Predictive analytics in fraud and AML

Clinton Mills

Received (in revised form) 2nd January, 2017

GBG DecTech, First Floor, 722 Mt Alexander Road, Moonee Ponds, Victoria 3039, Australia
Tel: +61 3 9377 8700; E-mail: cmills@dectechsolutions.com

Clinton Mills *has more than 25 years' experience in the use of technology to manage consumer and small business fraud and credit risk and compliance throughout the Asia Pacific, Middle East, African and European regions. He has worked with many banks and other financial services companies globally to implement solutions to prevent fraud and manage risk and compliance. Clinton has been the Managing Director of GBG DecTech for 15 years, a Microsoft Gold qualified partner in application development with Silver in data analytics and data platform. Clinton reports to the Group Managing Director of GBG, an identity data intelligence company listed on the London Stock Exchange that helps organisations make decisions about the customers they serve and the people they employ.*

Abstract

The common problem we are all facing in fraud risk and compliance these days is how to address the challenge of reducing false positive rates to optimise detection for fraud and, very importantly when monitoring transactions for anti-money laundering/counter-terrorist financing (AML/CTF), how to avoid being overwhelmed by alerts. This paper aims to introduce to the reader the importance of considering the use of predictive analytics in the financial crimes prevention strategy and programme of any organisation. This paper starts by offering a detailed background of the scope of the fraud and AML/CTF problem in general, focusing on the high costs that many organisations face when trying to prevent and detect financial crimes and also protect their genuine customers from becoming victims of financial crimes. The paper goes on to describe the most common challenges that organisations face, in particular resource challenges when devising and implementing their strategies. It also encourages a collaborative approach to fraud prevention. The reader can expect to gain insightful information about how predictive analytics can be used in the prevention of financial crimes and what type of benefits it can deliver.

Keywords: predictive, model, detection, false positive, prevention, victim

Clinton Mills

INTRODUCTION

If this author had to pick the risk and compliance question that he is most commonly asked by customers and potential customers regardless of location, it is the following: 'How can I reduce my false positive rates to optimise detection for fraud and also very importantly, when monitoring transactions for our AML/CTF programme to avoid being overwhelmed by alerts?'

Unfortunately, there is not a one-sentence answer. Whether your organisation is in the business of banking and finance, insurance or superannuation/pension schemes, e-commerce or even betting and gaming there is no end of fraudsters lining up to commit financial crimes at your expense.

Most of us read about financial fraud in the media on a weekly basis, as well as money laundering and terrorism financing on a regular basis.

The challenge is to find the right balance between investment in technology and human resource as well as reducing losses due to financial crimes while at the same time being compliant with local and international regulations. All of this, of course, needs to be done on a limited budget, a difficult balancing act.

Journal of Financial Compliance
Vol. 1, No. 1 2017, pp. 17–26

2398-8053

What is the scope of the problem?

The total cost of a fraud, money laundering or terrorism financing attempt and complete set of risks facing a financial institution in the aftermath of a fraud attack or being used for money laundering or terrorism financing go far beyond the losses themselves. It is therefore important to consider the total cost: the average organisation may be losing 5 per cent of annual revenues to fraud[1] while the global loss is US$3.7 trillion.[2]

It is a well-known fact that many financial organisations still do not have a firm grasp or ability to accurately report on losses due to credit defaults versus losses due to financial crimes such as application fraud, transaction fraud, money laundering or terrorism financing.

Some organisations see overlap between credit losses as well as fraud losses and sometimes organisations find it difficult to separate them. For example, a fraudulent application for a credit card which ends up being approved and is used up to the limit with the first payment missed would end up in collections. If the debt ages without being collected it is often written off as a credit loss without being properly investigated to establish if it was actually a fraud loss.

The definition of the author, however, is pretty clear cut. A credit loss is a loss resulting from a 'credit bad', a result of one or more of the following:

- incapacity or inability to repay;
- refusal to pay a genuine debt (eg dispute with lender, dispute about fees or service etc).

A fraud loss is a loss resulting from a 'fraud bad', a result of one or more of the following:

- unwillingness to repay/no intention of repaying;
- UTC (Unable To Contact);
- FPD (First Payment Default);
- third party uses the identity or account of a victim or deceased person;
- individuals or companies suspected of or found guilty of financial crimes;
- individuals or companies who have attempted to defraud or successfully defrauded other financial services providers;
- individuals or companies who falsified information in order to obtain money;
- individuals or companies who received money knowing that a staff member of the lender fraudulently helped them (internal fraud or intermediary fraud).

On the other hand, we can define money laundering as follows:

- the concealment of the origins of illegally obtained money, in a number of ways, typically by means of transfers involving foreign banks or legitimate businesses;
- often purposed towards financial crimes, tax evasion and terrorism financing.

In summary, a credit bad is a result of a genuine customer not able to repay their debt (eg due to losing their job or becoming swamped with credit and therefore overcommitted) whereas a fraud bad is a result of a dishonest customer or a third party deliberately committing a financial crime.

There is one further slight complication in that not all fraud necessarily results in a loss. For example, 'soft fraud' may be committed by an individual who fabricates his or her income proof in order to obtain a higher credit limit which may not necessarily result in a loss to the lender as he or she may continue to pay his or her loan. Nevertheless, if he or she did default then it should be considered as a fraud loss rather than a credit loss.

This author has seen many instances where organisations are only counting the quantifiable financial losses as financial crimes losses, however he can guarantee that this is usually a significant underestimate of the total cost: in the majority of cases mentioned legal costs (both internal and external, which can obviously be significant) are usually not counted. In addition to that this author has observed that many organisations are not

accurately quantifying their losses caused by the amount of time and the number of fraud prevention resources that are required to conduct investigations in the areas of both prevention and also prosecution. Therefore, it is quite safe to say that even the commonly recognised costs of financial crimes tend to be underestimated.

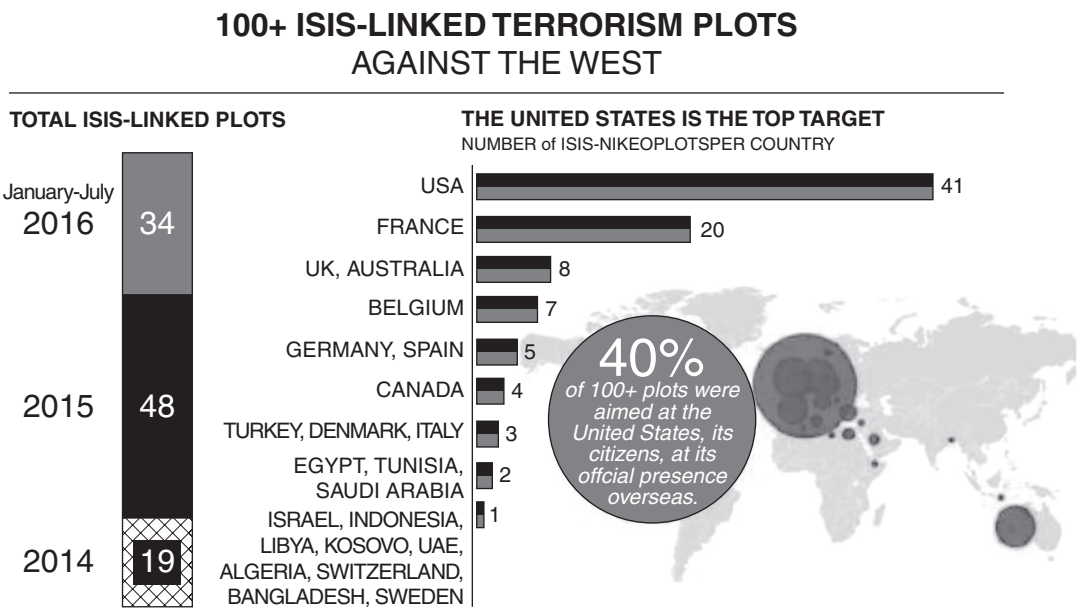
Now, however, this author wishes to highlight some of the often-forgotten hidden costs of fraud, the first of which is the reputational risk the organisation suffers as a result of the customer being left with the perception that the organisation has poor security and/or compliance. The second is the knock-on effect which can erode confidence in the brand of the organisation and this obviously results in customer loss of trust.

Unfortunately, this author has also seen instances of staff morale issues due to staff feeling they failed their customers by not being able to detect financial crimes occurring on customer accounts. Therefore, the whole cycle can result in customer and staff churn as well.

Many of us will also be aware of the even worse consequence, a fine from the regulator and in some cases prosecution and/or resignation of the management of the organisation. At least one bank fine for not detecting money laundering was so high it wiped out the profit of the bank for the entire year.

The top ten fines for non-compliance have ranged from hundreds of millions to billions of US dollars, the largest of which have been due to money laundering and terrorism financing lapses which should have easily been detected as well as due to anti-sanctions. Of the top ten fines, seven were due to non-compliance and the other three internal fraud/governance.

This author can state that there was little to no concern with money laundering or terrorism financing happening in Australia, as recently as 2007. But as can be seen in Figure 1, the global scene can change quickly,



Australia has been ranked third, along with the UK, on the terror hit list. Picture: Department of Homeland

Figure 1 Terror group list http://www.news.com.au/world/middle-east/isis-why-we-hate-you-magazine-details-six-reasons-for-war-on-liberalist-sodomites/news-story/c512bf5c5407f97aef3ad-19e7dfd27a4

with Australia now ranked third on the terror group hit list behind the US and France, equal with the UK.[3]

It can therefore can be seen that every country now needs to start taking terrorism financing seriously.

How can one cope with the resource challenges?

It is invariably difficult to move away from the fact that we need to assign a certain amount of human resource to both prevention and detection of fraud, money laundering and terrorism financing.

From the experience of this author the average number of alerts (either fraud alerts or AML/CTF alerts) that can be reviewed by a reviewer each day is approximately 50 while between 40 and 60 is still within the normal range, 40 for a new reviewer and 60 for an experienced reviewer: although if a particular case cannot be quickly determined as positive or false positive and needs further investigation these numbers assume the reviewer can pass the case off to an investigator. This author is also often asked what type of background his fraud prevention team needs (and similar applies for AML and CTF), which is responded to as follows:

- Fraud reviewer: it is good to get someone who has an education in finance, worked as a bank officer for at least a couple of years, customer interaction so they can understand banking processes and products well and demonstrated skills such as attention to detail and also an inquisitive attitude.
- Fraud investigator: this is the next step after having been a fraud reviewer for a number of years.
- Fraud manager: this is the next step after having been a fraud investigator for a number of years.
- Fraud analyst: it is good to get someone with an education in one or more of mathematics, statistics and engineering: this role requires attention to detail and an analytical mind.

This author often finds that organisations are not making simple investments in technology that could significantly reduce the amount of human resource (and therefore, significant cost) required to verify transactions with customers that could potentially be fraudulent, with the most obvious being the use of automated SMS. The use of SMS to confirm transactions with customers essentially facilitates faster (instant) customer contact and also the ability to verify a significantly higher volume of transactions through automated means rather than relying on a human reviewer to do so.

What are the challenges in fraud prevention and money laundering detection?

Firstly, there are five main difficulties associated with fraud prevention:

- It is uncommon
  Despite the fact that fraud is happening every day, legitimate transactions still significantly outnumber fraudulent transactions.

  Most organisations do not experience excessive amounts of fraud otherwise they would not be able to stay in business. But with small amounts of fraud occurring it is difficult to undertake comprehensive analysis and therefore to formulate strategies based on that analysis. A solution is to participate in a financial crimes bureau such as an application fraud bureau or a financial crimes exchange, industry level platforms for sharing data for the purposes of financial crimes prevention across multiple financial organisations (and often across multiple industries). Some organisations feel hesitant to share data which could help their competitors, a concern which is addressed in the note below about such ('Does sharing data help competitors?').

- It is well-considered
  Once fraudsters find a new modus-operandi they exploit it until discovered and blocked.

  Fraudsters are not one-off credit defaulters: they are often part of an organised crime ring, a syndicate or group of operators that has committed multiple identity takeovers or identity fabrications. Successful fraud has often been well planned and the majority of customer-facing staff within most organisations are not trained to detect let alone expect it.
- It is imperceptibly concealed
  Fraudulent transactions often exhibit the same characteristics and patterns as genuine transactions.

  There are two issues here, the first of which is that it is not unusual for genuine customer behaviour to change. Therefore, if we are going to generate an alert every time the customer does something slightly different we will have a lot of false positives to deal with. Secondly, fraudsters may mimic genuine customer behaviour before maximising the fraud potential ('bust-out fraud').
- It is time-evolving
  Fraud keeps changing daily, weekly and monthly, therefore the challenge is to devise strategies that can detect old, existing and new fraud.

  Business strategies around credit and fraud risk are completely different. Credit risk is relatively stable and does not change frequently however fraud risk is continuously changing: the fraud prevention strategy that worked well last month may not work well today. It is not so much of an issue to devise a strategy to detect fraud that has already occurred, as the modus operandi can be investigated and evaluated. Therefore if the same type of fraud happens again the strategy will be in place to detect it. The difficulty, however, is trying to predict the type of fraud that has not happened yet.
- It is carefully organised
  A fraud incident typically leads to many fraudulent transactions. Social network analysis is needed to detect the fraud early in order to minimise the loss.

  It is important to identify and highlight for investigation suspicious links in data before the fraud actually occurs. 'Suspicious links' could include multiple different accounts or customers sharing the same mobile phone number or address or transfers among a common set of accounts. Money laundering may not necessarily be one large amount but rather many small amounts.

Does sharing data help competitors?

Fraud prevention should be viewed as a collaborative issue and not a competitive issue. Organisations will not generate more revenue by preventing fraud but instead will reduce losses. Data sharing for the purposes of fraud bureau can therefore be viewed not as helping your competitors but rather as all members of the fraud bureau mutually helping each other for the betterment of each member and he betterment of the industry.

Sometimes, 'bigger' members (in terms of the volume and ticket size of applications processed) may believe they are potentially contributing more benefit to the fraud bureau than other smaller members. This is potentially true but bigger members will also save more fraud loss and therefore the benefit is commensurate with the contribution.

What is predictive analytics and where can it be used?

Predictive analytics in fraud prevention is the use of statistical processes and techniques to predict the likelihood that an application or transaction is fraudulent, based on the characteristics of that application or transaction without needing human subjective analysis. It provides fraud management with an objective assessment of the fraud risk that an application or transaction carries. Based on this measurement of risk (eg a fraud score between 0 and 1,000) fraud management can decide on the most appropriate action to be taken.

There are five primary objectives of predictive analytics or fraud models:

- *Accuracy:* the ability of a model to correctly classify as fraud or non-fraud new or previously unseen data.
- *Speed:* in generating and using a given model – especially in prevention, a fraud model must give a split-second decision.
- *Robustness:* ability to handle noisy data, missing values etc.
- *Scalability:* ability to efficiently handle large data sets, as in a transactional environment there may be hundreds of transactions coming in per second.
- *Interpretability:* ability for users to understand and gain insight from a particular model: a traditional scoring model is interpretable as opposed to a neural network which is essentially a 'black box'.

Predictive analytics have been successfully used in the following industries and areas:

- Banking and finance
  - banking and other lending product applications for credit, known as 'application fraud' models;
  - credit card and debit card issuing, known as 'transaction fraud' models;
  - merchant and ATM acquiring, known as 'transaction fraud' models;
  - online and mobile banking, known as 'transaction fraud' models;
  - anti-money laundering (AML), known as 'transaction monitoring' models.
- Insurance
  - policy underwriting and insurance claims, known as 'application fraud' models.
- Telecommunications
  - new mobile phone accounts, known as 'application fraud' models.

What type of data do fraud models use?

We should not pre-determine the data that fraud models use and rather analyse all available data. Both credit application fraud and transaction fraud/monitoring models use three types of data.

For credit application fraud models this includes the following:

- demographics eg channel, home postcode, education level, occupation;
- derived data eg age of applicant, mobile phone service provider, distance between home postcode and sourcing location;
- social network data eg number of applications from the same company in the last seven days, matching credit bureau history of applications from the same introducer.

For transaction fraud/monitoring models this includes the following:

- transaction information eg country code, transaction amount, POS entry mode, device type;
- calculated data eg average transaction amount for the last seven days, average number of transactions per day, frequency of this type of transaction;
- social network data eg frequency of transactions at the same merchant/ATM, number of customers sharing the same home address.

How do we build a fraud model and what can it deliver?

We need to gather sample data (called 'observations') which, for a credit application fraud model for example, would include the demographics mentioned above, from which we would calculate the derived data and the social network data. This data would be used to model which types of sample data are likely to result in a fraud application or a genuine application (called an 'outcome').

This is a binary outcome (ie fraud or genuine) and therefore we would often use logistic regression analysis to model the data.

Developing a robust model requires a certain amount of historical data. When developing both application and transactional models we usually recommend a

minimum of six months' worth of application or transaction data and a maximum of 12 months. Less than six months is not ideal as the model will be specific to recent fraud and may not cater well for fraud occurring over a longer period of time: we usually do not model data more than 12 months old as fraud trends change frequently, meaning that such data may not be representative of fraud happening now.

The 'robustness' of a model means its ability to be accurate over time and across the whole population of applications or transactions. A robust model requires at least 1,000 fraudulent observations during the historical period: it is possible to develop models on less fraudulent observations than that, say 500, however the model will not be as robust.

Fraud models are typically more predictive than credit models and can reach Gini coefficient of 70–80 per cent (predictiveness rating) whereas credit scorecards are usually around the 60–70 per cent mark. Some predictive fraud models can rank 50 per cent of the fraud applications/transactions in the top 0.5 per cent of fraud scores. It is true, however, that fraud models need to be redeveloped more frequently than credit models, again as credit risk is more stable over time compared to fraud risk. Ideally this author recommends that fraud models are redeveloped at least every 12 months so the changing nature of fraud can be continuously taken into consideration. While it is important that any model is monitored on a regular basis (at least quarterly) for its effectiveness the strong recommendation of this author is not to spend too much effort on scorecard validation and even fine-tuning exercises as it is much more efficient to simply redevelop these.

A common approach this author recommends in the use of fraud and AML models is in the reduction of false positives. Using both a predictive analytics and rules based approach allows more strict fraud/AML rules to be applied for high scoring (high risk) applications and transactions, as these are are statistically more likely to be fraud/AML/CTF. Conversely, less strict fraud/AML rules can be applied for low scoring (low risk) applications and transactions as these are statistically less likely to be fraud/AML/CTF, which will significantly reduce the false alerts and false positive rate.

Out of interest, there are several characteristics that we commonly see appearing in our predictive models, firstly for transaction fraud detection:

- Authorisation type
- Time and distance in between transactions
- Attempted spend/withdrawal above limit
- Time of day
- Multiple high risk transactions in a row

And secondly for money laundering (based on reported incidents):

- Country to country combinations
- Currency to currency combinations
- Accounts being accessed from multiple different locations
- Account holder details occurring on multiple accounts (eg contact number, home address)
- Sudden increase in account activity/rapid movement of funds

How do I address the false positive challenge?

This is actually the most common question this author is asked, which is always responded to with a seven-point plan:

- Build and maintain a whitelist of safe attributes, for example:
  - Accounts
  - Customers
  - IP addresses
  - Staff
  - Merchants.
- Avoid triggering alerts for behaviour already investigated and proven to be genuine.
- Continuously use champion/challenger testing which in fraud detection and AML is more important than ever. Apply your normal strategy to the majority of the

population ('champion') but a competing approach to a random minority of the population ('challenger'). Evaluate the effects of the champion versus challenger strategies in terms of fraud detected versus false positive rates. If the challenger was more effective then replace the champion strategy and devise a new challenger strategy. This author recommends that a champion/challenger strategy should run for three months.

- Review, maintain and clean up blacklists and watch lists regularly or otherwise put an expiry date on them.
- Fine tune matching rules to avoid unnecessary alerts.
- Automate manual actions eg convert a phone call to an SMS.
- Use predictive scores to apply less strict strategies for low risk applications or transactions.
- For AML, identify and understand the risk points to your business and apply the appropriate rules that will mitigate and manage those risks. This will enable your AML programme to be more specific, tailored and not generic in order to satisfy your regulator, as well as significantly reduce false positives.

It is absolutely imperative for organisations to consider all monetary channels in order to be completely compliant. Typical examples are shown in Figure 2.

With the number of customers moving to online and electronic channels it is no longer an option to grab IP and device information but rather imperative. Customers continue to move from branch, direct sales and cardholder present channels to online, internet and mobile device channels.

Device fingerprints these days can give us 53 pieces of information about the device and location from which an application or transaction is originating. This includes information such as the device ID, the IP address, the language on and location of the device.

Figure 3 chart shows the importance of gathering such information. On the left-hand side global online banking usage statistics show that the number of people who have never used online banking continues to decrease and the number of people using it daily continues to increase.

Similar trends are shown for mobile banking usage statistics which show the importance of being continuously aware that fraud prevention strategies need to keep up with the changing behaviour of customers and therefore relevant fraud prevention strategies.

Trust in your organisation has also now become a primary factor, which includes trust in the organisation to hold customer data securely and also prevent fraud. Figure 4 shows the behaviour that trust or distrust can drive.

Figure 2 Monetary channels

Product/Channel	Used For
Online and mobile banking	All transactions occurring via digital channels
Internal	Transactions originating via tellers or call centre staff
Credit card	All credit card transactions (issuing)
ATM	All transactions occurring at ATMs
Merchant	All acquiring transactions
Payments	Foreign trade, telegraphic transfers, SWIFT etc
General personal and business banking	General suspicious monitoring, such as direct debits, non-monetary transactions, deposit and withdrawal activity, cheques etc
Treasury	All treasury and other ledger transactions

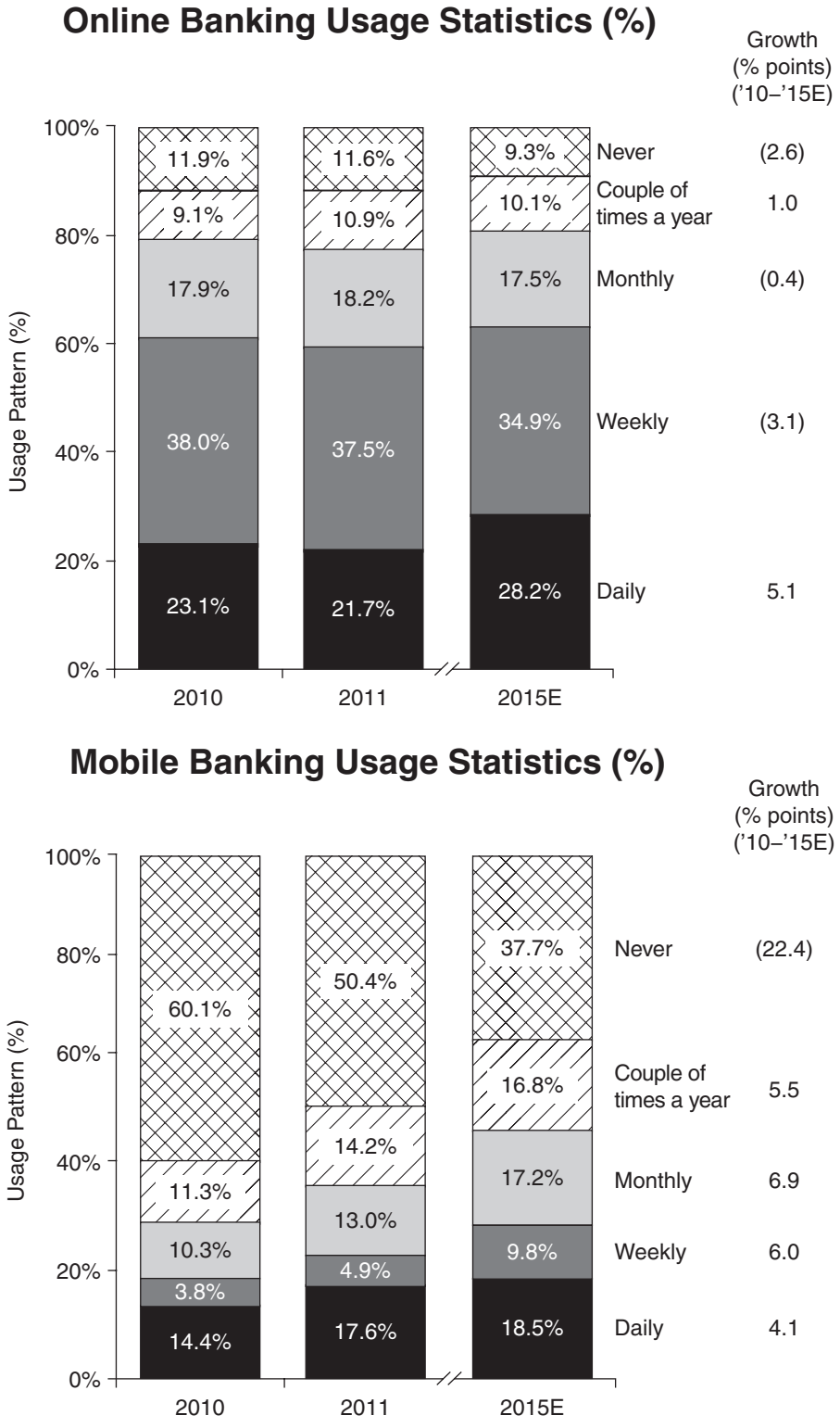


Figure 3 Banking usage

Source: Capgemini Analysis, 2012; 2012 Retail Banking Voice of the Customer Survey, Capgemini; and World Retail Banking Report 2012, Capgemini and Efma.

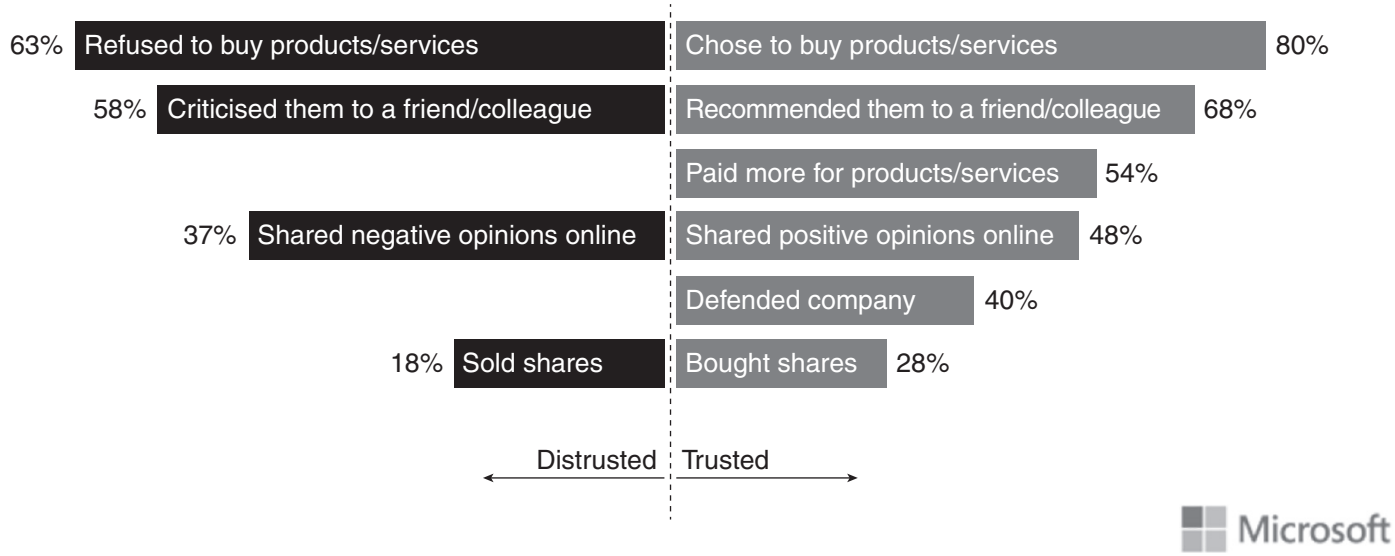


Figure 4 Trust in innovation matters
Source: Edelman Trust Barometer Survey, 2015; question on actions in relation to organisations you trust/distrust.

CONCLUSION

In summary, predictive analytics will play an increasingly important role in each of fraud, AML and CTF prevention and detection. A robust set of rules is always a good starting point but cannot alone detect all fraud and financial crimes: Organisations therefore are recommended to consider introducing predictive analytics into their financial crime prevention strategies at the earliest opportunity.

Organisations are also expected to invest in the protection of genuine customers, to ensure their identity and account is not compromised. There are some organisations who invest in an increasing amount of staff to manually verify more transactions but this significantly increases their costs. Based on the experience of this author the investment in predictive analytics is worthwhile as it enables a higher detection rate while keeping dreaded false positives to a minimum.

References

(1) The Association of Certified Fraud Examiners (ACFE) (2014), 'Report to the Nation on Occupational Fraud & Abuse – Global Fraud Study'.
(2) Ibid.
(3) news.com.au (accessed 4th August, 2016).