Technological solutions to fraud prevention

Mike Southgate, AFEP
May 2016

Fraud detection systems come in a wide range of guises, from the very simple systems which detect last minute changes or maintain a list of known fraud data, to higher end systems which aim to detect changes in payment behaviours or user activities and detect fraudulent transactions in flight.

Like any technological solution, the size and scale of the problem must be understood. A large scale fraud engine designed to detect thousands of alerts a minute is unlikely to be suitable to a small scale firm which has limited instances of fraud. This is because Fraud is an evolving process, and the systems used to detect it need to be constantly updated to reflect new typologies.

Fraud engines also need to be finely attuned to the business purpose and nature of your clients activities. What looks fraudulent for one client base is likely to be regular activity for another client. For example, credit card companies may often flag overseas transactions as suspicious and block cards, which can be immensely frustrating for a regular traveller. Once the system is tuned and becomes aware of the customers frequent travelling, it can be tuned to relax and alert less for that particular customer.

This guide aims to talk through some of the systems and solutions which exist for fraud prevention, and the pitfalls which may occur in choosing a technological solution. This guide does not aim to recommend any particular vendor or carrier, and firms should consider their own risks when choosing a solution.

Big Versus Small scale Solutions

Before considering a large scale (Expensive) fraud engine which has capacity for tens of thousands of reviews a day, the scale and type of fraud should be considered.

Systems designed to detect large volume frauds are unlikely to be tuned to detecting mid level expenses fraud by your employees. High volume systems are also designed to learn “On the job” via machine learning, so may need high volumes of frauds or huge transaction volumes before they can develop a Typology. 3 instances of email fraud a year are unlikely to be a sufficient learning sample.

Registered address c/o Currencies Direct, 45th floor, 1 Canada Square, Canary Wharf, London E14 5AA. Company No. 07917853. Technological Solutions to fraud prevention: AFEP May 2016.

Typology
Noun - "a classification according to general type"

Before they are in the door

One of the best ways to prevent fraud is still with extensive Customer Due Diligence.

The more information you hold on a customer, the more likely you are to spot Red Flags in their due diligence (Customer claims to have a home in Spain but is paying to Argentina?), and the better you understand their business model, the more likely you are to spot changes in transactional behaviour (That doesn't look like an order for Steel widgets…) Additional CDD will also help the firm identify flags and markers which will identify fraud.

Detailed due diligence also plays a part in the 3rd parties which your firm may deal with, or who refer customers to you. For example if your firm is receiving referrals from a company which offers entirely unregulated products and services you may find that the level of fraud relating to these referrals is high.

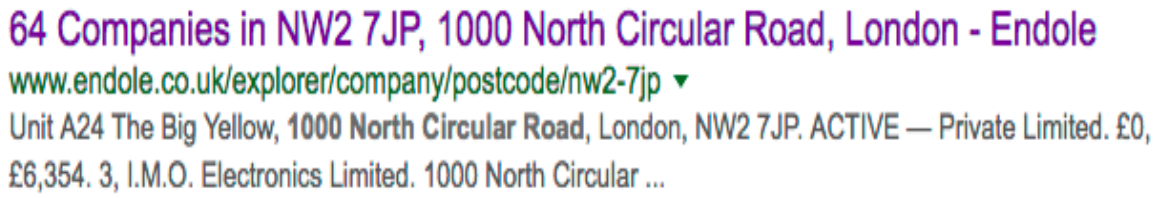
If a particular beneficiary is pointing customers to your firm, this may be because a loophole exists in your processes which makes it easier for customers to sign up, or because lapse controls exist. Where you notice an increase in unsolicited referrals, this may be an additional indicator of fraud.

It should also be noted that Employee fraud may be prevalent at this point, a single sales person who brings onboard a new referrer and then handles all customers may be complicit in the fraud, controls can be created which may circumvent this without excessive technological interventions.

Electronic fraud screening tools for CDD do exist and will search the information your customer provides against a database of known Fraud markers or information mismatches and where possible compare it to unseen markers in your customer's application.

For example if your customer claims to be in the UK, but applicant IP address is in Belarus the system will detect this. The system may also automatically identify "Suspicious" addresses. For example, the address "1000 North Circular Road":

Registered address c/o Currencies Direct, 45th floor, 1 Canada Square, Canary Wharf, London E14 5AA. Company No. 07917853. Technological Solutions to fraud prevention: AFEP May 2016.



Which is a Big Yellow storage company location, hosting 64 companies, 25% of which are less than a year old and have filled no annual documents. Applicant firms from this address may require some additional scrutiny, particularly if they are a new firm.

The tool may also have a database of known "Bad devices" which the fraud tool will be aware of. A client who has recently applied for 10 other accounts with other brokers may be flagged if they do so from the same device or IP address, or where a fraudster has used a device in the past to commit fraud, this will flag.

It should be noted that these tools will require integration and will need visibility of as much application data as possible, including data the customer does not fill in, such as IP, Device ID, location, how long the form took to complete etc and so integration will be extensive, but options from ThreatMatrix, Iovation and other vendors listed below.

Small scale solutions

Sanctions tools:
Where a firm has a known fraud risk, for example a known beneficiary firm which is receiving unauthorized investments, it may be worth utilising existing controls to block this beneficiary.

Many sanctions screening tools allow the systems owner to inject their own sanctions data into the list, in effect creating your own watchlists.

The FCA maintains a list of known "Unauthorised investment firms" which your watchlists vendor may not include. Adding these manually may prevent clearly fraudulent activity.

Similarly when a firm encounters a fraudster through their own experience, details of the beneficiary can be added to the list to prevent a recurrence.

Change management:
Many frauds involve changes, either to the beneficiary at the last moment, to the controller of an account or to the contact details at a firm so that confirmations are not received.

Controls around change management may mean that in order to update a customer record, back office review and approval is required. Beneficiary changes after a payment is confirmed may flag to asks more questions of your customer (Did you get this change

Registered address c/o Currencies Direct, 45th floor, 1 Canada Square, Canary Wharf, London E14 5AA. Company No. 07917853. Technological Solutions to fraud prevention: AFEP May 2016.

request via email just after you sent payment confirmation to your supplier?) This allows extra checks (such as checking that a new email address is a related corporate email) to take place.

Change management and 2 pairs/4 eyes checks are also useful at reducing internal employee fraud by preventing a single actor from setting up and creating payments which are fraudulent.

Customer flags:
Certain customer types are more susceptible to certain frauds. A corporate customer is unlikely to be the victim of frauds relating to pension investment scams, conversely an older customer is unlikely to be paying a steel company who has just changed their invoice details.

Flags in the system, for example “Customer has just reached pensionable age” may alert staff if the user calls in claiming they are going to invest in bamboo farms in Venezuela.

Emails and Confirmation calls:
Emails are susceptible to a range of hacks. An email which is 1 character off, or is Tony.Hutchinson instead of TonyHutchingson is unlikely to be noticed by a human user. Similar domain names, (Google.com versus Gooogle.com) can be hacked by adding certain extra characters.

Handling communications through your CRM means that the system will detect the incorrect email address by not associating them with your customer. Alternatively creating formal contacts in most email systems means that emails from unknown individuals will make it clear when the original contact does not get in touch.

Where a user facilitates a relationship solely via email, a confirmation call should be made to a known contact number (Not the one from the email signature!)

Large Scale Solutions

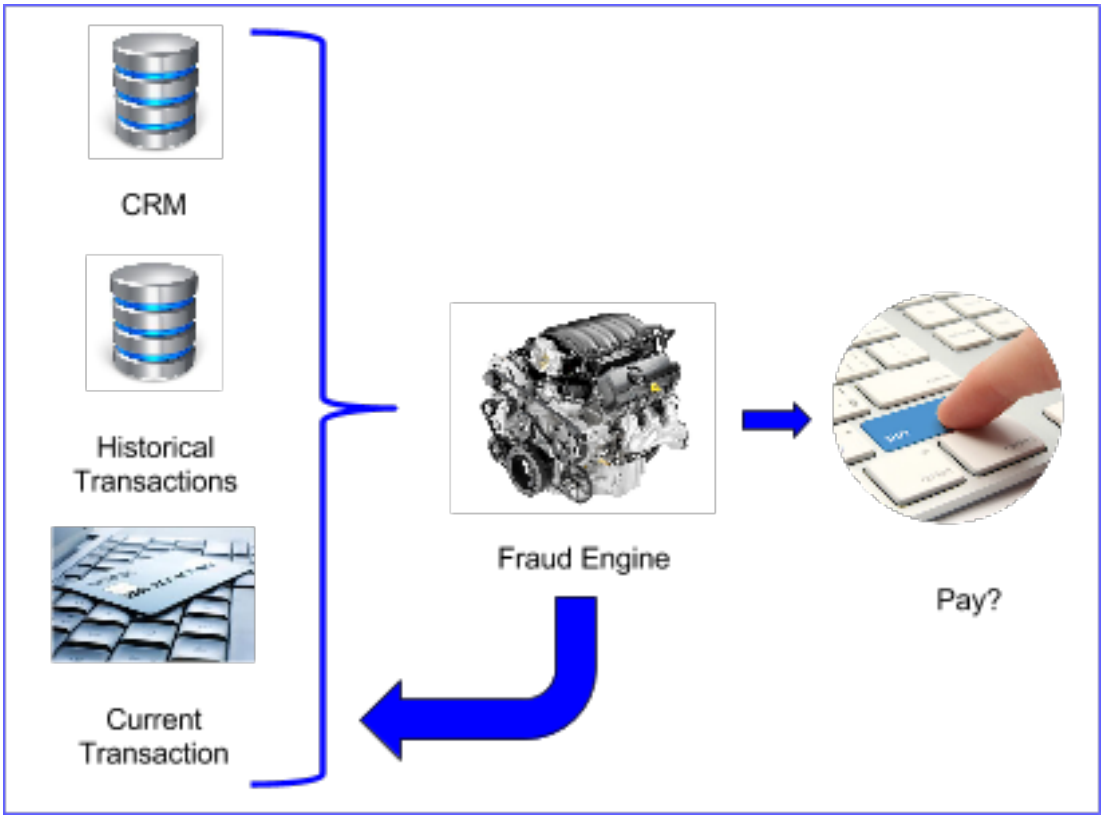
A large range of tools exist which aim to detect fraud. Fraud engines typically assign each payment a score, based on a series of metrics. A really simple fraud score system may have the following inputs –

- Value of Transaction
- Frequency of Transaction
- Location
- If this is the first payment to a beneficiary
- Age of customer

Registered address c/o Currencies Direct, 45th floor, 1 Canada Square, Canary Wharf, London E14 5AA. Company No. 07917853. Technological Solutions to fraud prevention: AFEP May 2016.

A Customer who often spends only £25-50, once a week, in the same supermarket and has done so for 2 years on a credit card, is likely to flag when attempting a new transaction for $1000 in a different country, at an auto parts store.

A system may assign 5 points to each of these elements, with 1 point being assigned for "Normal" activity, and 5 points for "Abnormal" activity. Out of a total score of 25 possible points, the system may prevent a transaction taking place if it has a score of over 12.



Such a solution requires a large volume of live inputs for each transaction, including customer data, historical transaction data and data of the current transaction. The more data that can be input into a system, the more effective a decision can be made about the transaction being assessed.

This means that a fraud engine will be very similar to a sanctions screening system and should be one of the final stages of a payments workflow. This prevents last minute changes to the transaction from affecting the fraud decision.

Registered address c/o Currencies Direct, 45th floor, 1 Canada Square, Canary Wharf, London E14 5AA. Company No. 07917853. Technological Solutions to fraud prevention: AFEP May 2016.

Device Identification
Device ID's, or Fingerprinting uses a series of markers to establish whether your user is logging in from their normal device. This may look at markers such as the device type, operating system, Language and serial number to ensure your user not only knows their password, but is logging in from a trusted device. Sudden logins from a different PC will be a clear red flag for Fraud.

The volume of details of the current transaction which are included in a decision can be wide ranging. For example, the device used for a transaction may be very specific, so when a fraudster utilises a different device to attempt a transaction (For example logs in from a different PC) the system recognises the device and refuse this transaction.

The system may also be able to consider the payment method used, recognising that transactions which are paid for on Debit cards have a higher incident rate of Fraud when compared to transactions settled by a wire transfer from the customer.

Large scale systems are often highly customised and will need to know the “Normal” transaction that takes place through your firm. The flow of data will also have to be specific to the different systems that you firm has. Calibration of the system will also need to take place to reduce the volumes of false positives, and similarly to a sanctions screening system changes in the transaction process flow will result in a change in the fraud system.

Large or Small?

Which system or solution your firm chooses will depend on the type and scale of fraud which the firm is experiencing and how orders are received.

Firms with a small scale fraud issue (A few incidents a year) need to consider how large the problem is, and whether there is a simple process change which might help, or if existing systems can be used to reduce losses.

Registered address c/o Currencies Direct, 45th floor, 1 Canada Square, Canary Wharf, London E14 5AA. Company No. 07917853. Technological Solutions to fraud prevention: AFEP May 2016.

Vendors

https://www.iovation.com/ - Device Fingerprinting and fraud detection systems - Provides a list of “Bad Actor” devices know to be involved in fraud.

https://www.featurespace.co.uk/ - UK Based startup offering a holistic fraud tool.

http://www.niceactimize.com/ - Case management and fraud engine tools.

http://banking-software.com/ - Provides core banking solutions and fraud and money laundering tools.

https://www.threatmetrix.com - Compliance Assurance software and Transactional review tools

http://www.cybersource.com/ - Part of the Visa group, also offers its fraud tools outside of card processing.

Registered address c/o Currencies Direct, 45th floor, 1 Canada Square, Canary Wharf, London E14 5AA. Company No. 07917853. Technological Solutions to fraud prevention: AFEP May 2016.