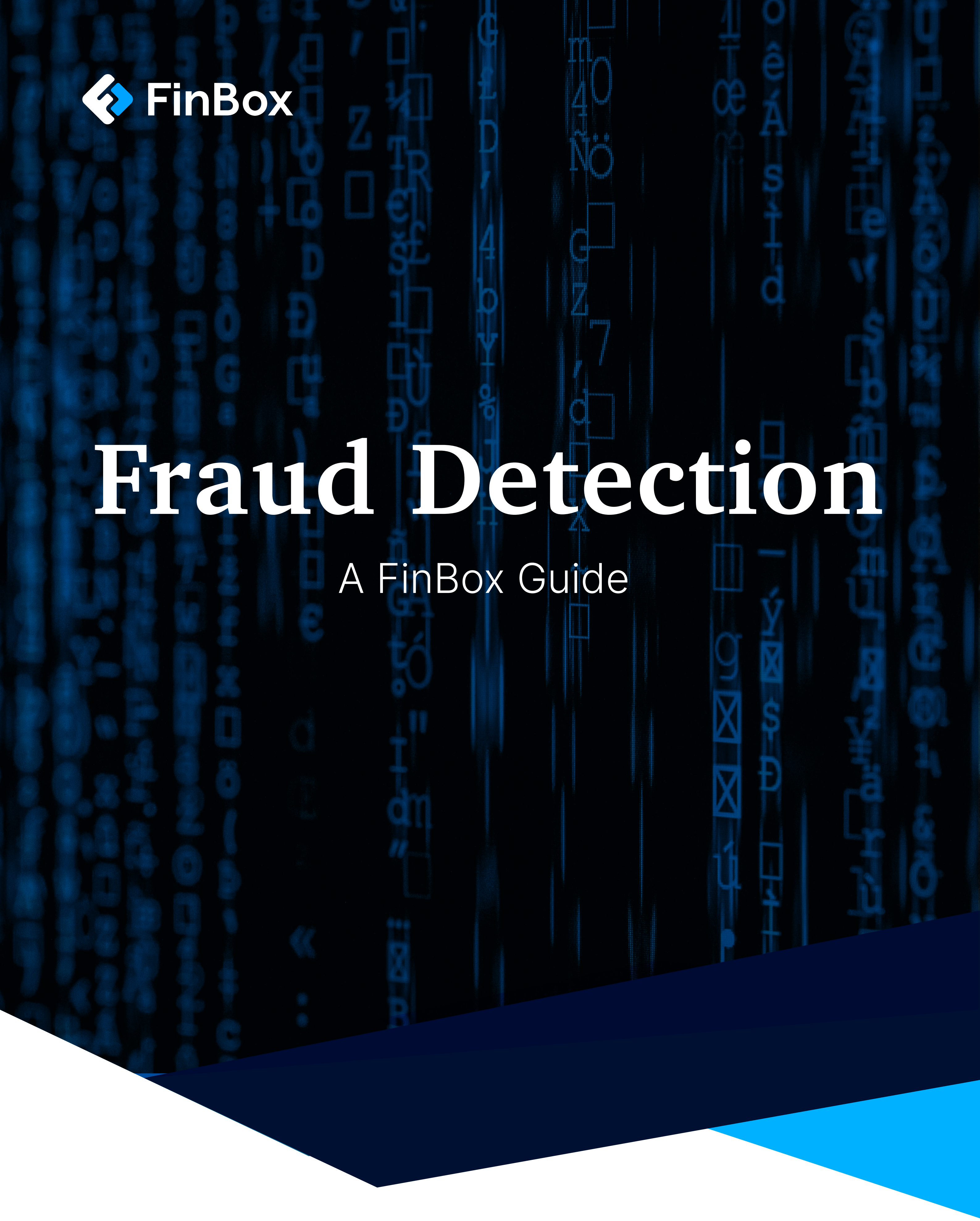


FinBox

Fraud Detection

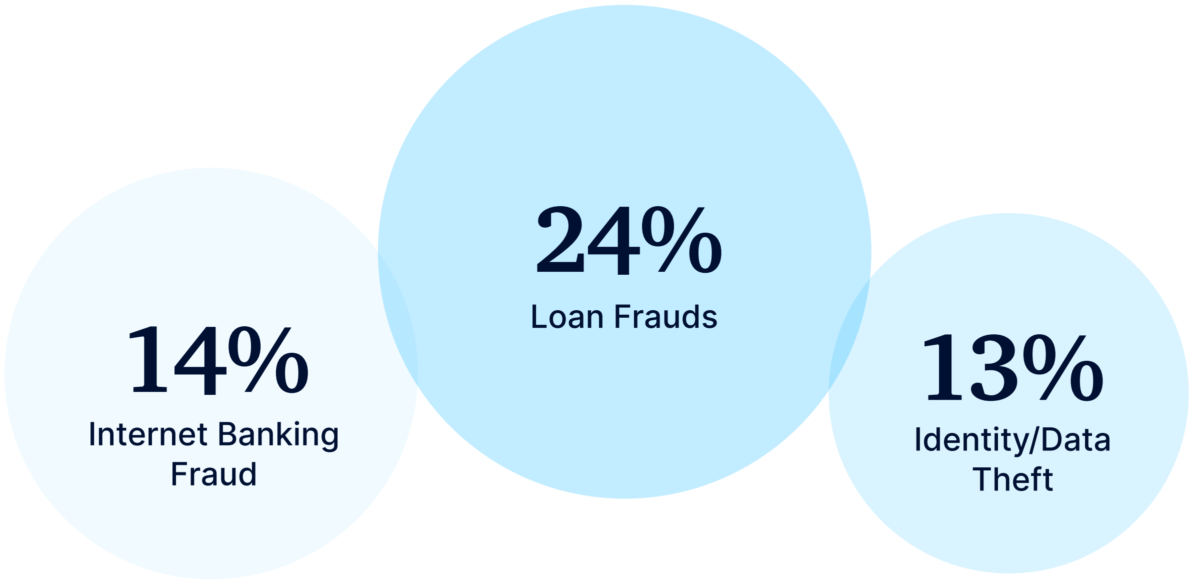
A FinBox Guide

www.finbox.in

Introduction

If one asks a banker what keeps them up at night, it's likely to be the risk associated with fraud. Irrespective of the safeguards, fraud is almost inevitable in today's hyper-digitalised world. A Deloitte survey reveals that banking fraud will continue to rise in the future.

The same survey also showed that bank executives are most concerned about loan frauds (24%), mobile/internet banking fraud (14%) and identity/data theft (13%).



14%
Internet Banking Fraud

24%
Loan Frauds

13%
Identity/Data Theft

The Reserve Bank of India (RBI) data, which might miss a lot of unreported frauds, revealed the following:

FRAUDS IN 2021-2022 WORTH

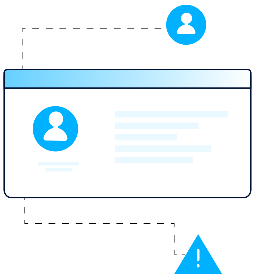
₹60,414 crore

OVER THE LAST 7 YEARS, BANKS HAVE LOST

₹100 Cr/day

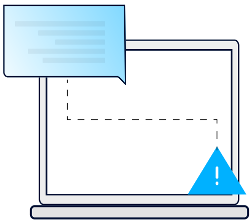
For every rupee lost to fraud, the total cost to business is actually much higher due to network fees, increased operational costs, and data enrichment.

Common types of frauds



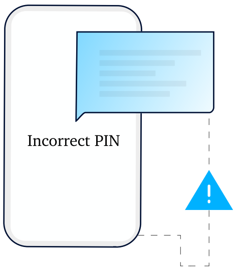
Identity Fraud

One of the most pervasive fraud schemes is identity theft. Identities can be stolen, bought on the dark web, or synthesised. Fraudsters can buy stolen credentials for as little as $15 on the dark web, and they can be sold for upto $500 too. Synthetic IDs on the other hand incorporate disparate elements of real identities to look believable, such as a photo from one PAN card and an address from a different Aadhaar card.



Behavioural Fraud

Any deviation from regular programming could raise a behavioural red flag. If a potential borrower has installed/uninstalled lending apps in a window of say two months, or they've spent more than they usually do, or have recieved more cash deposits than their usual salary credit, it can raise alarms on a well-trained machine learning model. A behavioural fraud then acts as an alarm for fraudulent activity and/or incoming delinquency.



Transaction Fraud

Any transaction in the account that was not authorised directly by the card/account holder is considered to be a fraudulent transaction. But it could also consider things like a business account that hasn't had any credit transactions in the last 15 or 30 days, or even payments that are in oddly rounded numbers such as multiples of 100.

Fraud detection

At its core, fraud detection is the cornerstone of a good risk management strategy. And all good fraud detection solutions should be rule-based. The way we look at it at FinBox, rule-based fraud prevention techniques let you automatically approve, review or block user actions.

A fraud detection rule is simple - it helps you decide if an activity is fraudulent or not. The rules can be based on correlation, statistics, or logical comparison. All fraud rules need data to be activated. For example, the data could be an IP address - let's say you know that an IP address belongs to a fraudster and it appears on a blacklist.

The most basic type of rule based on if/then logic would be -

If IP address = 192.169.1.2, then block website access.

Of course, the only way to make fraud detection more effective and efficient is to have more access to data (via data enrichment). It allows for greater precision while deciding what is considered fraud and what is not. Stacking multiple rules allows businesses to build a fraud scoring mechanism to mitigate risk as they see fit.

At FinBox, we can broadly categorise fraud detection rules in the following ways - it runs from basic, static rules to more complex velocity checks. The more complex ones are put in place to analyse behaviour rather than looking at single data points.

Static rules

A static rule is the most straightforward fraud rule - it follows the if/ then logic. It is considered static because the outcome of the rule is inflexible and strict - for instance, blocking a user action.

The earliest static rules had to do with IP addresses. If an IP address was found on a blacklist, a transaction would be blocked. However, static rules can get creative based on the data you have at hand.

For instance, one of the most common types of frauds we find is people tampering with the bank statement - it can range from duplicating transactions from another account to changing the metadata of the PDF file itself.

How do we detect fraud then? For instance, based on the data we've collected, we know when a PDF is edited based on the name of the author. Static rules in fraud detection for a bank statement can be based on a few things

- ⚠ The user has tampered with the statement (based on the PDF author name)
- ⚠ The user has modified one transaction but hasn't modified the balance amount - this scores as an inconsistency and pushed for further review
- ⚠ The user could be rotating credit - deposit money from account A, for instance, into account B to appear like the user has enough balance to avail credit and push it back to account A
- ⚠ Transaction fraud - Usually, salaries aren't credited in multiples of 1000s. However, if there is a transaction of INR 50,000 with the 'salary' tag - it could be flagged as potential fraud.

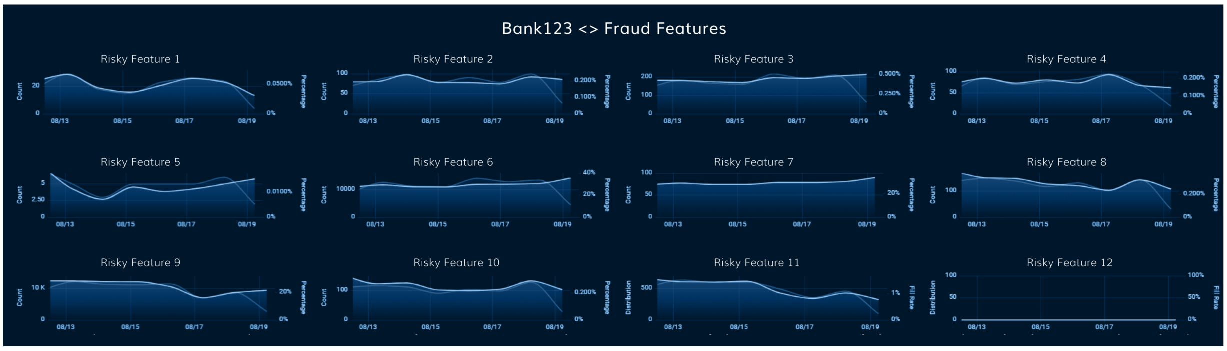
While static rules are extremely useful and sophisticated, one big downside is that it could give rise to false positives - basically, flag fraud where there is none. For instance, in device-based underwriting a loan application could be flagged for fraud based on how many times a phone has been rebooted or whether it is rebooted at all.

False positives are harmful for business. If a potential customer is wrongly flagged as fraudulent, there's a chance of your Net Promoter Score (NPS) dropping and consequently, your bottomline. **Which is why static rules are better utilised as indicators.**

Risk scoring rules

Scoring rules are essentially in place to inform a risk strategist about how risky a potential borrower is, based on certain actions and behaviours and are assigned risk scores.

As can be seen in the visualisation below, FinBox's machine learning models monitor multiple rules closely.



Based on these rules, each feature is given a score to calculate how risky the user action is -and ultimately how likely they are to default as is seen below.

Risky App Features	Threshold Values	Share (Capture Rate)	Default Rate
Risky Feature 1	>0	0.04%	33%
Risky Feature 2	>0	0.02%	33%
Risky Feature 3	>0	0.20%	29%
Risky Feature 4	>0	0.54%	27%
Risky Feature 5	>0	0.25%	24%
Risky Feature 6		1%	27%

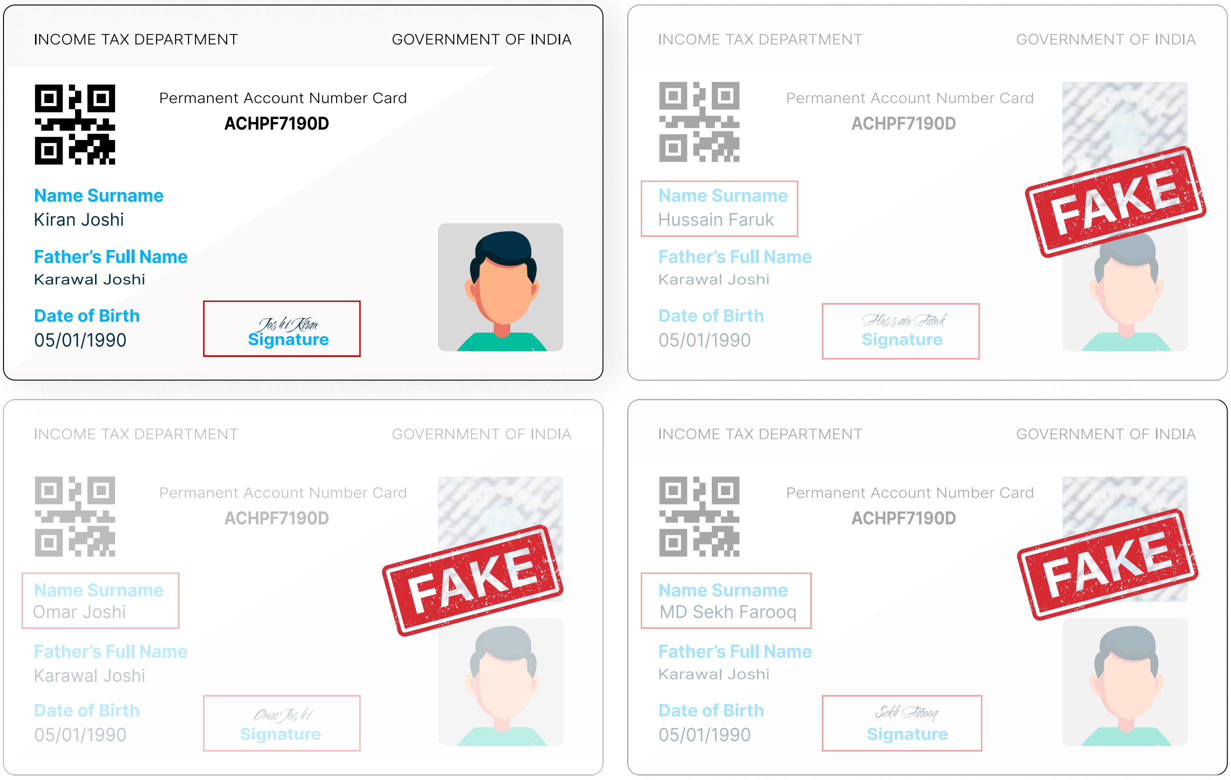
Risky feature 1, for instance, indicates the number of data editor apps a user has on his/her phone. As you can see, users who use such apps usually have a delinquency rate of 33%. This combined with other such suspicious behaviour, captures ~1% of the population with a very high delinquency rate.

Velocity rules

These rules are used to determine potential fraudulent actions based on behaviour patterns and their velocity.

The simplest understanding of velocity rules is the number of attempted logins on any website. If you've entered the password wrong more than a few times, you'll be logged out for a few hours or even up to a day. If businesses have no barriers there, potential fraudsters can use credential stuffing or brute force to crack the login details. A velocity rule would come in handy here. A rule could look at the number of attempts made within, say, five minutes.

If an applicant, for instance, applies multiple times using the same PAN card template, but changes names and PAN numbers, it can still be detected as fraud. It could look something like this -



INCOME TAX DEPARTMENT GOVERNMENT OF INDIA
Permanent Account Number Card
ACHPF7190D
Name Surname
Kiran Joshi
Father's Full Name
Karawal Joshi
Date of Birth
05/01/1990
Signature

INCOME TAX DEPARTMENT GOVERNMENT OF INDIA
Permanent Account Number Card
ACHPF7190D
FAKE
Name Surname
Hussain Faruk
Father's Full Name
Karawal Joshi
Date of Birth
05/01/1990
Signature

INCOME TAX DEPARTMENT GOVERNMENT OF INDIA
Permanent Account Number Card
ACHPF7190D
FAKE
Name Surname
Omar Joshi
Father's Full Name
Karawal Joshi
Date of Birth
05/01/1990
Signature

INCOME TAX DEPARTMENT GOVERNMENT OF INDIA
Permanent Account Number Card
ACHPF7190D
FAKE
Name Surname
MD Sekh Farooq
Father's Full Name
Karawal Joshi
Date of Birth
05/01/1990
Signature

Velocity rules apply at this stage to reject loans at the pre-disbursal check stage.

This rule could be triggered if any of the behavioural category frauds occur within a given time frame, say one day, for instance. It's largely used to monitor suspicious movements of money or build predictors for behaviour. If a user has availed multiple other loans within a short time frame, that could also be a velocity rule trigger. This can be useful in the context of AML (anti money laundering).

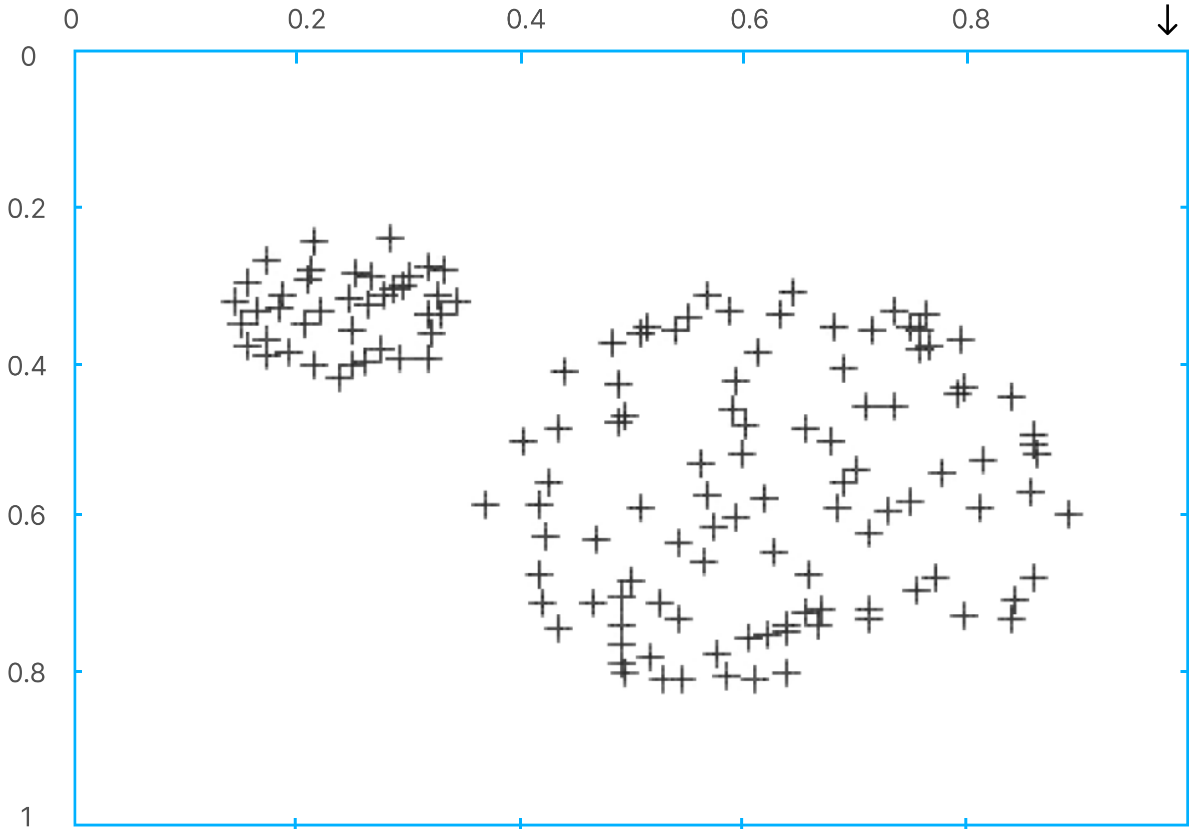
Machine learning rules

AI-driven ML models traverse through troves of data to analyse multivariate interactions in customer profiling data and spot suspicious patterns, which can not be detected through individual rules.

Segmenting customers and outlier detection through Neural Network-driven models, enables lenders to flag customers who are most likely to be fraudulent, who can then either be rejected automatically or manually investigated before disbursal. When there is enough data around credit card usage, for instance, and when there's a need to find the entities behind fraudulent activities or identify techniques used by fraudsters, clustering helps. Clusters, like in the figure below, help break down data to make patterns visible; this helps in outlier detection wherein dissimilar, inconsistent activities are detected.

At FinBox, our machine learning models run in real-time and gather data from devices as it happens. Machine learning models trained on extensive data means our deep learning models are highly efficient in flagging fraudsters.

Cluster Analysis



Fraud detection at FinBox

We're in the business of making lending decisions quick, efficient, and inclusive. That means relying on our rigorously trained machine learning models and carefully designed fraud rules to correctly assess potential borrowers.

We use our proprietary data products, DeviceConnect and BankConnect to flag fraudulent behaviour -

DeviceConnect

Think of this as an in-built fraud scanner and underwriting tool. It checks for the number of connected devices to a particular user, verifies identity via mobile/utility bills, all accessed via text messages; it also checks for apps that could potentially indicate fraudulent activity like SMS editor, data editor, fake GPS apps, and it also checks for whether or not your phone was rooted recently. DeviceConnect's fraud detection capabilities are based on these data points, alongside the triangulations, irregularities, and eccentricities in that data.

BankConnect

FinBox's bank statement analyser checks for document tampering, whether or not there's a mismatch in the user's details and the account details provided, whether the transactions in the bank statements match another bank statement, etc.

Our fraud methodology, a combination of the four fraud detection rules built, is enabled by our data products. In a study conducted by FinBox, we found that 7% is the average default rate. We backtested our fraud detection models and found out that out of the 2.2% population identified with fraud, 24% of them eventually defaulted.

This means our fraud detection methodology prevents defaults and damages at three-five times the average rate.

> Out of 2.2% population identified with fraud, 24% of them eventually defaulted.

Conclusion

We're in the business of lending and making credit accessible to largely underserved segments. Traditionally, credit scores are the result of payment history, debt burden, length and type of credit history; this is fast becoming an outdated system that is holding the economy back. The question then is how to redefine credit scoring, while ensuring more business for banks and ensuring customer satisfaction and trust. Our answers usually are a combination of a good work ethic and the power of big data analysis to not just generate optimal credit scores and collection timelines, but also fraud scores and new credit risk models.

It might seem challenging to build an efficient credit scoring model but it's entirely possible with the right tools. The challenge is in trusting personal information lenders acquire through standard KYC processes and avoiding fraud from stolen/synthetic identities.

But the good news is, your business can grow safely knowing that everyone has a digital footprint and with the right tools, they can be leveraged to not just detect fraud, but build customer loyalty.

Author's Bio

Rajat Deshpande
Co-Founder & CEO, FinBox

Rajat is a Fintech specialist and a startup enthusiast who started FinBox along with his co-founders with a mission to lay out digital infrastructure for alternate finance solutions. Under his leadership, FinBox has built multiple products in the Embedded Finance and Big Data credit analytics spaces. FinBox has enabled over 16 million lending decisions in India and SE Asia.
In his prior stints, Rajat was associated with the global consulting firm ZS, Citigroup and GoPigeon Logistics as Head of product.
He holds a Dual (BTech+MTech) degree in Mechanical Engineering from IIT, Bombay.

Anant Deshpande
Co-Founder, FinBox

Anant is a co-founder of FinBox. At FinBox, Anant leads lending and builds credit origination systems powered by alternate data and traditional data. In his earlier role at Home Credit, he drove Big Data-based loan underwriting of a $2B consumer loan portfolio. Anant has previously been associated with global consulting firm ZS Associates and TransOrg Analytics where he owned P&L and productised analytical consulting. He is a regular marathoner and holds a B.Tech in Chemical Engineering from Nagpur University.

Aparna Chandrashekar
Content Specialist, FinBox

Aparna is a content specialist at FinBox focused on building thought leadership, long form content and videos. Prior to FinBox, she was a journalist involved in disseminating news across formats, with a specialisation in TV journalism. She's worked with Reuters, ET Now and India Today as a reporter, writer, producer with a focus on business and policy. She holds a degree in Economics from NMIMS University and a post-graduate diploma in journalism from the Asian College of Journalism.

At FinBox, we are building the digital credit infrastructure and risk intelligence suite of the future. We provide full-stack API and SDKs for businesses to embed credit products into the platforms, and connect them with a diverse network of lenders. Our risk-intelligence offerings work seamlessly to improve conversions, onboarding experiences as well as overall NPS for a variety of digital credit products run by large lenders across the world

Book a demo

www.finbox.in