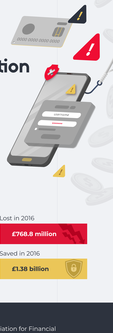
Fraud Management: Detection And Prevention In Banking Industry



Nowadays, the banking industry is facing an acute problem of fraud. The problem is global, and no country is fully protected. Fraudsters have become experts in hijacking online sessions: they steal client credentials and use malware to swindle funds from unaware account holders.

In his book "Future Crimes" Marc Goodman explains that **"criminals are often the first to exploit emergent technologies and turn their complexity against their users".**

According to Financial Fraud UK report, in 2016 financial fraud losses across payment cards, remote banking and cheques resulted in astonishing **£768.8 million**, an increase of 2% compared to 2015. At the same time, prevented fraud totaled **£1.38 billion** in 2016. The anti-fraud measures undertaken by the banks and card companies helped to save up to £6.40 in every £10 of attempted fraud transaction.

Lost in 2016
£768.8 million

Saved in 2016
£1.38 billion

Total 2016 financial fraud losses by type

The Association for Financial Professionals' 2016 Payments Fraud and Control Survey found that 73% of finance professionals reported an attempted or actual payments fraud in 2015. In the face of such threats, banking institutions are looking for the best options possible to fight against cybercrime.

Financial Fraud UK report

Data Analysis Software

One of these options is the use of data analysis software which, in most cases, guarantees an impeccable fraud detection. Modern systems allow fraud examiners to analyze business data and check how well the internal control system is operating. As the result, they can designate transactions that denote fraudulent activity or the elevated risk of fraud.

There is a spectrum of analysis measures that can be applied to tackle fraud. It ranges from contextual situations for a singular fraud investigation to a repeatable analysis of financial processes susceptible to criminal activity in the first place.

If the risk of fraud is really high, financial and banking institutions can employ a **constant or continual approach** to fraud detection. It works particularly well in situations where preventive controls are not practicable or efficient.

The majority of modern financial service companies have **increased management requirements** for information as the audit adjustment is moving from the conventional cyclical approach to a risk-based and longstanding model.

To disclose fraudulent activity, a lot of banks use **special transaction monitoring systems.** By and large, they represent domestically produced software which demands an operator intervention. However, traditional security systems can function well for detecting individual point-of-sale, real-time fraud. But that is only the tip of an iceberg.

There is a list of analytical techniques used to detect fraud. The most effective among them are:

1. **Classification**
   To find patterns among various data elements
2. **Statistical parameters calculation**
   To detect outliers that could reveal fraud
3. **Numbers stratification**
   To disclose unordinary (reductantly high or low) entries
4. **Joining random diverse sources**
   To denote matching values (such as addresses, names and numbers) where they shouldn't exist
5. **Duplicate testing**
   To note duplicate transactions such as claims, payements or finance report items
6. **Gap testing**
   To find out any missing items in serial data where there should be none
7. **Entry dates validation**
   To estimate inappropriate or suspicious times for posting or information entry
8. **Numeric values summation**
   To identify control sums which may have been falsified

Despite all these measures, customers that use their own confirmed devices to complete online transactions may still become the victims of fraud.

The most popular schemes for cheating are:

- Session stealing
- Man-in-the-middle
- Key-loggers
- Phishing

In order to avoid any type of such attacks, banking institutions are advised to undertake a number of security measures:

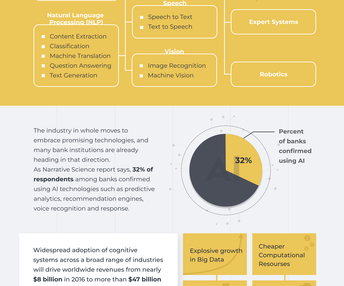
- **They must do their best to stop machine-resident and web-based attacks from fraudulent transactions in progress.**
- **They shouldn't forget to vindicate online banking clients from session-based transaction attacks.**

Our advice here is to **smoothly test the efficiency of fraud-screening models** and rules and update them when testing reports point out the need. Ideally, the system automatically stores the investigation outcome for further use in future. Software models, which are continually refined readily adapt to brand new knowledge. **Auto-generated network graphs** allow strategists catch symptoms and patterns which lead to reformed controls and new monitoring practical methods. This mixture of visibility and adaptation prevents both arising and future threats.

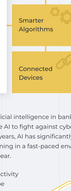
The perspectives for the future also go beyond the scope of any single company. As more companies **choose automated and integrated fraud management systems**, the potential is here to make up a vast consortium of banking institutions sharing their collective experiences in order to get better fraud detection percentage.

AI Technology and Fraud Prevention

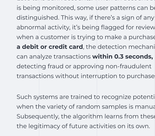
It's fair to say that AI has become quite a buzzword in various fields of business. The financial services industry is no exception. Originally introduced in the 1950s, AI has gained a new wave of popularity just recently due to the variety of reasons. One of them is, obviously, the adoption of new standards in security.



The industry in whole moves to embrace promising technologies, and many bank institutions are already heading in that direction. As Narrative Science report says, **32% of respondents** among banks confirmed using AI technologies such as predictive analytics, recommendation engines, voice recognition and response.



Widespread adoption of cognitive systems across a broad range of industries will drive worldwide revenues from nearly **$8 billion** in 2016 to more than **$47 billion** in 2020 with banking named as one of the top two industries to lead the change.

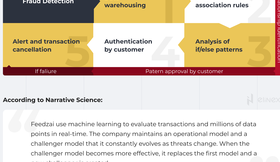


- Explosive growth in Big Data
- Cheaper Computational Resources
- Smarter Algorithms
- Cloud
- Connected Devices

Again, one of the most important uses of artificial intelligence in banking sphere concerns fraud detection. Banks are beginning to utilize AI to fight against cybercrime and address complex issues in real time. Over the last ten years, AI has significantly improved the monitoring process: now it's is capable of learning in a fast-paced environment and respond to fraudsters' techniques as they appear.

Let's take bank accounts. When an account activity is being monitored, some user patterns can be distinguished. This way, if there's a sign of any abnormal activity, it's being flagged for review. So, when a customer is trying to make a purchase **using a debit or credit card**, the detection mechanism can analyze transactions **within 0.3 seconds,** detecting fraud or approving non-fraudulent transactions without interruption to purchases.

Such systems are trained to recognize potential fraud through supervised training, when the variety of random samples is manually classified as genuine or fraudulent. Subsequently, the algorithm learns from these manual classifications to determine the legitimacy of future events on its own.



According to Narrative Science:

> Feedzai use machine learning to evaluate transactions and millions of data points in real-time. The company maintains an operational model and a challenger model that it constantly evolves as threats change. When the challenger model becomes more effective, it replaces the first model and a new challenger is created.

> Another company, ThetaRay, offers a platform that provides financial institutions with the possibility to detect threats such as lending fraud, ATM hacks, money laundering and cyber attacks.

Within several years, the strategic use of AI and machine learning will become an integral part of banking organizations' security principles.

AI can save banks considerable money by eliminating complex fraud cases and protecting their brand. Here at Elinext, we offer a variety of software development services to achieve success in such a market environment. With nearly 100 professionals, we approach challenges from every angle to quickly grasp the data, workflows, compliance requirements, and math behind securities, trading and investments.

elinext.com