An effective approach to preventing application fraud

Experian Fraud Analytics

Experian™
Decision Analytics

complex²confident
The growing threat of application fraud

Fraud attacks are increasing across the world
Application fraud is a rapidly growing problem around the world. Economic hardship has driven increasing numbers of over-indebted individuals to misrepresent their qualifications for credit. Additionally, credit application processes are increasingly vulnerable to third party application fraud, because personal information commonly used for passwords and identity verification is no longer concealed. Much of this information is easily accessible on the Internet or via Social Media, and sophisticated fraudsters abuse it to commit application fraud.

Financial institutions are further vulnerable to fraud attacks since customers expect a rapid response to credit applications, even via those channels that do not require face-to-face proof of applicant identity. These factors, combined with other emerging trends, undermine the security of credit application processes.

At the same time, advances such as Chip and Pin technology have made it harder to commit transactional fraud, so fraudsters are increasingly turning to application fraud attacks. Application fraud has generated a serious and compounding leak in the profitability of financial institutions.

Applications increasingly vulnerable to fraud:
- Personal info available on Social Media
- Instant credit decisions expected
- Physical proof of ID not required

Transactions increasingly protected from fraud:
- Chip and Pin
- Validated card activation and password for online card use
- 3 digit security number

Figure 1: Credit applications are increasingly vulnerable to fraud

- Application fraud is a growing problem
- Over-indebted individuals increasingly misrepresent credit qualifications
- New transactional fraud defences has shifted third party fraudsters attention to the application stage
- Credit processes more vulnerable due to personal information shared on social media
- Demand for rapid response adds to vulnerabilities
Heavy application fraud losses hidden in “normal” bad debt
The frequency of application fraud is commonly under-estimated as resulting losses are often hidden amongst ‘normal’ bad debt. Analysis of fraud cases and non-fraud cases shows that fraudulent applications result in significantly higher credit amounts and loss rates. This is illustrated in Figure 2.

*Figure 2: Loss rates (%) and exposure amounts by fraud type*

First party fraud is fraud committed in a person’s own name. Third party fraud is fraud committed in the name of someone else. As can be inferred from the graphics, a low percentage of fraudulent applications cause a significantly higher percentage of total losses to financial institutions.

Experian uses advanced modelling techniques and qualitative methods based on expert knowledge to build rating systems that best suit each client’s circumstances, data and regulatory requirements.

The final models are the result of continuous interactions and workshops between our analytical team and the client, to ensure that they accurately and precisely meet pre-defined business needs and regulatory requirements.

Third party application fraud cases cause extreme losses
Third party fraud is a notorious form of application fraud often committed by organised crime rings that open accounts using stolen or synthetic identities.

It is essential to stop these cases at the application stage, since many of these will otherwise commit ‘bust-out fraud’. In its most costly form, fraudsters open accounts, establish transaction histories and even make payments to trick pattern detection technology into releasing repeated credit line increases, before disappearing after limit increases.
First party application fraud cases are heavily under-reported

First party fraud is fraud committed by the account holder. It results in losses that are less extreme than third party fraud for each case, yet is attempted in increasing volumes. A significant amount of fraud is misrepresented as bad debt, while analysis often reveals that it comes from the applicant’s deliberate attempts to mislead the credit providers.

It tends to involve the misrepresentation of income or credit qualifications, and can include deliberate misspelling of personal details to make debt collection more difficult, or to pass it off as third party fraud.

To understand the true situation, financial institutions need an objective, consistent process to assess each case. This enables fraud teams to assess accurately whether to collect from the first party or pursue third party fraud actions and obtain vital intelligence to improve overall fraud strategy.

Fraud losses tend to be significantly higher than “normal” bad-debt losses

Symptoms of fraud

The graphics below shows a range of defaulted cases ordered by their likelihood of being fraudulent. The diagnosis of fraud and non-fraud is based on the fact that fraudsters attempt to maximise the credit amount and rarely pay anything back.

The optimal operational definition of fraud may differ from firm to firm because the purpose of the fraud definition is to create an effective detection system to prevent the kind of fraud attacks that a specific financial institution experiences.
Optimal application fraud prevention strategies

**Strengthen fraud defences at the point of application**
Fraud and non-fraud losses are fundamentally different risks, so credit origination processes should have separate processes for fraud and non-fraud loss prevention.

Most fraud credits cannot be recovered once granted. Therefore, it’s essential for financial institutions to put in place a solid strategy for controlling fraud at the point of application. Fraudsters are drawn to the path of least resistance. Lenders with the weakest defences attract the most attacks and incur a disproportionate share of losses.

Credit scoring and credit policy rules are ineffective in preventing application fraud losses. Financial institutions need to implement fraud analytics for spotting and stopping it.

**Optimise the business impact of fraud prevention strategies**
Fraud prevention uses specialised technologies, information structures and predictive models. However all these elements should be used as part of a fraud prevention strategy that is set in order to contribute optimally to the origination business results.

The improved fraud process leads to optimised decisions, actions and priorities for both automated systems and manual effort of staff. The goal of the fraud prevention process is usually to maximise fraud loss savings net of fraud prevention costs.

We use advanced analytics to identify the optimal prevention strategy for the fraud prevention goal of the business. Figure 4 shows a (simplified) goal function that identifies the optimal level of prevention effort for a fraud prevention unit where the net fraud savings are maximised.

---

Fraud is a fundamentally different risk to non-fraud losses. Credit scoring is ineffective in preventing application fraud

---

**Simulation: Fraud losses and costs**

- **Fraud Loss Prevention** = \( L \)
- **Cost of Prevention** = \( C \)

**Simulation: Net Fraud prevention benefits**

- **Net Fraud Prevention** = \( L - C \)
- **Max benefit gained by reviewing the x% highest risk cases**

**Figure 4: Business Goal Function**

---

Fraudsters are drawn to the path of least resistance. Lenders with the weakest defences attract the most attacks and incur a disproportionate share of losses
Implementing application fraud prevention analytics

An effective fraud prevention solution identifies the applications most likely to be fraudulent. Every application is rated accordingly to its risk of fraud so investigators know which to review and which can safely be ignored.

This allows financial institutions to allocate fraud prevention resources more efficiently and focus investigators on cases with the highest likelihood of fraud, exactly where their contribution matters.

Experian’s framework for fraud prevention is based on four key development phases (Figure 5). These are customisable to each financial institution’s business goals and data assets to deliver a solution that helps identifying and controlling fraud in the most efficient way.

The development framework ensures all clients benefits from Experian’s global experiences.

Identifying and classifying historic fraud cases

Firstly, it is essential to correctly classify historic fraud cases and thus define the fraud event to be prevented. Experian consultants carry out a thorough analysis of the financial institution’s existing fraud management processes, data assets and historic fraud cases.

The quality of models developed for fraud detection is heavily reliant on the definition of the event to predict which should be aligned with the institution’s business and practice. This analysis is key to a strong fraud prevention solution.
Building fraud predictor information

This phase involves analysing new and existing data sources to create amalgamated information to predict fraud. All data available normally for application scoring is used, as well as new ways to derive more value out of existing and new data.

Examples of information created for use in fraud prediction models are:

a) Creation of batch or dynamic databases of linked fraud cases (fraud rings)
b) Deriving information on geographic concentrations of fraud cases and addresses with suspicious activity
c) Creating dynamic warning flags indicating inconsistent information between current and historic information across available databases (including previous applications, credit bureau data and other sources of internal and external data)

Experian’s research in these areas continuously identifies and tests new ways to acquire and use data in fraud management solutions that Experian delivers around the world.

Using advanced analytics for application fraud detection

Fraud is a complex problem that requires sophisticated solutions. Advanced fraud analytics is the core of Experian’s solution, and our specific method depends on each financial institution’s portfolio characteristics and data availability. Experian considers the following elements when recommending the most suitable analytical techniques:

• Fraud type
• Number of historic applications available
• Number of historic fraudulent applications available
• The scale of the analytical problem at application point

The relation between the data available and suitable analytical methods are summarised in Figure 7 below. If there are few applications or fraud cases, then expert models or unsupervised learning must be used. If a large volume of information is mined for instant, dynamic fraud detection, then a high performance Map and Reduce type NoSQL (Not only SQL) solution may be required.

![Figure 7: Data availability and analytical methods](image-url)
Selecting the right fraud strategy

Finally, the quantitative business model (goal function) is used to set the fraud prevention strategy. It simulates the business impact on fraud savings, prevention costs, detection rates, false positive rates and the delay of customer responses for any strategy.

After selecting a strategy, it is then translated into strategic segments with recommended actions and priorities on high-risk applications.

Benefits of Experian Fraud Analytics

Experian’s analytical solution for fraud prevention ensures that the **optimal fraud prevention effort is expended on new applications**.

Our fraud prevention solution ensures **faster and more profitable decisions and a better overall customer experience, while minimising fraud losses**. The solution focuses investigation effort based on fraud and false positive rates, minimises customer process delays and lost revenues.

Experian’s **fraud expertise, best use of data, and advanced analytics** form a unique and powerful combination to help financial institutions fight application fraud.

**Experian Fraud Analytics**

- Minimises fraud losses by identifying and focusing on the applications most likely to be fraudulent
- Ensures optimal fraud prevention effort is expended on new applications
- Enables faster, more profitable decisions and a better customer experience
Case study:
European bank identifies 52% of the fraud cases by only focusing on 5% of the lowest fraud scoring customers

Client
European subsidiary of a large international banking group

Business challenge
- Increasing levels of bad debt and write-off losses due to fraud in the loans portfolio
- Manual fraud prevention process not fast enough and incurred high operational cost

How Experian helped
- Data enhancing analytics
- Developed highly predictive models using several statistical multivariate and machine learning techniques
- Defined optimal strategy for the fraud prevention process through simulation and consultancy

Benefits
- Focusing on 5% of the population with lowest fraud scores identified 52% of fraud cases
- Fraud detection rate of reviewed cases > 9 times higher than portfolio average
- Manual refer costs paid back more than 19 times
- Higher customer service levels due to faster processing time

Figure 9: Trade off - detection rate versus refer rate

More than 50% of fraud can be detected by reviewing as few as 5% of all applications. This result is obtained by implementing Experian Fraud Analytics in the application process.