presence, and known fraud databases.

2.2 Behavioral Biometrics

Fraud Risk Mitigated:

- Identity theft or account takeover,
- Bot attacks and scripted submissions,
- Use of proxy or remote-controlled sessions.

Description:

Behavioral biometrics monitor the user's physical interactions, including typing speed, keystroke patterns, mouse movements, scrolling behavior, and mobile gestures. These patterns are nearly impossible to replicate and can reveal whether a human or a bot is completing the onboarding. They can also help detect whether the person is familiar with the data being entered, which helps uncover impersonation fraud.

Collection Method:

- The process is invisible to the user and doesn't affect the experience.
- Collected passively through the user interface using JavaScript-based libraries (for example, BioCatch and BehavioSec).

2.3 Enhanced Address Verification with Geolocation Cross-Check

Fraud Risk Mitigated:

- Synthetic identities,
- Cross-border fraud attempts,
- Use of fake, incomplete, or mismatched address data.

Description:

While customers self-report their address, it can be cross-verified using IP geolocation and, if the onboarding occurs via mobile, optional GPS data. Mismatches between the reported and actual physical locations can indicate fraud or identity misuse. However, in cases where a legitimate user is located in a different country during the onboarding process (for example: traveling, on business, or vacation), the system should allow for flexibility. A geographic mismatch could occur even with accurate address data, so additional verification steps may be required to confirm the user's address, such as confirming via email, mobile verification, or submitting supporting documents.

Collection Method:

- IP-based geolocation is captured automatically during onboarding, providing the user's approximate location.
- For mobile devices, location services (GPS) can be enabled to triangulate the user's position.
- Browser geolocation API may be used to estimate the user's location, especially when they are on a computer.
- Address verification services (for example: Loqate, Melissa) can validate the structure and legitimacy of the reported address.
- In cases of geolocation mismatches, users can be asked to provide further verification through alternative methods, such as mobile verification or submitting proof of residence.

2.4 Selfie with Liveness Check and Document Matching

Fraud Risk Mitigated:

- Identity theft,
- Synthetic identities,
- Deepfakes and document forgery.

Description:

A customer is prompted to take a selfie with liveness detection, and this image is matched to an uploaded or government-verified ID. Advanced biometric verification ensures that the person is real and physically present during onboarding - not a photo, video, or bot.

Collection Method:

- Directly from the customer using a smartphone or webcam.
- Integrated through providers like Veriff, Onfido, Jumio, or iDenfy.

2.5 IP Reputation and VPN/Proxy Detection

Fraud Risk Mitigated:

- Cross-border loan application fraud,
- Bot attacks or coordinated fraud attempts,
- Anonymized fraud (use of proxies or TOR).

Description:

Checking the IP address against global threat intelligence databases allows identification of suspicious patterns such as use of blacklisted IPs, public VPNs, datacenter IPs, or TOR nodes.

Collection Method:

- Collected passively from the user session.
- Verified through IP intelligence providers (for example: MaxMind, SEON, IPQualityScore).

2.6 Public Database Cross-Check (PEP, Sanctions, Watchlists)

Fraud Risk Mitigated:

- Use of stolen identities,
- Money laundering risks,
- High-risk customers from sanctioned entities.

Description:

Cross-referencing a user's identity against politically exposed persons lists, sanctions databases (Office of Foreign Assets Control, European Union, United Nations), and criminal watchlists adds a layer of due diligence and aligns with anti-money laundering (Anti Money Laundering) standards.

Collection Method:

- Fully API-based, real-time, and invisible to the customer,
- Identity data submitted by the user is automatically checked through providers like ComplyAdvantage, Refinitiv, or World-Check.

2.7 Summary

These additional data points are especially useful for building a multi-layered fraud defense system that starts from passive data collection and escalates verification depending on risk level. It can be combined into a risk-based onboarding system where low-risk users are onboarded quickly, and high-risk users go through more extensive checks. Furthermore, authenticator APPs or SMS confirmations can be integrated, but it is optional.

3. Fraud Detection Framework

The following fraud detection framework outlines a unified, scalable, and multi-layered process that can be applied across all countries for onboarding new loan applicants. It balances automated efficiency, intelligent risk scoring, and human oversight where necessary.

3.1 Step-by-Step Workflow Overview

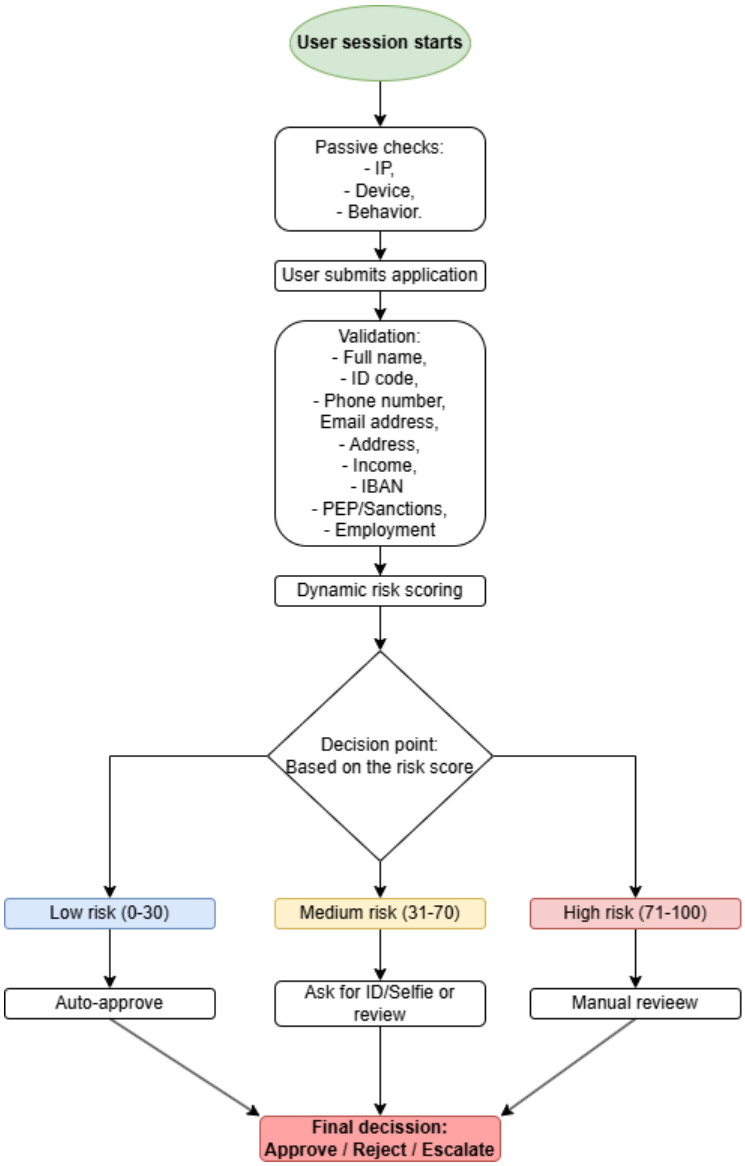

Figure 1. Step-by-step fraud verification workflow diagram.

Stage 1: Initial Data Collection & Passive Risk Profiling

Occurs as soon as the user lands on the onboarding page.

Automated Checks:

- Device fingerprinting,
- VPN/proxy/TOR detection,
- IP address analysis & geolocation,
- Email/phone number structure validation,
- Digital footprint scoring (email, phone, IP, domain age),

- Behavioral biometrics (mouse movement, typing patterns).

Purpose: Identify anomalies and assign an initial risk profile before user submits the application.

Stage 2: Application Submission Validation

Triggered when the user submits their personal, financial, and employment data.

Automated Checks:

- Run sanctions/PEP/AML checks,
- Address consistency versus Geolocation,
- Name, ID, address, and IBAN format validation,
- Verify employment data via payroll API (if available),
- Cross-check self-reported income with official income data,
- Fraud pattern matching (for example: reused IBANs, duplicate devices).

Purpose: Validate structured data inputs and look for contradictions or high-risk indicators.

Stage 3: Dynamic Risk Scoring and Categorization

Performed after data enrichment and validation.

Risk Scoring Factors:

- Device reputation (shared/blacklisted),
- Geolocation and document consistency,
- Employment verification success/failure,
- Financial data mismatch (declared vs. official),
- Digital ID strength (email/phone age, footprint),
- Behavioral trust score (human vs. bot behavior),
- Past fraudulent flags (internal or third-party data),
- Scoring Output: A dynamic fraud risk score (0–100) is calculated using weighted factors. This score determines the next step in the process.

3.2 Manual Review Triggers

Applications are automatically flagged for human review under the following conditions:

- High fraud risk score (for example, > 70),
- Device/IP used in previously flagged applications,
- Selfie/document mismatch or failed liveness check,
- Repeated submission attempts with varying details,
- Mismatch between declared and verified income/employment,
- No verifiable digital footprint (email/phone too new or suspicious),
- Suspicious transactions in uploaded bank statements (gambling, crypto exchange, payday loans, etc.).

Manual reviewers receive a risk summary dashboard showing red-flagged data points and raw inputs for context.

3.3 Decision Points and Actions

Risk Score Range	Review Level	Outcome
0–30 (**Low**)	Fully automated	Auto-approval
31–70 (**Medium**)	Conditional verification	Ask for selfie/ID or light review (passive checks before final decision)
71–100 (**High**)	Manual review required	Rejection or escalated verification (fraud investigation depending on local policies)

Table 1. Table of decision points and actions.

3.4 Recommended Third-Party Integrations

To support this framework, the following services are recommended:

Needs	Recommended Tools
Device fingerprinting	FingerprintJS, SEON, ThreatMetrix
Digital footprint scoring (email/phone)	Ekata, SEON, Emailage
Behavioral biometrics	BioCatch, BehavioSec
Identity document check + selfie match	Veriff, Jumio, Onfido, iDenfy
IP reputation / VPN / TOR detection	IPQualityScore, MaxMind, SEON
PEP, Sanctions, AML checks	ComplyAdvantage, Refinitiv, World-Check
Risk scoring engine (optional orchestration)	Sift, Feedzai

Table 2. Table of methods and recommended tools.

3.5 Summary of the Workflow

1. **User Session Starts:** Passive risk profiling begins immediately,
2. **Application Submitted:** Data enrichment and validation with external sources,
3. **Risk Score Calculated:** Fraud level assessed using multi-point scoring,
4. **Next Step Determined:** Automated decision or flag for review,
5. **Manual Review (if needed):** A human evaluates high-risk applications,
6. **Final Decision:** Approval, conditional request, or rejection.

4. Implementation Considerations

A well-designed fraud framework must not only detect and prevent fraud effectively but also adapt over time, remain transparent, and ensure a seamless experience for legitimate users. Below are the core implementation considerations across three pillars:

- Monitoring,
- Measurement,
- Customer experience.

4.1 Measuring Effectiveness

To assess how well the fraud framework is performing, I would implement both quantitative and qualitative methods. The key goal is to understand the framework's ability to detect fraud early, reduce financial losses, and minimize false positives.

Approach:

- Conduct A/B testing: Compare fraud detection outcomes between the current setup and the new framework on a sample of applications.
- Implement a fraud risk score tracking system to analyze patterns and refine weightings.
- Periodically run retrospective analysis on confirmed fraud cases to identify missed signals or weaknesses.
- Collect feedback from manual review teams to refine scoring logic and rule triggers.

Additional Tools:

- Machine learning models can be used to retrain based on new fraud cases and evolving behaviors.
- Alerting systems can be set up for sudden changes in fraud rates or unusual applicant behaviors.

4.2 Key Metrics to Monitor

A strong fraud framework must be data-driven. Below are the most important metrics I would track continuously:

Indicators	Purpose
Fraud Detection Rate (True Positive Rate)	Percentage of fraud cases successfully caught before disbursement.
False Positive Rate	Rate at which legitimate users are flagged or rejected.
Manual Review Volume & Pass	Rate that measures efficiency of human reviewers and decision logic.
Approval Rate by Risk Band	Insight into how each risk category performs in terms of conversion.
Average Time to Decision	Evaluates speed of processing and customer satisfaction.
Fraud Losses per Approved Loan	Tracks financial exposure and the cost-effectiveness of the system.
Drop-off Rate During Onboarding	Identifies friction points causing good users to abandon onboarding.
Re-offending User Rate	Checks whether known fraudsters are re-entering through new identities.

Table 3. Table of indicators and monitoring objectives.

4.3 Balancing Fraud Prevention with Customer Experience

Fraud controls must be smart enough to detect risk without creating friction for good customers.

Use Risk-Based Layering

- Apply lightweight, invisible checks (for example: device fingerprinting, IP checks) to all users by default.
- Escalate to more checks (for example: selfie, document upload) only for medium or high-risk applicants.

Minimize False Positives

- Continuously tune thresholds based on feedback and confirmed fraud,
- Leverage behavioral biometrics and digital footprinting to reduce reliance on hard KYC for low-risk cases.

Offer Guided and Assisted Verification

- If additional verification is required, provide a clear explanation and easy-to-follow steps.
- Allow customers to save progress and return later if they can't complete the onboarding in one session.

Provide Fast-Track for Trusted Users

- For returning customers or users with verified digital IDs, allow streamlined onboarding with fewer steps.

4.4 Summary

A fraud detection framework is only as valuable as its ability to evolve, perform consistently, and retain legitimate customers. With the right metrics, feedback loops, and customer-centric approach, we can create a system that's not only secure, but also scalable, adaptive, and user-friendly.